Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONCOURS EXTERNE POUR LE RECRUTEMENT D'INSPECTEURS DES DOUANES ET DROITS INDIRECTS DES 13, 14 ET 15 JANVIER 2020

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 1

(DURÉE : 4 HEURES – COEFFICIENT 6)

Rédaction d'une note de synthèse à partir d'un dossier relatif aux questions économiques, financières et sociales

À partir des documents suivants, vous rédigerez une note d'environ 4 pages consacrée à la cybersécurité.

AVERTISSEMENTS IMPORTANTS

L'usage de tout matériel autre que le matériel usuel d'écriture et de tout document autre que le support fourni est **interdit**.

Toute fraude ou tentative de fraude constatée par la commission de surveillance **entraînera l'exclusion du concours.**

Veillez à bien indiquer sur votre copie le nombre d'intercalaires utilisés (la copie double n'est pas décomptée).

Il vous est interdit de quitter définitivement la salle d'examen **avant le terme de la première heure.**

Le présent document comporte **35 pages** numérotées.

Tournez la page, SVP

Liste des documents

DOCUMENT 1

Appel de Paris : Pour la confiance et la sécurité dans le cyberespace

Site FRANCE DIPLOMATIE, 12 novembre 2018

Le cyberespace joue désormais un rôle capital dans tous les aspects de notre vie ; il relève de la responsabilité d'un grand nombre d'acteurs, chacun dans son domaine propre, de le rendre plus fiable, plus sûr et plus stable.

Nous réaffirmons notre soutien à un cyberespace ouvert, sûr, stable, accessible et pacifique, devenu partie intégrante de la vie sous tous ses aspects sociaux, économiques, culturels et politiques.

Nous réaffirmons également que le droit international, dont la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international coutumier, s'applique à l'usage des technologies de l'information et de la communication (TIC) par les États.

Nous réaffirmons que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne et que le droit international des droits de l'Homme s'applique au cyberespace.

Nous réaffirmons que le droit international constitue, avec les normes volontaires de comportement responsable des États en temps de paix et les mesures de développement de la confiance et de renforcement des capacités élaborées dans le cadre des Nations Unies, le fondement de la paix et de la sécurité internationales dans le cyberespace.

Nous condamnons les cyberactivités malveillantes en temps de paix, notamment celles qui menacent des individus et des infrastructures critiques ou qui ont pour effet de leur causer des dommages importants, sans discernement ou systémiques, et nous accueillons avec satisfaction les appels invitant à améliorer leur protection.

Nous nous félicitons également des efforts déployés par des États et des acteurs non étatiques pour venir en aide de manière impartiale et indépendante aux victimes de l'usage malveillant des TIC, que celui-ci intervienne en période de conflit armé ou non.

Nous reconnaissons que la menace constituée par la cybercriminalité impose de redoubler d'efforts afin d'améliorer la sécurité des produits que nous utilisons, de renforcer nos défenses face aux criminels et de favoriser la coopération entre toutes les parties prenantes, tant à l'intérieur de nos frontières nationales qu'au-delà de celles-ci, et que la Convention de Budapest sur la cybercriminalité est à cet égard un outil essentiel.

Nous reconnaissons les responsabilités des principaux acteurs du secteur privé pour développer la confiance, la sécurité et la stabilité dans le cyberespace et nous encourageons les initiatives qui visent à accroître la sécurité des processus, produits et services numériques.

Nous nous félicitons de la collaboration entre les pouvoirs publics, le secteur privé et la société civile en vue d'élaborer de nouvelles normes de cybersécurité permettant aux infrastructures et aux organisations d'améliorer leurs systèmes de cyberprotection.

Nous reconnaissons que tous les acteurs peuvent apporter leur soutien à un cyberespace pacifique en encourageant la divulgation responsable et coordonnée des vulnérabilités.

Nous soulignons la nécessité de développer une vaste coopération dans le domaine du numérique et les efforts de renforcement des capacités de tous les acteurs, et nous encourageons les initiatives qui permettent d'accroître la résilience et les compétences des utilisateurs.

Nous reconnaissons la nécessité d'une approche multi-acteurs renforcée et d'efforts supplémentaires afin de réduire les risques qui pèsent sur la stabilité du cyberespace et d'établir davantage de fiabilité, de capacité et de confiance.

À cet effet, nous nous déclarons résolus à agir de concert, au sein des instances existantes et par le biais des organisations, institutions, mécanismes et processus appropriés, pour nous venir mutuellement en aide et mettre en place des actions en coopération afin, notamment :

- d'empêcher les cyberactivités malveillantes qui menacent des individus et des infrastructures critiques ou qui leur causent des dommages importants, sans discernement ou systémiques, et d'y remédier ;
- d'empêcher les activités qui portent atteinte intentionnellement et dans une large mesure à la disponibilité ou à l'intégrité du cœur public de l'internet ;
- de développer notre capacité de prévenir les interférences de la part d'acteurs étrangers destinées à déstabiliser des processus électoraux au moyen de cyberactivités malveillantes ;
- d'empêcher le vol de propriété intellectuelle à l'aide des TIC, notamment des secrets industriels ou autres informations commerciales confidentielles, dans l'intention de procurer des avantages concurrentiels à des entreprises ou à un secteur commercial ;
- d'élaborer des moyens d'empêcher la prolifération d'outils malveillants et de pratiques informatiques destinés à nuire ;
- d'accroître la sécurité des processus, produits et services numériques tout au long de leur cycle de vie et d'un bout à l'autre de la chaîne d'approvisionnement ;
- de soutenir les actions visant à développer une hygiène informatique avancée pour tous les acteurs ;
- de prendre des mesures pour empêcher les acteurs non étatiques, y compris le secteur privé, de mener des actions cyber offensives en réponse à une attaque dont ils seraient victimes, pour leur propre compte ou pour celui d'autres acteurs non étatiques ;
- de favoriser une large acceptation et la mise en œuvre de normes internationales de comportement responsable ainsi que de mesures de développement de la confiance dans le cyberespace.

En vue d'assurer le suivi des progrès accomplis sur ces sujets dans le cadre des instances et mécanismes appropriés, nous convenons de nous réunir de nouveau en 2019 lors du Forum de Paris sur la paix et du Forum sur la gouvernance de l'Internet à Berlin.

DOCUMENT 2

Revue stratégique de cyberdéfense [Extraits]

Site du Secrétariat Général de la Défense et de la Sécurité Nationale- 12 février 2018

1.5 Une régulation internationale encore trop balbutiante

Le tableau présenté précédemment d'une menace toujours plus structurée et de systèmes rendus plus vulnérables par la numérisation et leur inter-connectivité croissante s'inscrit dans un contexte international où aucun accord multilatéral n'a encore pu être trouvé pour établir une architecture et des règles de sécurité communes régissant les relations entre États et entre acteurs privés et publics à l'ère numérique.

1.5.1 Les négociations internationales sur la régulation du cyberespace à un tournant

Le cyberespace n'est pas totalement dépourvu de normes et de règles, dans la mesure où celles du droit international ou les grandes principes qui régissent les relations entre États s'y appliquent. Ainsi, les négociations, sous l'égide des Nations-Unies, du « groupe des experts gouvernementaux sur la cybersécurité » (GGE), organisées dans des formats différents à cinq reprises entre 2004 et 2017, ont permis de reconnaître, dès 2013, l'applicabilité du droit international, et notamment de la Charte des Nations-Unies, au cyberespace, puis de consolider, en 2015, un socle d'engagements volontaires de bonne conduite pour les États dans ce domaine. Ces « normes de comportement responsable » s'articulent autour de plusieurs grands principes ou objectifs. Afin de faciliter la coopération et réduire les risques d'incompréhensions, il est ainsi recommandé aux États de faire preuve de transparence sur leur organisation et leur posture nationale en matière de cybersécurité et d'adopter un comportement coopératif vis-à-vis des pays victimes d'attaques émanant de leur propre territoire, en particulier lorsque l'attaque vise une infrastructure critique. Afin de renforcer la résilience globale de l'espace numérique, chaque État est également encouragé à renforcer sur le plan national sa propre cybersécurité, et notamment celle de ses systèmes les plus sensibles, comme ceux des infrastructures critiques. Un autre objectif est de lutter contrer la prolifération des outils informatiques malveillants et de préserver l'intégrité de la chaîne d'approvisionnement numérique. On peut également rappeler qu'il est apparu important pour les États participant à ces négociations de s'engager, hors contexte d'opérations militaires, à ne pas endommager des infrastructures critiques d'un autre État ou à détériorer leur capacité à fournir leur service au public.

À l'occasion du dernier cycle de négociations du GGE 2016-2017, la France a fait des propositions à ses partenaires pour approfondir ce travail et préciser l'ensemble de ces normes, notamment sur l'interdiction des pratiques de *hack back* (contre-attaque cyber) par des acteurs privés ou encore l'imposition d'un contrôle des exportations pour les outils cyber malveillants. Ces propositions ont dans l'ensemble fait l'objet d'un consensus, mais les négociations ont échoué sur la question – dé-corrélée – des modalités d'application du droit international à la conduite des États dans le cyberespace.

Cet échec des négociations au sein du GGE de l'ONU est le signe d'une divergence fondamentale de perception, parmi les différents pays, de l'architecture internationale de sécurité devant régir les relations entre États à l'ère numérique. À court et moyen terme, cette incompatibilité signe l'arrêt des négociations à l'ONU sur le comportement responsable des États dans le cyberespace.

L'échec de ce dernier cycle de négociations ne remet nullement en cause les normes et principes agréés au cours des années précédentes. De plus, il ne doit pas mettre un terme aux efforts de la France et de la communauté internationale en vue de promouvoir des normes de comportement et

mesures de confiance en faveur de la stabilité et de la sécurité internationale du cyberespace.

Au-delà des seules relations entre États, un important effort de régulation reste notamment à mener autour des activités du secteur privé. L'irruption du numérique comme nouvel outil et espace de confrontation confère en effet à ce secteur, et particulièrement à certains acteurs systémiques, un rôle et des responsabilités inédites dans la préservation de la paix et de la sécurité internationale.

Sur ces différents sujets, les États ne seront pas en mesure de créer et d'imposer seuls des règles à tous les acteurs du cyberespace. Ces dernières années, plusieurs initiatives visant à promouvoir certaines visions de la régulation internationale du cyberespace, selon une approche holistique intégrant des acteurs du secteur privé et de la société civile ont d'ailleurs vu le jour.

Lancée en février 2017 par le ministre des affaires étrangères des Pays-Bas, la Commission globale sur la stabilité du cyberespace (Global Commission on the stability of cyberspace) a pour objectif de développer des propositions originales en matière de normes internationales, dans le but d'encourager un comportement responsable des acteurs étatiques et non-étatiques dans le cyberespace. La Commission est composée de vingt-six commissaires (dont un commissaire français) représentant une large variété de régions géographiques et de parties prenantes (gouvernements, industrie, communauté technique, société civile) et choisis en fonction de leur légitimité à s'exprimer sur les différents aspects du cyberespace. Lors de la Conférence globale sur le cyberespace tenue à New Delhi en novembre 2017, cette Commission a appelé États et acteurs non-étatiques à s'engager à protéger le « cœur public de l'internet ».

Par ailleurs, des entreprises privées entendent aussi peser dans ces débats. *MICROSOFT* a ainsi, dès 2014, proposé aux États un ensemble de normes de comportement relatives aux différents aspects de la sécurité internationale du cyberespace (lutte contre la prolifération, gestion responsable des vulnérabilités, assistance en cas de crise) avant de proposer en 2016 que ces normes soient reprises dans une « Convention de Genève du numérique ». *MICROSOFT* est également à l'origine d'un ensemble de règles de comportement à destination du secteur privé (le *TechAccord*).

1.5.2 Des fondements théoriques en construction

Dans ce monde « post - GGE » dans lequel nous vivons désormais, où la paix et la sécurité internationales de la société numérique sont encore en construction, et les rôles respectifs que doivent y jouer les États et les acteurs privés encore à définir, les fondements théoriques de la cyberdéfense sont encore, au sein des pays comme au sein de différentes organisations internationales, en discussion. Plusieurs grandes tendances se dégagent cependant.

La classification des menaces et la gravité des attaques informatiques apparaît, tout d'abord, comme une nécessité partagée. Les États-Unis ont élaboré une grille d'appréhension des cyberattaques qui, si elle ne peut être transposée sans adaptation à l'ensemble des pays au regard des spécificités des organisations de leur cyberdéfense, constitue une référence intéressante.

Par ailleurs, des avancées technologiques remettent en cause certaines des prérogatives régaliennes. L'extraterritorialité des données appelle également la structuration de fondations théoriques nouvelles.

Enfin, la question de l'application du concept de dissuasion au cyberespace continue à faire l'objet de nombreux débats au niveau international. La France réserve, quant à elle, le terme de dissuasion au domaine nucléaire militaire. Garantie ultime de notre souveraineté, la dissuasion se fonde sur la nature unique de l'arme nucléaire. L'arme cyber ne saurait exercer l'effet de retenue ou de dissuasion très spécifique constaté et entretenu avec la dissuasion nucléaire en raison de ses effets profondément différents. Enfin, la « grammaire » de la dissuasion nucléaire est singulière et ne s'applique pas aux actions cybernétiques.

Le concept de « cyber-dissuasion » avancé par certains emporte au moins trois limites :

– tout d'abord, tout acte de dissuasion est fondé sur une rhétorique claire et crédible. Or, en matière de cyber, dévoiler publiquement ses capacités revient à compromettre leur efficacité dans la mesure où cela peut conduire l'adversaire potentiel à prendre les mesures nécessaires pour nier toute possibilité d'attaque cyber. La « cyber dissuasion » ne peut donc avoir une efficacité absolue, car les armes sur lesquelles elle s'appuie peuvent rapidement s'avérer inefficaces si des contre-mesures sont déployées ;

– deuxième limite, les armes cyber n'exercent pas le même effet dissuasif que les armes nucléaires, ces dernières ayant la capacité unique d'infliger des dommages absolument inacceptables, hors de proportions avec le bénéfice de l'agression. Il s'agit d'une arme d'une autre nature, sans continuité avec les moyens conventionnels et cyber. L'équation est donc forcément différente pour la menace de l'emploi d'une arme cyber ;

– la dissuasion nucléaire repose, enfin, sur un dialogue dissuasif entre États dotés. Elle demeure aujourd'hui une composante essentielle de la sécurité et de la stabilité internationale, notamment dans la zone euro-atlantique. La situation est différente avec les armes cyber dans la mesure où celles-ci peuvent être produites et surtout utilisées – pour les moins sophistiquées d'entre elles – assez facilement par un grand nombre d'acteurs, étatiques ou non. Par conséquent, les armes cyber ne sont pas en mesure de susciter des équilibres stratégiques pourvoyeurs de stabilité dans la zone euro-atlantique.

La vocation de dissuasion dans le cyberespace utilisée par nos partenaires britannique et américain désigne en réalité un concept différent du nôtre : il s'agit, par une combinaison de mesures défensives, de résilience et de riposte (pas nécessairement cyber) de « dissuader » (au sens américain) un adversaire. C'est la reproduction dans le domaine cyber d'un débat stratégique qui dure depuis 60 ans et qui nous a notamment déjà opposés sur les notions de « dissuasion conventionnelle » ou de « dissuasion par déni ».

Il est en revanche possible, notamment à l'OTAN, de gérer ces divergences doctrinales anciennes. Le *Cyber Defence Pledge*, la reconnaissance de cyberespace comme domaine d'opérations, la politique de protection des infrastructures cyber de l'Alliance constituent des messages qui visent à décourager l'adversaire et contribuent, à ce titre, à renforcer la posture globale de dissuasion et de défense de l'Alliance. Une forme de découragement des velléités d'agressions contre des membres de l'OTAN dans le cyberespace est donc possible et acceptable.

1.6 Les différents modèles d'organisation de cyberdéfense dans le monde

1.6.1 Dans le domaine cyber, les puissances sont nombreuses et bien identifiées

Une dizaine d'acteurs particulièrement puissants en matière de cyberdéfense dominent la scène internationale : la communauté dite des « *Five eyes* », qui regroupe les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande, du nom de l'alliance qui réunit les services de renseignement technique de ces pays depuis la Seconde guerre mondiale, la Russie, la Chine, Israël, l'Allemagne et la France.

Engagé depuis le début des années 2000, l'effort français en matière de cyberdéfense s'inscrit dans une dynamique de développement capacitaire et de réflexion stratégique que l'on retrouve dans les pays anglo-américains (États-Unis et Royaume-Uni), en Allemagne, comme en Russie, en Chine et en Israël.

Les stratégies de cyberdéfense de ces pays reposent toutefois sur des modèles distincts (avec d'une part un modèle regroupant au sein des agences de renseignement les aspects défensifs et offensifs et,

d'autre part, un modèle séparant distinctement ces deux aspects), ainsi que sur des visions du cyberespace opposées (les visions russe et chinoise apparaissant comme fondamentalement différentes de la vision occidentale).

Par ailleurs, si l'effort capacitaire est partagé, les moyens humains et financiers mobilisés par ces différents pays s'inscrivent dans des ordres de grandeur hétérogènes. De plus certains pays ont adopté ou vont adopter des politiques de protectionnisme notamment pour maîtriser totalement l sécurisation de leurs réseaux.

Le cyber, une priorité stratégique partagée par les États-Unis, le Royaume-Uni, l'Allemagne, la Russie, la Chine et Israël

Leader incontesté dans le domaine de la cyberdéfense, les États-Unis ont pris conscience avec un temps d'avance sur les autres puissances mondiales, dès la fin des années 1990, des risques pesant sur leurs systèmes d'information et de communication et leurs infrastructures. Un décret présidentiel sur la protection de l'infrastructure critique est signé en 1998, et le *Department of Homeland Security* est créé en 2001 pour protéger les réseaux étatiques. Héritage d'une attention portée de longue date au renseignement technique, les États-Unis accordent une priorité stratégique à la cyberdéfense. […] Le modèle de cyberdéfense américain se distingue du modèle français, fondé sur la séparation des capacités offensives et défensives. Les capacités de cyberdéfense américains sont en effet largement concentrées au sein de la communauté du renseignement. Ce modèle, s'il a l'avantage de permettre une mutualisation des compétences techniques nationales au sein du pôle d'expertise que constitue la NSA, présente néanmoins des inconvénients. Il pose en effet la problématique de l'acceptabilité par le secteur privé des interventions de l'État en matière de sécurité des systèmes d'information, dans un contexte marqué par les révélation d'Edward SNOWDEN, qui ont mis en lumière l'ampleur des renseignements techniques qui auraient été collectés par la NSA.

Le modèle britannique est proche du modèle américain. Le Royaume-Uni a adopté une stratégie nationale en matière de sécurité de l'information dès 2003 ; cette première stratégie mettant l'accent sur le partenariat entre les secteurs publics et privés au sein du *National Infrastructure Security Coordination Center*, afin notamment d'assurer la sécurité des réseaux et des systèmes informatisés de contrôles industriels. Le Royaume-Uni a présenté sa nouvelle *National Cyber Security Strategy* en novembre 2016. Elle constitue le nouveau cadre d'action du gouvernement britannique pour la période 2016 – 2021. L'objectif est que le Royaume-Uni puisse, à l'horizon 2021, être en situation d'être « sûr et résilient face aux menaces cyber afin de se montrer prospère et confiant dans le monde numérique ».

C'est en 2011 que le gouvernement fédéral allemand a adopté sa première stratégie nationale de cybersécurité. Sa version actualisée en 2016 traduit une vision du cyberespace très proche de celle de la France. Paris et Berlin partagent des orientations stratégiques communes sur de nombreux sujets techniques, tels que la cryptographie ou la certification des produits de sécurité, mais également politiques, comme la promotion de l'Union européenne résolue et dynamique en matière de sécurité numérique. Cette proximité fait de l'Allemagne un partenaire privilégié de la France au sein des diverses enceintes internationales traitant de ces sujets, et confère au couple franco-allemand un rôle d'impulsion majeur dans les projets européens relatifs à la sécurité des systèmes d'information.

C'est en 2006 que le *Plan de développement national pour les sciences et les technologies* du gouvernement chinois mentionne pour la première fois les enjeux de sécurité des systèmes d'information critiques. La cyberdéfense est élevée au rang de priorité absolue en 2014, avec la création du *Groupe dirigeant restreint pour la sécurité des réseaux centraux et l'informatisation*,

organe stratégique rassemblant les plus grands décideurs politiques du pays. Le président XI JINPING a alors choisi d'assurer personnellement la présidence de ce *Groupe dirigeant restreint*, envoyant un signal fort au pays mais également à l'ensemble de la communauté internationale. Une place prépondérante est accordée à la cybersécurité dans le Livre blanc chinois, adopté en mai 2015. Il constitue une première reconnaissance publique de l'existence de capacités cyber-offensives et introduit une doctrine de *défense active*, assurant d'une réponse potentiellement militarisée, de nature cyber ou non, à toute action jugée contraire aux intérêts de Pékin. En décembre 2016, dans le prolongement de ce Livre blanc, la Chine publie pour la première fois une stratégie nationale de cybersécurité, qui appelle à rechercher « la paix, la sécurité, l'ouverture, la coopération, et l'ordre dans le cyberespace » et affirme son ambition de devenir une « superpuissance cyber ». Le cyberespace est considéré par les autorités chinoises à la fois comme un lieu et un moyen de développement économique et de contrôle de l'opinion. L'approche chinoise de cyberespace se distingue nettement de l'approche occidentale dans la mesure où elle confère à l'État une mission de « sécurité de l'information », qui s'étend bien au-delà de la « sécurité des systèmes d'information ». Cette vision, que la Chine partage avec la Russie, est héritée du fort attachement des régimes de ces pays au contrôle étatique de l'information : l'État ne doit pas uniquement assurer l'intégrité de ses réseaux mais également contrôler le contenu des informations qui y transitent. Cette approche est en opposition fondamentale avec la conception occidentale du cyberespace.

Dès son arrivée au pouvoir, Vladimir POUTINE a montré son intérêt pour le cyberespace. Il dote en 2000 la Russie de sa première doctrine de *sécurité informationnelle*, qui décrit la sécurité de l'information comme une composante essentielle de la sécurité de l'État. La doctrine russe s'est étoffée dans les années 2010 avec la publication de la doctrine militaire de la Fédération de Russie de 2010, les *Points de vue conceptuels sur les activités des Forces armées dans l'espace informationnel* de 2012. La Russie se distingue nettement de la plupart des grandes puissances occidentales dans sa conception du cyberespace. Marquée par une préoccupation de contrôle de l'information héritée de la période soviétique, la vision russe ne se limite pas aux systèmes d'information mais s'étend à l'ensemble de la sphère informationnelle. Par opposition aux doctrines cyber des États occidentaux, centrées sur la protection des contenants, la doctrine russe, tout comme la doctrine chinoise, s'intéresse avant tout au contenu. Cette perception s'incarne dans le concept de *défense informationnelle*, qui constitue un pilier de la doctrine russe. Moscou place ainsi les activités d'influence, en particulier dans leur dimension psychologique, au cœur de sa cyberstratégie. Les médias y sont pleinement intégrés en tant que forces de *contre-propagande*, et de nombreuses agences de « *trolling* » rémunèrent des internautes pour relayer massivement des messages pro-russes sur les réseaux sociaux. L'organisation de la cyberdéfense russe repose sur des capacités dans ce domaine largement concentrées au sein de la communauté du renseignement.

Israël, enfin, est aujourd'hui en pointe en matière de cyberdéfense, grâce à un dispositif gouvernemental performant en lien avec l'armée, le monde universitaire et l'industrie. La stratégie israélienne n'a pas encore fait l'objet d'un document officiel.

Des efforts capacitaires asymétriques

L'analyse de ces organisations révèle un développement capacitaire hétérogène, sur les plans humain et financier, des pays pouvant être considérés comme les principales puissances cyber.

Le budget des États-Unis dans le domaine de la cyberdéfense s'est élevé à 14 milliards de dollars en 2016 […]. En 2016, le *Department of Homeland Security* (DHS) comptait 691 agents dans le secteur de la cybersécurité et a réalisé 818 millions de dollars d'investissements dans ce domaine, soit 2 % de son budget total. Pour sa part, l'US-CERT dispose d'un budget de 98 millions de dollars pour 203 agents. Enfin, si le budget affecté à la NSA est une information classifiée, il est estimé proche de 10 milliards de dollars et ses effectifs supérieurs à 30 000 agents.

La nouvelle *National Cyber Security Strategy* du Royaume-Uni, présentée en novembre 2016, prévoit un investissement budgétaire de £1,9 milliards sur les cinq ans à venir.

Les ressources et le budget du ministère de l'intérieur allemand affectés à la cybersécurité ne sont pas connus avec précision, le BSI emploie quant à lui plus de 700 agents, auxquels devraient s'ajouter 100 nouvelles recrues d'ici fin 2018.

Les capacités cyber-offensives chinoises, dont le périmètre exact demeure difficile à évaluer, se concentrent principalement au sein de l'*Armée Populaire de Libération*, qui constitue le fer de lance des actions d'espionnage politique et économique visant l'étranger. Cette dernière fait actuellement l'objet d'une importante réforme, dont un des objectifs est la mutualisation des ressources d'attaque et de défense au sein de l'armée.

1.6.2 Des puissances de taille modeste capables de déployer des capacités offensives avancées

Si ces quelques pays se sont positionnés assez tôt sur le sujet, il serait très surprenant que d'autres pays n'aient pas déjà investi fortement dans des capacités offensives. En effet, la divulgation des outils américains et les outils de hacking disponibles sur des marchés plus ou moins officiels peuvent permettre à des États, même de taille modeste, de construire des capacités offensives pour peu qu'ils disposent d'une main d'œuvre compétente. Aussi, des pays comme la Corée du Nord, le Pakistan et l'Iran ou bien encore le Japon, la Corée du Sud et l'Inde, comme de nombreux pays européens, ont déjà des capacités, même s'il est difficile de les évaluer.

DOCUMENT 3

« Cybermenace : avis de tempête »

Institut Montaigne, rapport novembre 2018 - extraits

PROPOSITIONS POUR AUGMENTER LA CYBERRÉSILIENCE DU TISSU ÉCONOMIQUE FRANÇAIS

Si le numérique apparaît aujourd'hui comme un catalyseur de l'innovation et du progrès, il est toutefois nécessaire que tous les acteurs concernés prennent la mesure des risques inhérents au cyberespace pour être en mesure de prévenir et contenir les effets systémiques pouvant découler d'une cyberattaque destructrice d'ampleur. Le chapitre suivant expose les propositions de ce rapport pour augmenter la cyberrésilience du tissu économique français face à des scénarios de type « cyber ouragan ».

Menées entre mars et octobre 2018, les auditions et les travaux du groupe de travail ont permis d'identifier trois enjeux majeurs pour atteindre cet objectif :

• mobiliser l'ensemble du tissu économique pour anticiper un cyber ouragan ;

• démultiplier les compétences et être solidaire en cas de crise majeure ;

• pouvoir répondre à des attaques larges et rapides de manière efficace.

Les recommandations du groupe de travail ont donc été axées autour de ces trois piliers.

Mobiliser l'ensemble du tissu économique

Pour les entreprises cotées d'une certaine taille :

1. Encourager la rédaction d'un rapport sur les risques cyber à disposition des administrateurs, voire une intégration partielle dans les rapports annuels.

Constat :

Les entreprises du CAC 40 ont beaucoup communiqué ces dernières années sur leurs plans de transformation numérique. [...]

Ce constat est toutefois à nuancer. 25 % des groupes du CAC 40 uniquement abordent directement la problématique de la cybersécurité au niveau des comités exécutifs. Les investissements réalisés et les plans d'actions mis en œuvre pour couvrir ces risques sont encore peu mentionnés par les groupes français. Les investissements restent morcelés et à des niveaux hétérogènes : seules 12,5 % des entreprises du CAC 40 annoncent avoir lancé un programme de cybersécurité contre 75 % qui ne mentionnent que des plans d'action unitaire morcelés. Plus surprenant, seulement 58 % des entreprises du CAC 40 faisaient mention du RGPD dans leurs documents de référence en 2017.

Recommandation :

Le manque de communication au plus haut niveau en matière de cybersécurité est à la fois le témoin du manque de sensibilisation des équipes dirigeantes et la marque du manque d'intégration de la

cybersécurité à la stratégie d'entreprise.

Pour répondre à ces carences, nous proposons d'encourager la rédaction d'un rapport sur les risques cyber à disposition des administrateurs et d'intégrer partiellement ces risques et les contre-mesures au rapport annuel.

Cette proposition vise deux objectifs :

• Le premier est de sensibiliser les dirigeants à l'étendue de leurs risques cyber. La documentation destinée aux administrateurs est bien sûr suivie attentivement par la direction générale ; y inclure un résumé des risques cyber de l'entreprise et les actions prévues pour y répondre assurerait donc une implication accrue de toute l'équipe dirigeante.

• Le second est d'obtenir la validation par les administrateurs, dont c'est l'une des missions, de la stratégie de l'entreprise pour répondre à ces risques.

Ce document pourra inclure des volets sur les sujets de : la menace contextualisée à l'entreprise ; l'implication des instances dirigeantes ; la gouvernance de la cybersécurité et les plans d'action de couverture des risques ou programmes de cybersécurité ; l'intégration de la cybersécurité dans la stratégie numérique ; la protection des données personnelles ; la cyberassurance ; la sensibilisation...

Ce rapport, non public, serait seulement destiné aux administrateurs de manière à éviter toute exploitation par des acteurs mal intentionnés et pour éviter de porter atteinte à l'attractivité de l'entreprise. En cas de publication intégrée dans le rapport annuel, le volet sur les risques cyber pourrait exposer les incidents répertoriés plutôt que le détail des risques qui doit rester à la discrétion de l'entreprise.

Pour les ETI/PME/TPE :

2. Mobiliser les réseaux des métiers du chiffre (experts-comptables et commissaires aux comptes) pour réaliser un diagnostic cybersécurité annuel avec un cahier des charges minimum (construit avec les autorités nationales). Il serait communiqué aux dirigeants à titre d'information avec les recommandations de base pour couvrir les risques.

Constat :

L'institut de recherche technologique SystemX évalue à 50 000 le nombre de PME victimes d'une cyberattaque en 2017 avec des dégâts financiers significatifs pour leur trésorerie. Trop peu sensibilisées au risque cyber, des attaques courantes comme le rançongiciel ou les fraudes au président ont touché de nombreuses PME l'année dernière.

Face à cela, leur niveau d'investissement en matière de cybersécurité reste décevant : un premier indicateur de ce manque d'investissement est leur faible recours aux offres d'assurance cyber. Évidentes quand il s'agit du risque d'incendie ou de vol, elles le sont beaucoup moins en matière de cybersécurité. L'audition réalisée par l'Institut Montaigne auprès d'une responsable cyber dans une grande société d'assurance nous apprend ainsi que si 100 % des entreprises du CAC 40 ont souscrit des assurances cyber (elles étaient 80 % en 2016 avant les attaques Wannacry et NotPetya), seulement 30 % des ETI en France sont couvertes. Ce taux est encore plus faible pour les TPE/PME, signe de la sensibilisation qu'il reste encore à faire.

Or, les PME sont régulièrement les cibles d'attaques, notamment car ce sont des points d'entrée privilégiés des attaquants dans la chaîne d'approvisionnement des grands groupes. [...]

Recommandation :

Notre proposition s'appuie sur un constat simple : l'individu auquel le chef d'entreprise pense naturellement quand il s'agit d'évaluer ses risques, qu'ils soient financiers ou d'une autre nature est l'expert-comptable ou le commissaire aux comptes. Ces métiers du chiffre sont très bien connectés aux PME et se positionnent comme des tiers de confiance pour l'entreprise et son environnement. D'après un expert auditionné par l'Institut Montaigne, le nombre d'entreprises touchées par ces professions s'élève à 2 150 000 (2 000 000 pour les experts comptables et 150 000 pour les commissaires aux comptes).

Nous proposons donc de les mobiliser pour intégrer des diagnostics cybersécurité et rendre ces diagnostics obligatoires dans un second temps. Ces évaluations pourraient reposer sur un document préétabli en partenariat avec des experts en matière de cybersécurité. Des recommandations seraient alors adressées, sous forme informatives, par l'expert-comptable ou le commissaire aux comptes, pour poser les fondements d'un plan de réponse.

Au-delà d'alerter et de sensibiliser les chefs d'entreprise sur le sujet, cette recommandation pourrait, dans un temps plus long, participer à mettre en place un dispositif vertueux via un système de notation (profil de risque A/B/C/D...). Par exemple, la notation Banque de France permet d'apprécier la situation financière des entreprises par rapport à un ensemble de règles méthodologiques et communes : les chefs d'entreprise sont naturellement incités à rechercher une note maximale pour rassurer leurs investisseurs sur leur capacité à respecter les engagements et de résistance face aux évolutions de l'environnement. La notation cyber issue de l'évaluation par les experts-comptables et les commissaires aux comptes pourrait, par exemple, servir aux cyberassureurs : les chefs d'entreprise pourraient alors être incités à rechercher une note élevée pour bénéficier de bonus sur leur prime de cyberassurance.

3. Inciter et mobiliser les grands groupes sur leur responsabilité pour augmenter le niveau de cybersécurité de leur chaîne d'approvisionnement et de leurs fournisseurs.

Constat :

Pour rendre plus efficace leur logistique, la plupart des grands groupes ont fortement intégré leurs procédures et leurs systèmes avec ceux de leurs fournisseurs : il existe par exemple des systèmes de suivi des stocks partagés ; de nouvelles commandes peuvent ainsi être directement envoyées au sous-traitant en cas de besoin.

La chaîne d'approvisionnement des grands groupes intègre donc de plus en plus de systèmes numériques. Cette interconnexion, si elle facilite la production, introduit bien sûr de nouveaux risques cyber. Il peut maintenant suffire aux cybercriminels d'attaquer un fournisseur de taille moyenne pour avoir accès aux données de plusieurs entreprises, voire du groupe directement. Dans certains cas, ils peuvent également interrompre le fonctionnement des services des entreprises.

Les liens numériques entre entreprises d'une même chaîne d'approvisionnement sont donc le reflet d'une nouvelle chaîne de risques, dans laquelle l'élément le plus faible peut mettre en danger l'ensemble du groupe. [...]

Recommandation :

Nous proposons donc que les grands groupes forment et sensibilisent les petites entreprises et les fournisseurs dont ils dépendent à la cybersécurité, en rendant disponible une partie de leurs experts.

La multiplication de ces échanges pourrait se matérialiser au sein de « centres d'accélération » tel que préconisé dans le rapport de l'Institut Montaigne « Industrie du futur, prêts, partez ! », mesure reprise par Edouard Philippe dans son plan pour transformer l'industrie par le numérique.

4. Inciter à la création et à la souscription d'offres cybersécurité pour les TPE/PME/ETI, en particulier des offres de connectivité réseau intégrant par défaut des mesures de sécurité de base (nettoyage du trafic), des offres d'applications métier (ex. ERP) sécurisées par défaut et des offres de cyberassurance, incluant des services en cas d'incidents.

Constat :

Les PME et ETI, a fortiori les TPE, n'ont pas accès aux mêmes compétences en cybersécurité que les grands groupes. Ainsi, l'existence de solutions sur étagère destinées aux TPE/PME/ETI de manière à ne pas avoir besoin de développer ou acquérir de nombreuses compétences en cybersécurité est crucial.

D'autres pays ont déjà lancé cette démarche : le Centre national de cybersécurité britannique (NCSC), à travers son programme active cyber defense, et la ville de New York, par le biais de la startup Quad9, fournissent respectivement des services de sécurisation de sites web et du réseau Internet gratuitement pour certains usages. Pour ce faire, les opérateurs et les fournisseurs de service doivent être mobilisés. [...]

Recommandation :

Pour répondre au besoin des PME/TPE/ETI, il faut donc favoriser la création d'offres sur étagère, simples, transparentes et ne requérant pas de compétences fortes.

Il n'est pas nécessaire que toutes ces mesures soient à l'initiative de l'État. Certaines initiatives pourront être lancées dans le cadre d'un travail en commun entre l'État et les opérateurs, mais il semble nécessaire que le développement de ces offres intégrant la sécurité par défaut soit une évolution naturelle des services des fournisseurs de manière à développer ou maintenir un avantage concurrentiel. L'alternative coercitive, qui imposerait cette évolution par la réglementation, ne saurait se justifier ici et pourrait être contre-productive. [...]

L'État peut en revanche rendre plus visible ces offres de cybersécurité en les structurant par la labellisation (les Visas de sécurité ont vu le jour en France et l'action est en cours au niveau européen) ou par le lancement d'appels d'offres de l'État sur des services sécurisés.

Pour les secteurs critiques

5. Faire évoluer le corpus réglementaire, en particulier les textes liés à la loi de programmation militaire (LPM) 2014-2019, pour y ajouter des exigences précises de cyberrésilience (réalisation annuelle d'un exercice de crise, existence d'un système d'information de crise indépendant du système d'information nominal, introduction de diversité technologique sur les systèmes d'information d'importance vitale, etc.).

Constat :

L'article 22 de la loi de programmation militaire (LPM) de 2014 -2019 et la transposition de la directive Network and Information Security (NIS) en droit français apportent déjà beaucoup d'éléments sur la protection des infrastructures d'importance vitale et de services essentiels. En particulier, la LPM 2018 permet désormais aux opérateurs télécoms de mettre en oeuvre des mesures de détection d'activités malveillantes sur leurs réseaux. Ces mesures, ciblant initialement les opérateurs d'importance vitale (OIV) sont élargies aux opérateurs de services essentiels (OSE).

Recommandation :

Nous proposons de faire évoluer le corpus réglementaire, en particulier les arrêtés sectoriels fixant les règles relatives à la sécurité des systèmes d'information des OIV prévues par l'article 22 de la LPM 2014 et des OSE, pour y introduire des exigences de cyberrésilience ; les règles suivantes pourraient être rendues obligatoires :

• réalisation annuelle d'un exercice de crise cyber ;

• existence d'un système d'information de crise indépendant du SI nominal ;

• mise à disposition de capacités de reconstruction après un sinistre majeur.

Et pour des secteurs ciblés, il pourrait être demandé l'introduction d'une diversité technologique sur les SI d'importance vitale.

Démultiplier les compétences et être solidaire en cas de crise

6. Créer un parcours de formation financé par l'État en contrepartie d'un engagement dans la réserve de cyberdéfense pour un nombre minimum d'années afin de réaliser un appui opérationnel en cas de crise et de maintenir les compétences (entraînement, action de prévention…).

Constat :

Les nombreuses cyberattaques de ces dernières années en sont le témoin : le niveau général de la menace augmente et les organisations peinent à combler le retard en matière de sécurisation des systèmes alors même que l'innovation suit son cours et que de nouvelles solutions technologiques voient le jour. Le marché de la cybersécurité est ainsi aujourd'hui en forte croissance.

Mais cette activité connaît aujourd'hui une limite majeure : la disponibilité de professionnels compétents dans le domaine. Le recrutement d'ingénieurs et techniciens formés à la cybersécurité est donc un facteur limitant de la montée en régime du marché français et international.

Face à ce constat, l'ANSSI a lancé un programme de labellisation nommé SecNumEdu qui vise à qualifier les formations initiales en cybersécurité de l'enseignement supérieur pour apporter une assurance aux étudiants et employeurs concernés que la formation répond aux critères retenus par l'ANSSI avec les acteurs du domaine.

Les écoles et organismes de formation réagissent également avec l'apparition de nouvelles formations à tous les niveaux, notamment avec la création de nombreux masters spécialisés. Parallèlement, le recrutement de profils différents, plus expérimentés ou issus d'autres métiers, pour combler ces carences est une alternative suivie avec attention. La bonne transition de ces profils suppose donc une formation de qualité… Or, le coût des études longues (Bac + 5) ou de formations de reconversion constituent une barrière financière.

Recommandation :

Nous proposons la création d'un parcours de formation, incitatif, financé par l'État. Cet appui de la puissance publique exigerait un engagement de l'étudiant pour un nombre minimal d'années auprès de l'État. La réserve de cyberdéfense, rattachée au commandement de cyberdéfense, et constituée de 400 réservistes opérationnels, pourrait ainsi bénéficier de leur soutien en cas d'attaque d'envergure. L'une de leurs missions principales est la restauration des capacités opérationnelles des systèmes impactés. La réserve de cyberdéfense est actuellement en cours de refonte par le COMCYBER et l'ANSSI.

Ces formations pourraient être assurées dans des écoles disposant de cursus spécialisés ou dans les centres de formation de l'ANSSI (en identifiant des moyens spécifiques à sa montée en puissance).

Toutefois, la contrepartie ne doit pas se limiter à des sujets de cyberdéfense mais aussi s'ouvrir à des sujets civils, de manière à mobiliser les diplômés dans le temps en dehors de situation de crise (pour des formations, des actions de prévention ou de sensibilisation). Les réservistes pourraient à ce titre constituer un tissu de formateurs capables d'intervenir dans ces circuits de formation.

7. Étendre le rôle de la réserve de cyberdéfense à la résolution de crises touchant les acteurs privés et augmenter le nombre et les compétences des réservistes en en faisant la promotion auprès des acteurs du secteur privé et de la recherche académique.

Constat :

Plusieurs réserves destinées au risque cyber ont été créées récemment. En mars 2018, le réseau de référents cybermenace de la Police Nationale a vu le jour. Rattaché à la sous-direction de la lutte contre la cybercriminalité (SDLC), il vise à sensibiliser les acteurs privés partenaires et à les alerter en cas de cyberattaque. De son côté, la réserve opérationnelle de cyberdéfense, lancée en mai 2016, est un réservoir de forces mobilisables en cas de crise majeure sur le territoire national. Elle comprendra 4 440 personnes en 2019, dont 40 postes permanents et 400 réservistes opérationnels composant le coeur du dispositif (dont 200 en région et outre-mer). Cette réserve a pour vocation d'intervenir principalement non seulement sur les réseaux du ministère de la Défense mais également au profit des OIV (opérateurs d'importance vitale), des administrations et de leurs sous-traitants. Elle a par exemple récemment été mobilisée dans le cadre de l'exercice interarmées de cyberdéfense (DEFNET). D'autre part, 4 000 réservistes citoyens sont mobilisables sur l'ensemble du territoire national.

Recommandation :

Inclure les chercheurs volontaires au sein de la réserve de cyberdéfense aurait le double avantage de répondre au besoin humain grandissant de la réserve, et de nouer des collaborations entre la recherche académique et l'ensemble de l'écosystème cybersécurité (institutionnels, DGA, ANSSI…). Il faut donc communiquer directement auprès du monde académique pour mettre davantage en lumière la réserve de cyberdéfense.

Leur intégration ne nécessite d'ailleurs pas de statut particulier : leur entrée dans la réserve doit rester sur la base d'un volontariat. Une formation en amont serait un prérequis pour être opérationnel en cas de mobilisation. Dans cette hypothèse, les chercheurs peuvent être mobilisés en cas d'urgence, mais ils peuvent aussi être mis à contribution sur des aspects de recherche pour constituer des scénarios d'attaque et préparer la réaction. L'INRIA s'est ainsi dotée de laboratoires à

haute sécurité informatique (LHS) à Nantes et Rennes afin d'accueillir des travaux de recherche destinés à sécuriser le réseau.

Au-delà du monde académique, nous proposons que des employés du secteur privé puissent eux aussi rejoindre plus généralement la réserve de cyberdéfense. Ceci suppose un soutien et un aménagement minimal de leurs ressources humaines et une communication accrue dans les entreprises. Mais les avantages sont nombreux : à la fois pour la réserve, qui bénéficierait de nouvelles passerelles avec les acteurs privés, d'ingénieurs et techniciens rompus à la gestion cyber en entreprise, mais aussi pour les entreprises. Celles-ci profiteraient de formations aux modes d'action et de planification valables en cas de crise pour des opérations militaires, et transposables au secteur privé.

Au-delà du défi de la montée en capacité des compétences cyber, cette recommandation vise aussi à étendre le périmètre d'intervention de la réserve de cyberdéfense à la résolution de crise touchant les acteurs privés. Dans le cas très précis d'un « cyber ouragan » incapacitant des pans entiers de l'économie française, la réserve de cyberdéfense pourrait constituer un vivier de compétences pour déployer les actions de résolution de crise sur le territoire national. Agissant en tant qu'intermédiaire et organe coordonnateur, l'ANSSI pourrait occuper un rôle de passerelle entre le monde de la cyberdéfense et celui des entreprises privées en cas de crise d'ampleur.

8. Proposer un cadre permettant aux acteurs privés de partager le personnel et leurs compétences avec leurs pairs en cas d'attaque.

Constat :

S'il existe aujourd'hui un manque de compétences cyber, celui-ci va s'amplifier dans les prochaines années. Les grands groupes, confrontés à de graves attaques l'année passée, ont déjà pu faire l'expérience des limites actuelles de leur effectif et des prestataires compétents lorsqu'une attaque généralisée se propage. [...]

La comparaison entre les ouragans cyber auxquels les entreprises seront de plus en plus confrontées et les états de catastrophe naturelle est ici légitime : lorsque la tempête Xynthia a touché l'Ouest de la France, des circuits de solidarité se sont naturellement mis en place pour répondre ponctuellement à la crise. Des entreprises, certaines ayant des missions de service public, ont mis à disposition une partie de leurs ressources.

Recommandation :

Nous proposons donc de mener ce changement de paradigme en mettant en place un cadre permettant aux acteurs privés de partager leur personnel en cas de grave attaque cyber, ingérable par leurs seules ressources.

Pour permettre une telle intervention, les conventions de mise à disposition et les dispositifs de détachement semblent être les plus appropriés. Contrairement au contrat de prestation, ceux-ci permettent le transfert de compétences vers une entreprise disposant déjà de la compétence requise, mais en quantité insuffisante, comme ce serait le cas lors d'une attaque majeure. [...]

La mise en œuvre de tels dispositifs s'anticipe : il faut définir une « force d'intervention rapide » préparée lors d'exercices de simulation afin de clarifier le partage des responsabilités et la chaîne de commandement. Ces passerelles, préparées et répétées, tracent le chemin pour des circuits de solidarité bien définis lorsqu'une crise cyber affectera ces entreprises. Il faut également rédiger ces

contrats en amont. Deux options existent :

• un contrat tripartite, entre les deux entreprises et l'employé volontaire, à signer lorsque la crise survient ;

• une convention entre les deux entreprises, complétée d'un avenant entre la société mettant ses compétences à disposition et son employé.

Le principal enjeu de cette proposition réside donc plus dans le changement de posture qu'elle suppose que sur des difficultés juridiques, et le défi est de favoriser les conditions d'un environnement de confiance entre acteurs du secteur privé. Afin de sensibiliser les acteurs en amont, une charte pourrait être signée par les entreprises participantes, sur le modèle de la Charte de solidarité en situation d'exception signée entre les acteurs privés et le ministère de l'Intérieur.

9. Renforcer la capacité d'échange opérationnelle de signatures d'attaques et d'informations sur les menaces a minima entre les entreprises stratégiques pour la nation, via une plateforme sécurisée d'échange opérée soit par l'État, soit par un ou des acteurs français majeurs de la cybersécurité et de confiance (avec une possible segmentation sectorielle).

Constat :

Des entreprises ne sont parfois prévenues de l'existence d'une menace que longtemps après le début d'une attaque, entraînant des conséquences potentiellement beaucoup plus importantes pour ces dernières. Des circuits d'échange d'information existent, notamment avec l'État, mais ils ne sont pour l'instant pas suffisamment efficaces et organisés.

Au sein de l'ANSSI, le CERT-FR (« Computer Emergency Response Team ») est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il apporte son soutien aux institutionnels, aux collectivités et aux OIV (« Opérateur d'Importance Vitale ») en matière de gestion de crise.

Certains groupes français ont créé des CERT locaux mobilisant leur écosystème : c'est le cas d'Airbus qui participe activement à un groupe de partage d'informations sensibles prolifique avec Boeing au sein de l'A-ISAC (« Aviation – Information Sharing and Analysis Center ») ou encore de la Société Générale ou de la BNP Paribas dans le monde bancaire.

Recommandation :

Nous proposons donc de renforcer la capacité d'échange opérationnelle de signatures d'attaques et d'informations sur les menaces entre les entreprises françaises stratégiques pour la nation, via une plateforme sécurisée d'échange opérée soit par l'État, soit par un ou des acteurs français majeurs de la cybersécurité et de confiance (avec une segmentation sectorielle). Cette structure pour échanger de l'information comblerait un manque flagrant aujourd'hui. L'ensemble des entreprises consultées s'accordent sur ce constat ; elles ne sont néanmoins pas encore parvenues à structurer cette piste, ne sachant pas si un pilotage par l'État est nécessaire.

Pouvoir répondre à des attaques larges et rapides

10. Mobiliser le tissu économique et l'État autour de l'intelligence artificielle pour détecter les attaques et réagir à la bonne vitesse (et sécuriser l'intelligence artificielle pour prévenir les dérives).

Constat :

Le rapport Villani fait état d'un important retard français dans l'utilisation de l'intelligence artificielle (IA) dans le domaine de la cybersécurité.

Pourtant les systèmes intégrant de l'IA se multiplient et ils ne sont pas toujours conçus pour prendre en compte les tentatives de détournement. Les attaques réussies se multiplient : trois grandes familles d'attaques sont aujourd'hui capables de détourner l'IA.

Les attaques par empoisonnement sont les premières : il s'agit de nourrir l'IA d'échantillons biaisés alors qu'elle est encore en période d'apprentissage pour en orienter les résultats. On peut citer en illustration la malheureuse expérience du chatbot « Tay » de Microsoft : la société avait créé un compte Twitter dont l'ensemble des messages reposait sur des algorithmes d'apprentissage automatique. Celui-ci fut tellement surchargé de messages haineux de la part de comptes malintentionnés qu'il finit par reproduire leur comportement, générant ainsi des messages à connotation raciste.

Les attaques par illusion consistent à alimenter l'IA avec une image biaisée de la réalité sans que cela ne soit détectable à l'œil nu. Les attaques par inférence permettent de solliciter l'IA non pas pour en détourner l'usage mais pour en révéler le fonctionnement interne.

Si l'IA nécessite donc une vigilance particulière, il faut néanmoins noter qu'elle est aussi en capacité d'apporter des solutions pour sécuriser les systèmes et réseaux informatiques. Face à des attaques en mesure de faire tomber des milliers d'entreprises en quelques minutes, l'IA devient nécessaire pour détecter suffisamment tôt ces menaces et y réagir de manière automatique.

Recommandation :

Nous proposons donc de promouvoir l'utilisation de l'IA dans le domaine de la cybersécurité pour détecter les attaques suffisamment vite et rester en mesure de réagir avant que l'attaque ne se propage trop fortement. [...]

Il faut donc accélérer les investissements dans les technologies d'apprentissage automatique associées à la cybersécurité pour être en mesure de répondre à des attaques larges et rapides.

11. Définir une doctrine opérationnelle spécifique à l'échelle de l'État pour faire face à une attaque large (actions opérationnelles pour mobiliser les acteurs de l'écosystème cybersécurité dans le tissu économique privé, anticiper des actions pour isoler le pays d'Internet, pour communiquer auprès du grand public en cas de destruction des moyens de communication classiques, etc.).

Constat :

La définition d'une stratégie de communication et de réponse opérationnelle en cas d'attaque majeure est essentielle : le risque serait d'avoir des canaux d'actions et de communication

strictement limités à l'ANSSI et aux OIV affectés. Mais le grand public ou la multitude d'entreprises touchées feraient également partie des victimes avec qui il faudrait communiquer. Dans cette situation, l'absence d'une stratégie de réponse et de communication solide pourrait mener à des conséquences plus graves en cas de panique générale.

En termes de communication, l'ANSSI participe déjà régulièrement aux exercices de crise du plan PIRANET, plan gouvernemental. Durant ces exercices, les scénarios joués présentent toujours des niveaux d'impacts très forts au niveau national, comme le secteur de l'énergie paralysé, des transports inopérants, des émeutes généralisées… Ces exercices incluent systématiquement des volets de communication vers le grand public. Aussi, le scénario d'une cyberattaque fortement impactante nécessite une communication vers la population. Dans la revue stratégique de cyberdéfense, il est prévu de préparer ces questions dans les différentes instances de l'État à la fois au niveau du message à communiquer et au niveau du canal de communication.

Recommandation :

En cas de crise, la bonne coordination des acteurs locaux, l'endiguement des zones touchées et la communication auprès du public sont autant de volets qui doivent être adressés par l'État dans une doctrine opérationnelle qui permette de faire face à une attaque large.

La première priorité opérationnelle est d'identifier des relais au sein des entreprises qui soient des points privilégiés pour l'État sous toutes ses formes (pour l'ANSSI mais aussi pour les forces de l'ordre par exemple). Dans les grandes entreprises, identifier les RSSI comme acteurs de confiance pour créer un réseau immédiatement mobilisable en cas d'attaque majeure. Dans les petites et moyennes entreprises, un équivalent reste à inventer.

Une fois ces acteurs mobilisés, la deuxième priorité consiste à endiguer la menace. Nous recommandons la mise en place de procédures d'urgence pour isoler un site industriel, une entreprise ou certains territoires du réseau le temps que l'attaque soit contenue. L'existence d'un véritable « bouton rouge » est une solution d'urgence pour activer un fonctionnement en mode dégradé et protéger la population sans disséminer la menace.

Enfin, la communication auprès du grand public, prérogative de l'État, est indispensable en temps de crise pour rassurer la population et éviter la perte de confiance en les institutions, effet parfois spécifiquement recherché par les attaquants. Toujours dans la logique de fonctionnement en mode dégradé, des plans de communication de crise en cas de défaillance des moyens usuels doivent donc être préparés : TV, radio, Internet…

12. Inciter et donner un cadre aux entreprises sur la mise en place d'une stratégie de défense active mais sans sortir du cadre législatif en vigueur.

Constat :

La nature des attaques informatiques évolue et se complexifie : elles ne se contentent plus toujours de contourner les défenses en place mais s'efforcent parfois de se maintenir dans le système informatique visé sans déclencher immédiatement l'attaque. L'attaquant améliore ainsi sa connaissance de la victime pour préparer une seconde attaque plus large (vols de données etc.).

Face à des attaques qui s'adaptent, un nouveau concept émerge : la défense active. Elle vise à mettre en place une stratégie de défense dont le but est de réduire la menace ou de ralentir la progression de l'attaquant sans se limiter à son propre système informatique (en collectant de l'information sur

l'attaquant par exemple) ou en agissant, dans le cadre légal, sur les outils utilisés par les attaquants.

Cette stratégie n'est pas à confondre avec la riposte directe (hack back en anglais) à laquelle la France s'oppose publiquement sur la scène internationale. Il existe en effet différents types de réponses possibles à une cyberattaque pour les entreprises s'inscrivant bien dans un cadre légal : la saisie de serveurs ou noms de domaine utilisés de façon malveillante par exemple.

Recommandation :

Nous recommandons donc de cadrer l'usage de stratégies de défense active avec, par exemple, la parution d'un guide de réponse à incidents incluant des principes de défense active.

13. Imposer un label de cyberrésilience pour les équipements les plus à risque pour pouvoir continuer à agir en cas de crise et préserver les vies humaines. Cela doit s'inscrire dans un mouvement de responsabilisation des éditeurs et des fabricants en imposant des mesures de fonctionnement garanti même en cas de cyberattaque pour les équipements les plus sensibles (médicaux, industrie à risque, véhicule, radio des services de secours…) et ce malgré la compromission des réseaux IT/OT/IoT.

Constat :

Les équipements sensibles intègrent rarement des mesures de sécurité assurant leur fonctionnement même en cas de défaillance ou d'attaque sur leurs composants informatiques, en particulier pour ceux qui assurent des fonctions de sûreté. En parallèle, la présence de plus en plus forte des objets connectés va augmenter l'exposition aux risques.

Recommandation :

Nous proposons de mettre en œuvre une démarche de labellisation des équipements les plus sensibles (médicaux, embarqués…) à l'échelle européenne, à l'instar du marquage CE, en imposant un fonctionnement de « survie » en cas de cyberattaques. C'est ce fonctionnement de sûreté, dans certains cas non-numérique (prenons l'exemple de la pédale de frein d'une voiture autonome), qui limite le danger en cas de défaillance des systèmes.

Notons que l'ANSSI analyse et certifie déjà de nombreux produits.

DOCUMENT 4

« Cyberattaques: le Conseil est désormais en mesure d'imposer des sanctions »

Communiqué de presse / Site du Conseil de l'UE, 17 mai 2019

Le 17 mai 2019, le Conseil a établi un cadre permettant à l'UE d'imposer des **mesures restrictives ciblées visant à décourager et contrer les cyberattaques** qui constituent une **menace extérieure pour l'UE ou ses États membres**, y compris les cyberattaques **dirigées contre des pays tiers ou des organisations internationales** lorsque des mesures restrictives sont jugées nécessaires pour réaliser les objectifs de la politique étrangère et de sécurité commune (PESC).

Les cyberattaques relevant du champ d'application de ce nouveau régime de sanctions sont celles qui ont des **effets importants** et qui:

- ont leur origine ou sont menées à l'extérieur de l'UE, ou
- utilisent des infrastructures situées à l'extérieur de l'UE, ou
- sont menées par des personnes ou entités établies ou agissant à l'extérieur de l'UE, ou
- sont menées avec l'appui de personnes ou entités agissant à l'extérieur de l'UE.

Les tentatives de cyberattaques ayant des effets potentiels importants sont également couverts par ce régime de sanctions.

Plus particulièrement, ce cadre permet pour la première fois à l'UE d'imposer des sanctions à des personnes ou entités qui sont **responsables de cyberattaques ou de tentatives de cyberattaques**, qui apportent un **soutien** financier, technique ou matériel à des cyberattaques ou sont **impliquées** de toute autre manière dans celles-ci. Des sanctions peuvent également être imposées à des personnes ou entités qui leur sont associées.

Les mesures restrictives comprennent, à l'encontre des personnes, l'**interdiction** de voyager vers l'UE et, à l'encontre des personnes et entités, le **gel des avoirs**. En outre, il est interdit aux personnes et aux entités de l'UE de mettre des fonds à la disposition des personnes et entités inscrites sur la liste.

Contexte

L'UE est consciente que le cyberespace offre des possibilités considérables, mais aussi qu'il présente des défis en constante évolution. Elle est **préoccupée par la multiplication des actes de cybermalveillance** qui visent à saper l'intégrité, la sécurité et la compétitivité économique de l'UE, et font peser un risque de conflit.

Le 19 juin 2017, le Conseil a adopté un cadre, la **boîte à outils cyberdiplomatique**, qui contribue à améliorer la coopération, prévenir les conflits, réduire les cybermenaces potentielles, décourager les éventuels agresseurs et influencer leur comportement. Il s'agit d'une réponse aux préoccupations croissantes suscitées par la capacité et la volonté accrues d'acteurs étatiques et non étatiques à commettre des actes de cybermalveillance.

Le 16 avril 2018, le Conseil a adopté des **conclusions sur les actes de cybermalveillance**, dans lesquelles il a souligné l'importance que revêt un cyberespace mondial ouvert, libre, sûr et stable, et a exprimé ses préoccupations quant aux activités d'acteurs malveillants.

Le 28 juin 2018 et le 18 octobre 2018, le **Conseil européen** a appelé à poursuivre les travaux sur la capacité de réaction aux cyberattaques et de dissuasion de ces attaques.

Le 12 avril 2019, la haute représentante a publié une déclaration au nom de l'Union européenne insistant sur la nécessité de respecter la primauté du droit dans le cyberespace, **exhortant les responsables à mettre un terme aux activités de cybermalveillance**, y compris le vol de propriété intellectuelle, et invitant tous les partenaires à renforcer la coopération internationale afin de promouvoir la sécurité et la stabilité dans le cyberespace.

L'UE demeure déterminée à conserver un cyberespace ouvert, stable et sûr, et réaffirme son attachement au règlement des différends internationaux dans le cyberespace par des moyens pacifiques. Dans ce contexte, l'ensemble des efforts diplomatiques déployés par l'UE devraient en priorité viser à promouvoir la sécurité et la stabilité dans le cyberespace au moyen d'une coopération internationale renforcée, ainsi qu'à réduire le risque de perceptions erronées, d'escalade et de conflits pouvant découler d'incidents liés aux technologies de l'information et de la communication (TIC).

DOCUMENT 5

« Les réponses de l'Anssi face aux cinq grandes cybermenaces »

Eitel Mabouong, Face au Risque, 3 mai 2019

Cinq grandes menaces liées au numérique ont récemment été listées par l'Anssi (l'Agence nationale de la sécurité des systèmes d'information). Cette même agence a livré un panel de solutions pour répondre efficacement à ces cybermenaces.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) a dévoilé son dernier rapport sur les menaces numéruques à la mi-avril. D'après ce rapport, il est ainsi question – concernant les cybermenaces – de *« 5 grandes tendances »* dégagées en France et en Europe durant l'année 2018.

Ces menaces ont été listées par ordre d'importance :

1. *Espionnage*
2. *Attaques directes* (contournement des mesures de sécurité des grandes entreprises par le biais d'un intermédiaire au système informatique plus vulnérable)
3. *Opérations de déstabilisation et influence*
4. *Génération et multiplication de* ***cryptomonnaies***
5. *Fraude en ligne* (les collectivités territoriales ou des acteurs du secteur de la santé sont les nouvelles cibles des cyberattaquants)

Pour l'agence, l'espionnage est *« le risque qui pèse le plus sur les organisations. Cela en raison d'un "financement important"* de la part des cyberattaquants. Les secteurs de la défense, de la santé ou encore de la recherche sont en outre les principales cibles des attaquants si l'on en croit ce rapport établi pour l'année 2018.

Directeur général de l'Agence nationale de la sécurité des systèmes d'information, Guillaume Poupard a notamment évoqué cette part grandissante de l'espionnage numérique.

> *« Des groupes très organisés préparent ce qui ressemble aux conflits de demain, en s'introduisant dans les infrastructures des systèmes les plus critiques »*, a dans un premier temps confié l'intéressé. Avant d'ajouter : *« Les attaquants exploitent de plus en plus les relations de confiance établies entre partenaires pour accéder aux informations qu'ils convoitent »*.

L'Anssi entend renforcer les partenariats

Devant ce constat, l'Anssi appelle notamment à un *« renforcement des partenariats avec des acteurs des secteurs public et privé ». « Face à l'ampleur de ces nouvelles menaces, l'Anssi a consolidé les liens tissés avec ses partenaires, au niveau national, comme au niveau européen »*, rappelle notamment l'agence.

Formation et responsabilisation

Outre les partenariats, il est par ailleurs question de formation dans ce rapport.

« L'agence a renforcé et développé des labels et des partenariats pour former et responsabiliser. Le dispositif SecNumedu qui labellise des formations initiales en cybersécurité de l'enseignement supérieur a été complété en 2018 par le programme SecNumedu-FC qui (...) permet d'éclairer les choix des employeurs ».

En plus de SecNumedu et SecNumedu-FC, *« le programme de sensibilisation en ligne »* SecNumacadémie a obtenu le « Coup de cœur des internautes » 2018 lors de la cérémonie MOOC of the year.

Fort de cette tendance, Guillaume Poupard entend prendre de l'avance sur ce domaine… En misant dès aujourd'hui sur les futures générations. Il souhaite ainsi que le secteur numérique fasse *« son entrée dans les manuels scolaires et la formation professionnelle, pour faire de chacun un acteur engagé »*.

Dans sa quête d'anticipation et de responsabilisation, l'Anssi a en outre relayé « L'appel de Paris » lancé par le président de la République le 12 novembre 2018. Le but est clair : « *Renforcer les responsabilités des acteurs privés de l'écosystème numérique »*. Mais également, connaître une *« véritable avancée pour l'autonomie stratégique européenne »*.

« La France a fait de la promotion de la paix et du renforcement de la stabilité du cyberespace l'une de ses priorités, (...) avec pour objectif d'élever le niveau de sécurité en Europe », a ainsi rappelé Guillaume Poupard en guise de conclusion.

DOCUMENT 6

« FireEye : zoom sur 5 groupes malveillants repérés en France »

Louis Adam, ZDNet, 17 octobre 2019

Sécurité : À l'occasion des Assises de la sécurité, la société FireEye donnait une présentation portant sur 5 groupes d'attaquants sophistiqués ayant été repérés en France et en Europe récemment.

Avec le rachat de la société Mandiant en 2013, FireEye est devenu un acteur majeur de la réponse à incident et un spécialiste des groupes d'attaquant de haut vol, fréquemment désignés sous le nom d'APT, pour Advanced Persistent Threat.

Aux assises de la sécurité, FireEye est venu présenter le travail de ses équipes au cours d'un atelier présentant 5 groupes d'acteurs sophistiqués ayant été repérés en France dans le courant de l'année 2018. Nous avons pu discuter avec David Grout, CTO EMEA de FireEye, qui nous a détaillé les cinq groupes actifs en France ayant retenu l'attention de la société.

Chaque société de cybersécurité ayant pris la liberté de nommer les groupes selon ses propres schémas, nous avons choisi de suivre les appellations de FireEye, mais un tableau regroupant les différentes appellations a été publié par le journaliste Lorenzo Francesci-Bicchierai à cette adresse. Cette ressource précieuse permet de limiter les maux de tête pour ceux qui tenteraient de s'y retrouver dans la jungle des appellations de groupes APT.

APT 10

FireEye travaille sur ce groupe depuis 2014, et celui-ci est bien connu des services.

En décembre 2018, la justice américaine a lancé une mise en accusation visant deux citoyens chinois ayant travaillé pour le groupe APT10. « Nous les avons vus actifs en France sur certaines cibles que je ne peux pas dévoiler. Leur spécialité, c'est de s'attaquer aux tiers de confiance afin de basculer ensuite sur leurs cibles et leur activité se concentre principalement dans le cyberespionnage. »

Ce style d'attaque, parfois décrit comme « attaque par rebond » ou « supply chain attack », est très populaire auprès des groupes d'attaquants sophistiqués : l'Anssi décrivait récemment des méthodes similaires dans un rapport publié sur son site web.

Prudente, l'Anssi n'attribue pas les attaques à un groupe particulier, mais le malware utilisé dans les attaques, PlugX, a déjà été utilisé par APT 10 dans le passé.

FIN6

Si l'acronyme APT est généralement utilisé par FireEye pour décrire les groupes d'attaquants opérant dans le domaine de l'espionnage, l'acronyme FIN est ici utilisé pour évoquer des groupes ayant des motivations purement financières. Le but n'est pas ici de voler des données, mais bien de récupérer de l'argent.

« C'est un groupe qui utilise des méthodologies proches des groupes soutenus par des États, mais qui finit généralement ses opérations par un ransomware doublé d'une demande de rançon. Ils se propagent sur le réseau de manière discrète et une fois qu'ils ont pris position, ils commencent à bloquer les machines, généralement pendant un week-end. ».

Aux dernières nouvelles, FIN6 avait recours aux souches de ransomware Ryuk et LockerGoga, deux variantes populaires et particulièrement efficaces de ransomware. FireEye explique être intervenu sur un ou deux cas en France dans lequel ce groupe était impliqué.

APT41

Un autre groupe chinois sur lequel FireEye a publié un rapport récent. Le groupe est également spécialisé dans l'espionnage industriel : « Les cibles du groupe sont alignées avec les priorités du programme **Made in China 2025** : ce programme publié par la Chine il y a quelques années liste plusieurs domaines technologiques et l'objectif affiché par la Chine est d'être en mesure de produire 80 % de ses besoins internes directement en Chine. »

Les cibles d'APT41 sont alignées sur les différents secteurs listés dans le rapport. FireEye a publié plusieurs indicateurs de compromission concernant ce groupe et selon David Grout, plusieurs opérateurs et acteurs français auraient retrouvé les traces de son activité en scannant leurs propres systèmes.

« La particularité de ce groupe, c'est peut-être leur double casquette : en journée, ils mènent des opérations de cyberespionnage classique, mais la nuit, on a constaté qu'ils opéraient dans une logique de cybercriminalité financière, notamment des escroqueries autour des monnaies virtuelles et des jeux en ligne. » Comme quoi, même les cybercriminels doivent savoir se diversifier.

UNC12/42

L'acronyme UNC est utilisé pour les groupes dont les motivations ne sont pas encore claires.

« C'est un groupe qu'on a vu plusieurs fois en Europe et en France. On a des indices qui nous laissent penser qu'il est basé en Europe ou aux États-Unis ».

La spécialité de ce groupe : la compromission d'Active Directory chez les cibles, peut être à des fins de revente pour d'autres groupes par la suite.

« Ils ont une particularité : ils exfiltrent la plupart du temps les données volées via des archives .rar chiffrées, mais ils utilisent toujours le même mot de passe pour l'archive. Depuis qu'on est arrivé à le décrypter, c'est d'ailleurs comme ça qu'on les reconnaît quand on intervient sur de nouvelles victimes : on teste le mot de passe et si ça fonctionne, on sait que c'est eux » explique David Grout.

APT39

Cette fois-ci, les experts de FireEye lient ce groupe à l'Iran. « Leur spécialité est la récupération de données personnelles à des fins de profiling, de potentielles cibles ou victimes. » APT39 est principalement actif dans le domaine des télécommunications ou des transports : le groupe se concentre sur la récupération de métadonnées ayant pour but de comprendre qui communique avec qui. « On suppose qu'ils récupèrent ces données afin de comprendre les liens entre différentes structures industrielles, ou bien anticiper certains rapprochements de type joint venture dans le domaine de la pétrochimie ou de l'aéronautique dans la zone du Moyen-Orient. »

DOCUMENT 7

« Vous avez environ 20 minutes pour contenir une attaque APT en provenance de la Russie »

Catalin Cimpanu, ZDNet, 20 février 2019

Technologie : Côté cybersécurité, les pirates agissant pour le compte de la Russie ne laissent aucune place à l'erreur. Un classement fait le point sur le « temps de déclenchement » nécessaire aux pirates pour infecter les réseaux d'entreprise.

Les agences gouvernementales et les entreprises disposent d'environ 20 minutes pour détecter et contenir une tentative de piratage en provenance de la Russie.

De nouvelles statistiques publiées par la société américaine de cybersécurité Crowdstrike classent les différents groupes de pirates en fonction de leur « temps de pénétration » ou « temps de déclenchement » (breakout time).

Un indicateur qui désigne le temps nécessaire à un groupe de pirates informatiques pour accéder à l'ordinateur d'une victime et à se infecter ensuite le reste du réseau une fois ce premier ordinateur compromis. Cela inclut le temps que l'attaquant passe à analyser le réseau local et à déployer son attaque afin d'escalader les droits d'accès pour s'emparer du contrôle des autres machines.

Cet indicateur est crucial pour les organisations, car il souligne le temps dont elles disposent pour détecter les infections et isoler les ordinateurs piratés avant qu'une simple intrusion ne devienne une menace pour l'ensemble du réseau.

Selon les données recueillies en 2018, CrowdStrike dit que les pirates russes (que la société appelle en interne « Bears ») sont les plus prolifiques et efficaces, avec un temps moyen de déclenchement de 18 minutes et 49 secondes.

Ils sont suivis par les groupes nord-coréens – les « chollimas » (un pégase coréen) – avec 2 heures et 20 minutes, les groupes de pirates chinois (les pandas) avec 4 heures, les iraniens (les chatons) avec 5 heures et 9 minutes, et les cybercriminels non identifiés comme travaillant pour des États (les araignées) avec environ 9 heures et 42 minutes.

« Le temps moyen global de pénétration que CrowdStrike a observé en 2018 pour toutes les intrusions et tous les pirates était de 4 heures et 37 minutes, une augmentation substantielle par rapport à 1 heure et 58 minutes enregistrées en 2017 », a déclaré l'équipe de CrowdStrike.

« Bien qu'il ne s'agisse certainement pas de la seule mesure permettant de juger de la sophistication, ce classement par temps de pénétration est un moyen intéressant d'évaluer les capacités opérationnelles des principaux pirates », ont-ils ajouté.

La capacité de sortir d'un ordinateur initialement compromis nécessite à la fois des compétences, des outils de piratage et des failles facilement exploitables. Il est normal que les groupes russes, nord-coréens et chinois se classent en tête de ce classement, car ils sont les acteurs les plus actifs en matière de cybermenaces sur la dernière décennie. Ces acteurs ont consacré de nombreuses ressources à la création d'outils avancés et au perfectionnement de leurs compétences.

Les mesures du « temps de déclenchement » sont incluses dans le rapport sur les menaces mondiales de CrowdStrike, Global Threat Report 2019. Le rapport embarque un résumé des cyber-opérations menées l'année dernière par des groupes de cybercriminels.

Voici quelques-unes des conclusions du rapport :

- Les attaques en provenance d'États ont été continues tout au long de 2018. Elles ont ciblé les dissidents, les adversaires régionaux et les puissances étrangères à des fins de renseignement.
- De nombreux pays ont utilisé les médias et les canaux diplomatiques pour prétendre qu'ils mettaient un frein aux cyberactivités de cette nature, mais ont poursuivi leurs activités comme d'habitude.
- 60 % des cyber-attaques impliquent une forme de malware.
- La Chine et la Corée du Nord ont été à l'origine de près de la moitié de toutes les attaques en provenance des États en 2018.
- Le piratage de la supply chain des entreprises au lieu d'attaquer directement les cibles est devenu une tendance majeure.
- L'Iran et la Russie concentrent leurs efforts de piratage informatique sur les entreprises de télécommunications.
- Les groupes de cybercriminels ont de plus en plus recours à la location de services ou d'outils fournis par d'autres groupes au lieu de créer leurs propres outils.
- Du côté des ransomwares, les cybercriminels ont adopté la tactique de la "chasse au gros gibier". Ils s’en prennent de façon ciblée aux grandes entreprises afin de pouvoir obtenir des rançons plus importantes en une fois.
- CrowdStrike a également observé une collaboration accrue entre acteurs criminels hautement sophistiqués.

DOCUMENT 8

La “nouvelle ENISA” : Europe Kicks off ! (par le général d’armée Watin-Augouard, fondateur du FIC)

Site Observatoire FIC [Le Forum international de la cybersécurité], 25 juillet 2019

Europe kicks off !

Telle était la *base line* du FIC 2019. Alors que l’Union européenne s’intéresse chaque année davantage au FIC, dont elle a favorisé la création, le FIC souhaitait soutenir les efforts qu’elle accomplit pour créer un espace numérique européen plus sûr et porteur de valeurs qui nous distinguent et nous rassemblent.

Malgré les vicissitudes, l’Europe numérique se réveille, il faut s’en réjouir, dès lors qu’elle complète les efforts accomplis par les États membres et offre un cadre favorable à une souveraineté partagée. Elle est productrice de règlements et directives, les plus connus étant le RGPD et le directive NIS. Cette directive pose des exigences relatives aux capacités nationales de cybersécurité et instaure les premiers mesures destinées à renforcer les secteurs d’importance vitale à améliorer la coopération stratégique et opérationnelle entre les États membres.

Le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019, relatif à l’Agence de l’Union européenne pour la cybersécurité (ENISA) et à la certification de cybersécurité des technologies de l’information et des communications a été publié au journal officiel de l’Union, le 7 juin. Il pérennise l’ENISA, dont le mandat allait s’achever en 2020, et crée une certification européenne à trois niveaux.

La « nouvelle ENISA », organisme de l’Union doté de la personnalité juridique, elle est désormais pérennisée. Son mandat (art. 3 du règlement) précise qu’elle doit fournir des conseils en matière de cybersécurité, favoriser la coopération opérationnelle à la fois entre les États membres et entre ceux-ci et les institutions, organes et organismes de l’Union. Elle a aussi pour mission d’apporter des compétences et jouer le rôle de centre d’information et de connaissance de l’Union. Elle doit encourager l’échange de bonnes pratiques entre les États membres et le secteur privé, proposer des actions à la Commission et aux États membres.

L’ENISA devra soutenir le développement et l’amélioration des centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux et de l’Union prévus par la directive (UE) 2016/1148, afin qu’ils atteignent un niveau de maturité commun élevé dans l’ensemble de l’Union. Elle ne doit pas se substituer aux États membres mais doit être en mesure de leur fournir un appui, à leur demande.

L’ENISA devrait participer aux actions de coopération avec l’OCDE, l’OSCE ou l’OTAN, sans préjudice du caractère particulier de la politique de sécurité et de défense de tout État membre.

Le nouveau règlement favorise le recours à la certification européenne de cybersécurité en vue d’éviter la fragmentation du marché intérieur. Il institue le principe de reconnaissance mutuelle au sein de l’UE des certificats délivrés par un État membre. Il s’agit de construire un cadre européen de certification de cybersécurité homogène pour éviter la pratique du « hopping de certifications » qui joue sur la différence du niveau d’exigence entre les États membres. Du passé le règlement ne fait pas table rase, puisqu’il ambitionne de « créer les conditions d’une transition en douceur des schémas existants relevant de ces systèmes vers les schémas relevant du nouveau cadre européen de certification de cybersécurité ». Selon le règlement, un « certificat de cybersécurité européen », est un document délivré par un organisme compétent attestant qu’un produit TIC, service TIC ou

processus TIC donné a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité. Un groupe des parties prenantes pour la certification de cybersécurité est établi. Ses membres sont sélectionnés par la Commission, parmi des experts reconnus représentant les parties prenantes concernées. Cette gouvernance de la certification doit adopter des schémas offrant trois niveaux : un niveau « élémentaire » pour les systèmes non critiques (objets grand public), un niveau « substantiel » et un niveau « élevé » pour les systèmes présentant les plus de risques aux cyberattaques.

Il était à craindre que la « nouvelle ENISA » soit un organisme supranational, tandis que les critères de certification favorisent le « moins disant » en optant pour le plus petit dénominateur commun. L'ANSSI – qui vient de fêter ses dix ans d'existence – ne pouvait voir ses efforts annihilés. Sur son site internet, elle exprime sa satisfaction.

Ancien inspecteur général des armées – Gendarmerie nationale, le général d'armée (2s) Watin-Augouard est le fondateur du FIC et dirige aujourd'hui le Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN).

DOCUMENT 9

« La cyberdéfense française renforce son ancrage rennais »

Hassan Meddah, L'Usine Nouvelle, 3 octobre 2019

L'armée renforce sa présence en Bretagne. La ministre des Armées inaugure un nouvel établissement du commandement de la cyberdéfense prêt à accueillir 400 experts informatiques. En Ille-et-Vilaine, l'armée s'organise pour se rapprocher des acteurs académiques et industriels pour capter plus rapidement l'innovation issue du secteur civil.

A Bruz, près de Rennes, les experts de la DGA disposent de fortes compétences en matière de maîtrise et protection de l'information ainsi qu'en guerre électronique (cyber)

Une fois n'est pas coutume, Florence Parly se rend jeudi 3 octobre à Rennes (Ille-et-Vilaine) et dans ses environs pour parler cyberdéfense. Au quartier Stéphant, dans la commune limitrophe de Saint-Jacques-de-la-Lande, elle va inaugurer le premier bâtiment du ComCyber, ce commandement en charge d'assurer la cyberdéfense de la France. Les nouveaux bureaux fortement équipés en moyens informatiques permettront d'accueillir 400 experts numériques. L'organisme créé en 2017 a pour mission d'assurer la protection des systèmes d'information du ministère des Armées mais également la conduite des opérations militaires dans le cyberespace.

La cyberdéfense est l'une des priorités affichées des armées. Durant la période 2019-2025, le ministère va y consacrer 1,6 milliard d'euros et recrutera 1100 cybercombattants. La Bretagne est le principal lieu de cette expertise avec 1600 spécialistes cyber sur les 4000 que comptera le ministère à l'horizon 2025. A une quinzaine de km au sud de Rennes, à Bruz, le centre de la DGA (direction générale de l'armement) concentre l'expertise des armées dans le domaine des communications électroniques et des technologies numériques. C'est donc un poste avancé indispensable pour comprendre les nouvelles formes de guerre dans le cyberespace et comment le pays s'y prépare.

A Rennes, l'armée veut également s'ouvrir aux acteurs académiques et privés regroupés au sein du pôle d'excellence cyber. Elle est consciente qu'en matière de cybersécurité, l'innovation est tirée fortement par le secteur civil. Florence Parly va inaugurer pour cela un lieu de rencontre entre les acteurs étatiques et leurs partenaires : la Cyber Factory. Il s'agit d'un open space de 200 m2 situé dans la zone d'activité de la Courrouze. Typiquement, la DGA, le ComCyber partageront des données avec les industriels pour améliorer les performances des algorithmes de sécurité informatique. La Cyber factory hébergera aussi un incubateur technologique dans le but d'accompagner des experts cyber du ministère des Armées désireux de développer leurs propres entreprises.

Profitant de son déplacement, la ministre signera un accord avec la société de gestion de fonds d'investissement ACE Management. Cette société gère 500 millions d'euros pour soutenir des entreprises dans les domaines de l'aéronautique, du maritime ainsi que de la cybersécurité et la défense. ACE Management vient de créer un fonds de 80 millions d'euros pour soutenir les pépites technologiques françaises et européennes dans le secteur de la cybersécurité.

"On s'est rendu compte que le domaine de la cybersécurité est peu attractif pour les investisseurs financiers. C'est un domaine considéré comme très technique, avec des cycles de développements et d'accès aux marchés qui sont parfois jugés trop longs" reconnaît-on au ministère des Armées. Le ministère s'engage à identifier des entreprises détenant un savoir-faire en matière de cybersécurité et à les proposer à ACE Management en vue d'une éventuelle prise de participation et d'un accompagnement de ces entreprises.

DOCUMENT 10

Dark web : la belle prise des douanes françaises

Romain Gueugneau, Les Échos, 16 juin 2018

Gérald Darmanin a annoncé le démantèlement du forum « Black Hand », une plateforme de vente illégale qui compte plus de 3 000 membres.

C'est une première en France. Les douanes ont mis hors de service l'une des plus importantes plateformes illégales actives sur le « dark web ». C'est le ministre des comptes publics, Gérald Darmanin, qui l'a annoncé lui-même ce samedi.

L'opération, présentée comme « hors norme » par Bercy, a permis de démanteler le forum Black Hand, très actif dans cette partie cachée de l'Internet et non référencée par les principaux moteurs de recherche - et par conséquent très prisée par les trafiquants en tous genres. Le site proposait à la vente depuis deux ans de nombreux produits et services illicites (stupéfiants, armes, faux papiers, données bancaires volées, etc), selon le communiqué du ministère.

Lutte contre la cyberdélinquance

« Le démantèlement de cette plateforme illustre la mobilisation de la douane dans la lutte contre les nouvelles formes de cyberdélinquance », s'est félicité Gérald Darmanin.

L'opération menée de façon simultanée dans plusieurs villes de France a permis de saisir près de 4.000 euros en liquide et environ 25.000 euros dans diverses monnaies virtuelles. Les enquêteurs ont également eu accès aux serveurs de « Black Hand » et saisir les données qu'ils contenaient.

D'après les enquêteurs, le forum était l'un des plus actifs en France : plus de 3.000 personnes y étaient inscrites selon les premières investigations techniques menées.

Interpellations

Plusieurs personnes ont été interpellées à l'issue de l'opération des douanes, dont la principale administratrice du site. Après les gardes à vue, quatre suspects ont été déferrés vendredi devant le parquet de Lille. L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) sera chargé de poursuivre l'enquête.

Si la prise est belle pour les douanes françaises, reste à savoir si elle permettra de limiter les trafics sur internet. Les fermetures de sites et les saisies de matériels et de données sont fréquentes, mais elles règlent rarement le problème, car les acheteurs trouvent très vite d'autres alternatives. Comme la nature, le « dark web » a horreur du vide.

DOCUMENT 11

« Cyberattaques : comment les États peuvent-ils se protéger ? »

Michael Techer, Entreprendre.fr, 20 septembre 2019

Tribune. Au printemps 2007, l'Estonie est devenue la première nation au monde à être victime d'une cyberattaque ciblée à grande échelle. Cette attaque DDoS (déni de service distribué) a paralysé le gouvernement et d'autres sites web critiques, ainsi que des systèmes tels que l'infrastructure bancaire, dans ce qui était à l'époque un des pays les plus connectés au monde, obligeant le pays à se déconnecter d'Internet pour rétablir ses services.

Depuis, les attaques à grande échelle contre des intérêts nationaux visant à endommager des infrastructures critiques et déstabiliser des pays se sont multipliées. Par exemple, le célèbre ver Stuxnet, détecté en juin 2010, ciblant une infrastructure « à haute valeur » en Iran et presque certainement parrainé par un État. Ou les États-Unis et le Royaume-Uni faisant une déclaration commune en avril 2018 concernant des cyberactivités malveillantes, prétendument perpétrées par le gouvernement russe.

Les cyberattaques ciblées à grande échelle visant des États peuvent avoir de nombreuses conséquences, allant de perturbations jusqu'à des décès. Que se passerait-il, par exemple, si l'alimentation en eau ou en électricité d'une ville était coupée, même pour une période de 36 heures ? Les entreprises ne pourraient pas fonctionner, les patients hospitalisés et les personnes vulnérables pourraient en mourir. Une attaque à grande échelle contre le système bancaire pourrait paralyser les marchés financiers, et faire chuter des entreprises, et même des économies. Des attaques qui perturbent les systèmes de transport tels que le contrôle du trafic aérien pourraient avoir des conséquences évidentes.

La cyberguerre menée par un État contre un autre est devenue un danger très concret. La question qui se pose alors est la suivante : que peuvent faire les gouvernements pour protéger leurs citoyens et leurs infrastructures ?

L'état actuel de la cybersécurité nationale

Il est important de se rappeler que les cyber-risques pesant sur des pays ne proviennent pas uniquement d'autres pays. Des organisations cybercriminelles, des terroristes, des hacktivistes et autres, utilisent des outils sophistiqués et réutilisent même ceux développées par des États, qui sont entrées dans le domaine public. C'était le cas de l'attaque globale du logiciel rançonneur WannaCry (et de l'attaque de NotPetya qui a suivi), qui a fait la une des actualités en 2017. Il n'est pas étonnant que le Rapport sur les risques mondiaux en 2018 publié par le Forum économique mondial place les cyberattaques en haut de liste, tant pour leur probabilité que pour leur impact. Ainsi, la plupart des États ont déjà cessé de considérer les cybermenaces comme étant « seulement » des pertes financières, des pertes de données ou des atteintes à la vie privée, pour en faire de véritables menaces à la sécurité physique et la vie.

La plupart des gouvernements adoptent désormais une approche à trois volets en matière de cyberdéfense. Premièrement, ils ont tendance à créer des cyberarmes, c'est-à-dire à mettre en place des comités et des administrations ont pour objectif d'étudier la meilleure stratégie, législation et approche pour faire face aux cybermenaces.

Deuxièmement, les gouvernements renforcent les programmes d'éducation et de sensibilisation. La plupart du temps, ils essaient de remédier à la pénurie mondiale en professionnels de cybersécurité, qui est estimée à environ 3,5 millions.

Troisièmement, ils établissent au moins un CERT (centre d'alerte et de réaction aux attaques informatiques) national civil, afin de faire face aux cybermenaces et aux cyberattaques. Les pays séparent généralement leur cyberdéfenses militaires et civiles. Pour la défense civile, ils peuvent avoir un seul CERT centralisé ou quelques CERT spécifiques à certains secteurs. Mais comme leur nom l'indique, les CERT sont, par définition, réactifs plutôt que proactifs. Ils n'agissent généralement qu'après qu'un incident informatique majeur soit en cours ou se soit produit. Certains CERT se dotent de moyens proactifs. Ils collectent des informations et tentent d'alerter sur les nouveaux risques émergents ou les attaques prévisibles, mais l'efficacité de ces mesures est limitée, car le cycle global de détection, d'analyse, de publication et de mise en œuvre peut prendre des semaines plutôt que quelques secondes ou quelques minutes.

En tout état de cause, la majorité des CERT n'a ni les moyens juridiques, ni la capacité technique de protéger les intérêts nationaux de manière proactive en temps réel ou presque. C'est là que les choses doivent changer. Aujourd'hui, même si un CERT est informé quelques heures avant une méga attaque, il n'a aucun moyen de bloquer l'attaque de manière proactive ni défendre les principaux secteurs, services publics, hôpitaux, aéroports et autres installations critiques.

Établir une cybersécurité nationale efficace

Examinons plutôt un modèle de sécurité que nous connaissons mieux. En plus de défendre les frontières d'un pays, les défenses de la sécurité intérieure utilisent des outils tels que le radar pour scruter le ciel à la recherche d'attaques imminentes de missiles contre les villes et l'intérieur du pays. Cela permet d'analyser les actions de l'ennemi et prendre des décisions intelligentes afin d'instruire les citoyens de s'abriter ou lancer des frappes antimissiles.

Une approche similaire devrait être adoptée pour les cyberdéfenses nationales. Des protections internes et périmétriques sont nécessaires pour se protéger contre tout un ensemble de menaces, tentatives d'attaques de DDoS, logiciels malveillants furtifs et destructeurs. Les principaux points d'accès aux infrastructures critiques du pays doivent être surveillés de manière proactive, avec alimentation des informations sur les menaces à un centre d'opérations afin d'identifier, analyser et déterminer de manière proactive la réponse correcte aux menaces entrantes. Cela peut être associé à la prévention des menaces en temps réel pour piéger les nouvelles menaces de logiciels malveillants évasifs avant qu'ils ne se propagent à grande échelle.

Cette couche d'analyse des menaces et de visibilité doit constituer un « parapluie » sur les cyberdéfenses et les sources de renseignements des organisations, pour garantir la résilience globale du pays. Ces protections doivent être aussi automatisées que possible pour assurer une réponse immédiate, avec un minimum d'intervention humaine, afin de coïncider à la vitesse à laquelle les menaces actuelles peuvent se propager. Les protections doivent s'appuyer sur des renseignements en temps réel et sur une visibilité de la situation afin de se défendre contre des menaces, même nouvelles et jamais vues auparavant.

Internet a révolutionné tous les aspects de la société, y compris la diplomatie internationale et la guerre. Pour se défendre contre les nouvelles générations de menaces, la seule approche valable consiste à adopter une approche holistique de la cyberdéfense nationale, capable d'identifier les premiers signes d'attaque et les maîtriser automatiquement, avant qu'elles ne causent des perturbations généralisées.