HM Government

# STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2016-2021

# Sommaire

# AVANT-PROPOS

Le Royaume-Uni compte parmi les chefs de file du secteur numérique. Notre prospérité dépend largement de notre capacité de protéger nos technologies, données et réseaux face à une multitude de menaces.

Toutefois, non seulement les cyberattaques sont de plus en plus fréqentes, de plus en élaborées, mais en cas de réussite, elles sont aussi de plus en plus dévastatrices. D'où les mesures décisives prises pour protéger à la fois notre économie et la vie privée des citoyens britanniques.

L'objectif de notre Stratégie nationale de cybersécurité est de donner au Royaume-Uni l'assurance, la capacité et la résilience nécessaires pour s'affirmer dans un univers numérique en mutation rapide.

Au cours de cette stratégie quinquennale, nous consacrerons 1,9 milliard GBP (soit environ 2,27 Mrd €) à la défense de nos systèmes et infrastructures, à la dissuasion de nos ennemis et au développement d'une capacité valable pour toute la société — des plus grandes entreprises, au citoyen individuel.

De l'hygiène informatique la plus élémentaire à la dissuasion la plus moderne, une approche holistique s'impose.

Nous mettrons en oeuvre des défenses plus imparables, des compétences plus puissantes, dans le but de faire d'une attaque quelconque sur le territoire du Royaume-Uni, une entreprise plus rhédibitoire sur le plan financier. Cette question n'est plus seulement du ressort des services informatiques, mais concerne l'ensemble de la population active. Les cyber-compétences doivent s'étendre à toutes les professions.

Le nouveau Centre national de la cybersécurité servira de pôle d'expertise de rang mondial et convivial aux entreprises comme aux particuliers. Il disposera également des moyens nécessaires pour intervenir rapidement, en cas d'incidents majeurs.

Le gouvernement est parfaitement conscient de son rôle de leadership, mais il favorisera également le développement d'un écosystème commercial plus divers, en reconnaissant les domaines dans lesquels l'industrie peut innover plus vite que lui. Il s'efforcera notamment, d'intéresser les jeunes talents les plus prometteurs aux métiers de la cybersécurité.

La menace informatique touchant l'ensemble de notre société, il est évident que chacun a un rôle à jouer dans notre riposte nationale. C'est la raison pour laquelle cette stratégie représente un effort de transparence sans précédent. Le débat à ce sujet ne peut plus se dérouler à huis clos.

Quoi qu'il en soit, cette menace ne peut pas être complètement éliminée. La technologie numérique fonctionne parce qu'elle est ouverte, mais cette ouverture est inévitablement porteuse de risque. Nous pouvons néanmoins réduire la menace à un niveau suffisant, pour nous permettre de rester à l'avant-garde de la révolution numérique. Cette stratégie explique comment y parvenir.

**Philip Hammond, député,**
**Chancelier de l'Échiquier**

# PRÉFACE

Nous sommes avant tout responsables de la protection de la Nation et de la conduite compétente de son gouvernement. Cette stratégie reflète ces attributions. Elle constitue une démarche audacieuse et ambitieuse pour lutter contre les nombreuses menaces auxquelles notre pays doit faire face dans le cyberespace. Certes, nous avons tous un rôle à jouer pour les gérer et les réduire, mais le Gouvernement est conscient de la responsabilité particulière par laquelle il doit diriger l'effort national requis.

Le Gouvernement s'engage à veiller à ce que les promesses faites dans cette stratégie soient tenues et à contrôler, à faire le point régulièrement sur l'avancement des mesures prises à cette fin. En outre, nous évaluerons régulièrement notre démarche et réagirons à l'évolution du niveau de menace, ainsi qu'aux progrès des technologies dans le domaine de la sécurité.

Le Gouvernement a par ailleurs une responsabilité spéciale envers les citoyens de la Nation, les entreprises et organisations implantées au Royaume-Uni, ainsi qu'envers nos alliés et partenaires internationaux. Nous devrions pouvoir leur assurer que tous les efforts consentis l'ont été, pour rendre nos systèmes sûrs,protéger nos données et réseaux contre toute attaque ou tentative d'ingérence. D'où la nécessité de définir les normes de cybersécurité les plus strictes et de les appliquer scrupuleusement, à la fois en tant que pilier de la sécurité nationale et du bien-être économique de notre pays, mais aussi en tant qu'exemple à suivre. Nous rendrons compte annuellement des progrès réalisés.

En tant que Ministre adjoint chargé du « Cabinet Office », de la cybersécurité et de la sécurité du gouvernement, je suis déterminé à veiller à ce que tous les éléments de cette stratégie soient mis en œuvre. Je travaillerai en étroite collaboration avec mes collègues du Gouvernement, nos partenaires des administrations décentralisées, du secteur public en général, du secteur industriel et des milieux universitaires, pour concrétiser cette ambition.

**Ben Gummer, Ministre adjoint chargé du « Cabinet Office » et « Paymaster General »**

# 1. SYNTHÈSE

1.1. L'avenir de la sécurité et de la prospérité du Royaume-Uni repose sur des fondations numériques. L'enjeu pour notre génération est de bâtir une société numérique prospère, capable de résister aux menaces informatiques, disposant des connaissances et capacités requises pour maximiser les opportunités, tout en gérant efficacement les risques.

1.2. L'Internet fait aujourd'hui partie des éléments incontournables de notre vie. Il présente pourtant un risque intrinsèque et sera toujours sujet aux tentatives visant à en exploiter les failles, pour lancer des cyberattaques. Cette menace ne peut pas être éliminée à 100%. Elle peut néanmoins être considérablement réduite, pour permette à la société de continuer à prospérer et à tirer parti des grandes opportunités découlant de la technologie numérique.

1.3. Étayée par le Programme national de cybersécurité du gouvernement britannique financé à hauteur de 860 millions GBP (environ 1 milliard d'euros), la Stratégie nationale de cybersécurité 2011 a considérablement amélioré la cybersécurité du Royaume-Uni. Elle a atteint d'importants objectifs, en misant sur le marché pour favoriser l'adoption de comportements en ligne sûrs. Cette approche n'a cependant pas abouti à l'ampleur et au rythme de changement nécessaires pour garder une longueur d'avance sur une menace en évolution rapide. Il est temps d'aller plus loin.

1.4. Notre vision à l'horizon 2021 envisage un **Royaume-Uni sécurisé, résilient face aux cyber-menaces, prospère et confiant dans le monde numérique.**

1.5. Afin de concrétiser cette vision, nous nous efforcerons d'atteindre les objectifs suivants :

• **DÉFENDRE** Nous disposons des moyens nécessaires pour défendre le Royaume-Uni contre les cybermenaces évolutives, intervenir efficacement en cas d'incident, veiller à la protection et à la résilience des réseaux, données et systèmes britanniques. Les citoyens, les entreprises et le secteur public disposent des connaissances et capacités nécessaires pour se défendre.

• **DISSUADER** Le Royaume-Uni sera une cible difficile pour toutes les formes d'agression dans le cyberespace. Nous détectons, comprenons, enquêtons sur les manœuvres hostiles menées à notre encontre et les perturbons, recherchons et poursuivons en justice leurs auteurs. Nous sommes équipés pour prendre, si nous choisissons de le faire, des mesures offensives dans le cyberespace.

• **DÉVELOPPER** Innovant et en plein essor, notre secteur de la cybersécurité est étayé par des travaux de recherche et de développement scientifiques de rang mondial. Notre vivier de talents autosuffisant, nous fournit les compétences nécessaires pour répondre aux besoins des secteurs public et privé à l'échelle nationale. Nos capacités d'analyse et notre expertise de pointe permettront au Royaume-Uni non seulement de faire face, mais aussi de surmonter les menaces et défis futurs.

1.6. Pour étayer ces objectifs, nous mènerons une **ACTION INTERNATIONALE**. Nous exercerons notre influence en investissant dans les partenariats qui façonnent l'évolution mondiale du cyberespace, de manière à promouvoir nos intérêts économiques et sécuritaires au sens large.

Conscients qu'ils améliorent notre sécurité collective, nous renforcerons nos liens avec nos partenaires internationaux les plus proches. De plus, nous développerons nos relations avec de nouveaux partenaires, afin de rehausser leurs niveaux de cybersécurité et de protéger les intérêts britanniques à l'étranger. Nous nous y emploierons à la fois dans nos relations bilatérales et multilatérales, y compris par le biais de l'UE, de l'OTAN et des Nations Unies. Quant à nos ennemis, à ceux qui menacent de porter atteinte à nos intérêts et à ceux de nos alliés dans le cyberespace, les conséquences de leurs actes leur seront signifiées, sans équivoque.

1.7. Pour parvenir à ces résultats dans les cinq prochaines années, le Gouvernement britannique entend intervenir plus activement et investir, tout en continuant à aider les forces du marché à améliorer les normes de cybersécurité sur l'ensemble du territoire. Le Gouvernement britannique, en partenariat avec les administrations décentralisées d'Écosse, du Pays de Galles et d'Irlande du Nord, collaborera avec les secteurs public et privé pour faire en sorte que les particuliers, entreprises et organisations adoptent les comportements nécessaires pour ne pas prendre de risque en ligne. Des mesures d'intervention seront mises en place (si nécessaire, et dans les limites des pouvoirs qui nous sont délégués), pour favoriser l'adoption d'améliorations dans l'intérêt du pays, notamment par rapport à la cybersécurité de l'infrastructure critique de la Nation.

1.8. Le Gouvernement britannique puisera dans ses propres capacités et dans celles de l'industrie, pour mettre au point et appliquer des mesures de cyberdéfense active[1] visant à renforcer significativement les niveaux de cybersécurité sur les réseaux britanniques. Ces mesures viseront notamment à réduire au minimum les formes les plus communes d'attaques par hameçonnage, filtrer les adresses IP réputées néfastes et bloquer activement l'activité malveillante en ligne. Ces améliorations de la cybersécurité de base, rendront le Royaume-Uni plus résilient aux menaces informatiques les plus communément déployées.

1.9. Nous avons créé un Centre national de la cybersécurité (sigle anglais NCSC). Autorité compétente pour traiter les questions liées à l'environnement de la cybersécurité au Royaume-Uni, il se chargera du partage des connaissances, de la lutte contre les vulnérabilités systémiques et du leadership, dans le cadre du traitement des questions déterminantes portant sur la cybersécurité nationale.

1.10. Nous veillerons à ce que nos forces armées soient résilientes et dotées des cyberdéfenses solides nécessaires pour sécuriser et défendre leurs réseaux et plateformes, rester opérationnelles et libres de manœuvrer à l'échelle mondiale, en dépit des cybermenaces. Notre Centre des opérations de cybersécurité militaire collaborera étroitement avec le NCSC ; nous veillerons à ce que les forces armées puissent lui prêter main-forte dans l'éventualité d'une cyberattaque nationale de grande ampleur.

1.11. Nous disposerons des moyens nécessaires pour réagir aux cyberattaques, comme nous le faisons pour n'importe quelle autre attaque, en recourant aux capacités les plus appropriées, cybercapacité offensive incluse.

[1] Comprendre les menaces qui pèsent sur les réseaux, puis concevoir et mettre en place des mesures pour lutter de manière proactive ou se défendre contre ces menaces. Les termes techniques sont expliqués dans le glossaire.

1.12. Nous profiterons de l'autorité et de l'influence du Gouvernement britannique, pour investir dans des programmes visant à remédier aux pénuries de compétences en cybersécurité au Royaume-Uni, des écoles aux universités et sur l'ensemble de la population active.

1.13. Nous lancerons deux nouveaux centres de cyber-innovation, pour favoriser le développement de cyberproduits de pointe et d'entreprises de cybersécurité dynamiques. D'autre part, nous consacrerons une part des 165 millions GBP (194 m €) du Fonds de défense et de cyber-innovation à la passation de marchés innovants dans les domaines de la défense et de la sécurité.

1.14. Au cours des cinq prochaines années, nous investirons un total de 1,9 milliard GBP (2,23 Mrd €) pour transformer radicalement la cybersécurité au Royaume-Uni.

# 2. INTRODUCTION

2.1. Au cours des vingt dernières années, les technologies de l'information et de la communication ont évolué et jouent un rôle dans quasiment tous les aspects de notre vie. Le Royaume-Uni est une société numérisée. Notre économie et notre vie quotidienne n'en sont que plus riches.

2.2. La mutation provoquée par cette numérisation crée de nouvelles dépendances. L'économie, l'administration publique et les services essentiels dépendent dorénavant de l'intégrité du cyberespace, des infrastructures, systèmes et données qui le soutiennent. Toute perte de confiance dans cette intégrité compromettrait les avantages de cette révolution technologique.

2.3. Si une grande partie du matériel informatique et des logiciels développés à l'origine pour faciliter l'interconnexion de cet environnement numérique ont privilégié l'efficacité, les coûts et la commodité pour l'usager, ils n'ont pas toujours intégré la dimension sécurité dès le départ. Or, des acteurs malveillants — États hostiles, organismes ou individus criminels ou terroristes — peuvent exploiter cet écart entre commodité et sécurité. Le réduire constitue donc une priorité nationale.

2.4. L'expansion de l'Internet au-delà des ordinateurs et des téléphones portables et vers d'autres systèmes cyber-physiques ou dits « intelligents », étend la menace d'exploitation à distance à une foule de nouvelles technologies. Les systèmes et technologies indissociables de notre vie quotidienne — réseaux de distribution d'électricité, systèmes de contrôle du trafic aérien, satellites, technologies médicales, installations industrielles, feux de circulation, etc. — sont connectés à l'Internet et, par conséquent, potentiellement vulnérables face au risque d'intrusion.

2.5. La Stratégie de sécurité nationale (sigle anglais NSS) 2015 confirme le statut de premier niveau (Tier One) de risque de la cybermenacepour les intérêts britanniques. Le Gouvernement y expose sa volonté déterminée de lutter contre les cybermenaces et de « mettre en place des mesures sévères et inédites, dignes d'un leader mondial de la cybersécurité ». La Stratégie nationale de cybersécurité donne une forme concrète à cet engagement.

2.6. Le Gouvernement inscrit cette nouvelle stratégie dans le prolongement des réalisations, objectifs et jugements de la première Stratégie nationale de cybersécurité, initiative quinquennale lancée en 2011. Au cours de cette période, le Gouvernement a investi 860 millions GBP (plus d'un milliard d'euros) et se félicite des résultats obtenus. Les politiques, institutions et initiatives développées ces cinq dernières années ont aidé le Royaume-Uni à s'affirmer parmi les leaders mondiaux de la cybersécurité.

2.7. Ces fondations sont donc solides. Pour autant, la persistance et l'ingéniosité de ceux qui nous menacent, la prévalence de nos vulnérabilités et les lacunes dans nos capacités et nos défenses, nous forcent à redoubler d'efforts pour rester en phase avec la menace. Seule l'adoption d'une approche holistique, nous permettra de sécuriser efficacement nos cyberintérêts. Notre volonté de continuer d'investir et d'intervenir repose sur les analyses suivantes :

• compte tenu de l'ampleur et du caractère dynamique des cybermenaces, de notre

vulnérabilité et de notre dépendance, le maintien de l'approche actuelle ne suffira pas pour assurer notre sécurité ;
• la promotion de l'hygiène informatique fondée sur le marché n'a produit ni le rythme ni l'échelle de changement requis ; en conséquence, il incombe à l'État de montrer la voie et d'intervenir de manière plus directe en usant de son influence et de ses ressources pour lutter contre les cybermenaces ;
• seul, le Gouvernement ne peut pas pourvoir à tous les aspects de la cybersécurité de la Nation. Une approche intégrée et durable, par laquelle les citoyens, les entreprises, les autres acteurs de la société et l'État contribuent pleinement à l'effort de sécurisation de nos réseaux, services et données, s'impose ;
• le Royaume-Uni a besoin d'un secteur de la cybersécurité dynamique, soutenu par un socle de compétences capable de rester en phase avec la menace évolutive, voire de l'anticiper.

**PORTÉE DE LA STRATÉGIE**

2.8. Cette stratégie a été conçue pour façonner la politique du Gouvernement, tout en proposant une vision cohérente et convaincante aux secteurs public et privé, à la société civile, aux milieux universitaires et à l'ensemble de la population.

2.9. La stratégie couvre l'ensemble du Royaume-Uni. Le Gouvernement britannique cherchera à faire en sorte qu'elle soit mise en œuvre sur tout le territoire, sachant que, dans la mesure où elle touche à des domaines décentralisés, il lui faudra travailler en étroite collaboration avec les gouvernements décentralisés, pour assurer son application en Écosse, au Pays de Galles et en Irlande du Nord (en respectant les trois instances juridiques différentes et les quatre systèmes éducatifs du Royaume-Uni). Les propositions définies dans cette stratégie et se rapportant à des domaines décentralisés, feront l'objet d'une mise en œuvre convenue avec ces gouvernements, conformément aux accords de décentralisation.

2.10. La stratégie présente les mesures proposées ou préconisées à destination de tous les secteurs de l'économie et de la société, des ministères du gouvernement central aux capitaines d'industrie, en passant par les particuliers. Son but est d'accroître la cybersécurité à tous les échelons pour notre bien commun. Elle servira de base au dialogue international du Royaume-Uni, pour promouvoir une bonne gouvernance de l'Internet.

2.11. Dans cette stratégie, le terme « cybersécurité » se rapporte à la protection des systèmes d'information (matériel informatique, logiciels et infrastructures connexes), des données stockées et des services qu'ils fournissent contre les accès non autorisés, préjudices ou utilisations abusives. Font partie de ces préjudices les dommages causés délibérément par l'opérateur du système, ou accidentellement, suite au non-respect des procédures de sécurité.

2.12. Conformément à notre analyse du défi à relever et dans le prolongement des réalisations de la stratégie 2011, le présent document couvre les points suivants :
• notre bilan à jour du contexte stratégique, notamment des menaces actuelles et évolutives : les acteurs qui constituent le plus grand risque pour nos intérêts et les moyens dont ils disposent ;
• un bilan des vulnérabilités et de leur évolution au cours des cinq dernières années ;
• la vision du Gouvernement à l'horizon 2021 en matière de cybersécurité et les grands objectifs pour la concrétiser, principes directeurs, rôles et responsabilités inclus et savoir comment et où son intervention fera une différence ;

• la façon dont nous entendons mettre notre politique en pratique : domaines dans lesquels l'État prendra les rênes et dans lesquels nous prévoyons d'agir en partenariat avec d'autres acteurs et
• la manière dont nous prévoyons d'évaluer nos progrès vers nos objectifs.

# 3. CONTEXTE STRATÉGIQUE

3.1. À l'époque de la publiation de la dernière Stratégie nationale de cybersécurité en 2011, l'ampleur et les incidences des progrès des technologies étaient déjà apparentes. Depuis, les tendances et opportunités décrites se sont accélérées. De nouvelles technologies et applications sont apparues, et la démocratisation mondiale des technologies liées à l'Internet, surtout dans les pays en développement, a multiplié les opportunités de développement économique et social. Ces tendances ont été ou seront porteuses d'avantages considérables pour des sociétés connectées comme les nôtres. Toutefois, plus notre dépendance vis-à-vis des réseaux s'intensifie au Royaume-Uni comme à l'étranger, plus les opportunités pour ceux qui cherchent à compromettre nos systèmes et nos données se multiplient également. De même, le paysage géopolitique a évolué. Les activités malveillantes en ligne se jouent des frontières internationales. Les acteurs étatiques testent leurs cybercapacités offensives. Les cybercriminels diversifient leurs efforts et étendent leurs modes opératoires stratégiques pour extorquer aux citoyens, organisations et institutions britanniques, des sommes toujours plus importantes. Les terroristes et leurs sympathisants montent de petits attentats, tout en ambitionnant de commettre des actes plus percutants. Dans ce chapitre, nous évaluons la nature de ces menaces, nos vulnérabilités et comment elles continuent d'évoluer.

**MENACES**

**Cybercriminels**

3.2. Cette stratégie traite la cybercriminalité dans le contexte de deux formes d'activité criminelle interconnectées :

• les délits cyberdépendants —infractions nécessitant obligatoirement le recours à des dispositifs issus des technologies de l'information et de la communication (TIC), dans des situations où les appareils sont à la fois l'instrument utilisé pour commettre l'infraction et la cible de l'infraction (par exemple, développement et propagation de logiciel malveillant pour de l'argent, piratage informatique pour voler, endommager, fausser ou détruire des données, un réseau ou une activité) et
• les délits en ligne — infractions classiques dont l'échelle ou la portée peuvent être augmentées en recourant aux ordinateurs, réseaux d'ordinateurs ou à d'autres formes de TIC (fraude et vol de données en ligne, par exemple).

3.3. La majeure partie des cyberdélits ciblant le Royaume-Uni — principalement la fraude, le vol et l'extorsion — est encore surtout commise par des groupes criminels organisés de langue russe opérant depuis l'Europe de l'Est, dans un contexte où beaucoup de services criminels axés sur le marché sont hébergés dans ses pays. Toutefois, la menace émane également d'autres pays et régions ainsi que de l'intérieur du Royaume-Uni, sachant que l'Asie du Sud et l'Afrique de l'Ouest constituent actuellement une menace émergente de plus en plus préoccupante.

3.4. Les services répressifs britanniques et internationaux, qui repèrent des individus clés responsables des activités cybercriminelles les plus préjudiciables à l'encontre du Royaume-Uni, ont souvent du mal à les poursuivre en justice, s'ils se situent dans une juridiction où les accords d'extradition sont limités voire inexistants.

3.5. Ces groupes criminels organisés sont principalement responsables du développement et du déploiement des logiciels malveillants de plus en plus sophistiqués, qui infectent les ordinateurs de nos citoyens, de nos entreprises et de notre administration. Même si leurs retombées se dispersent dans tout le Royaume-Uni, leur effet cumulatif est loin d'être négligeable. Ces attaques se font de plus en plus agressives et conflictuelles, comme l'illustre le recours croissant au *ransomware* ou rançonlogiciel et aux menaces de déni de service distribué (DDoS) à des fins d'extorsion.

3.6. Si les groupes criminels organisés présentent une menace significative pour notre prospérité et notre sécurité collectives, la menace persistante émanant d'actes de cybercriminalité moins ingénieux, mais répandus, perpétrés contre les particuliers ou les petites organisations est tout aussi inquiétante.

Les escroqueries bancaires en ligne, qui concernent les prélèvements frauduleux effectués par le biais des services en ligne des établissements bancaires des clients victimes, ont augmenté de 64 % en 2015, s'élevant à 133,5 millions GBP (environ 157 m €). Selon l'organisation *Financial Fraud Action UK*, la progression moins rapide du nombre de cas ( 23 %), prouve que les délinquants ont de plus en plus tendance à cibler les clients commerciaux et disposant d'un patrimoine net important.

**Menaces émanant d'États ou soutenues par des États**

3.7. Le Royaume-Uni fait régulièrement l'objet de tentatives de la part d'États ou de groupes soutenus par un État, de pénétrer sur ses réseaux pour en tirer des avantages politique, diplomatique, technologique, commercial et stratégique en ciblant surtout les secteurs de l'administration, de la défense, de la finance, de l'énergie et des télécommunications.

3.8. Les capacités et l'impact de ces cyberprogrammes d'État varient. Les nations les plus avancées continuent d'améliorer leurs capacités à un rythme soutenu, intégrant des services de chiffrement et d'anonymisation à leurs outils afin de rester secrètes. Bien qu'elles disposent des moyens techniques nécessaires pour se livrer à des attaques très élaborées, elles atteignent souvent leurs buts à l'aide d'outils et de techniques de base dirigés contre des cibles vulnérables, tant les moyens de défense de leurs victimes sont faibles.

3.9. Seuls quelques États disposent des capacités techniques nécessaires pour constituer une grave menace pour la sécurité et la prospérité globales du Royaume-Uni. Toutefois, beaucoup d'autres s'emploient à mettre au point des cyberprogrammes sophistiqués susceptibles, dans un avenir proche, de constituer une véritable menace pour les intérêts britanniques. Les États qui cherchent à développer leurs capacités de cyberespionnage peuvent se procurer, en vente libre, des outils d'exploitation de réseaux informatiques et les recycler à des fins d'espionnage.

3.10. Outre la menace d'espionnage, une poignée d'acteurs étrangers hostiles a mis au point et déployé des cybercapacités offensives, dont certaines sont aussi destructrices. Ces capacités menacent la sécurité des infrastructures nationales critiques et des systèmes de contrôles industriels britanniques. Certains États pourraient utiliser ces capacités en violation du droit international, convaincus de leur impunité relative et encourageant d'autres auteurs potentiels à les émuler. Les attaques destructrices demeurent rares à travers le monde, mais leur nombre et leur impact sont en hausse.

**Terroristes**

3.11. Les groupes terroristes continuent d'aspirer à mener des activités en ligne nuisibles, à l'encontre du Royaume-Uni et de ses intérêts. Les capacités techniques actuelles des terroristes sont jugées faibles. Pour autant, l'activité en date subie par le Royaume-Uni jusqu'à maintenant, fût-elle de faible capacité, s'est avérée disproportionnellement élevées : simples dégradations et activités de doxing (révélation en ligne de données personnelles piratées) permettant aux groupes terroristes et à leurs sympathisants d'attirer l'attention des médias et d'intimider leurs victimes.

« L'exploitation de l'Internet par des terroristes à leurs propres fins n'équivaut pas à du cyberterrorisme. Toutefois, compte tenu de leur présence de plus en plus incontournable dans le cyberespace et de la disponibilité de la cybercriminalité en tant que service, nous n'aurions pas tort de supposer qu'ils pourraient avoir les moyens de lancer des cyberattaques »

ENISA Paysage des menaces 2015

3.12. Dans l'immédiat, les attentats terroristes physiques plutôt que numériques, resteront dans l'immédiat la priorité des groupes terroristes. Au fur et mesure qu'une génération maîtrisant de mieux en mieux l'outil informatique s'engage dans l'extrémisme, échangeant peut-être des compétences techniques avancées, nous nous nous attendons à ce que les activités déstabilisatrices peu élaborées (dégradation ou DDoS) se multiplient à l'encontre du Royaume-Uni. La possibilité de voir apparaître un certain nombre d'extrémistes solitaires compétents se fera, elle aussi, de plus en plus réelle, tout comme le risque qu'une organisation terroriste cherche à recruter un initié établi. Les terroristes emploieront probablement n'importe quelle cybercapacité afin d'en maximiser les effets potentiels. Par conséquent, même une augmentation modeste des capacités des terroristes pourrait constituer une menace significative pour le Royaume-Uni et ses intérêts.

**Hacktivistes**

3.13. Les groupes hacktivistes sont décentralisés et axés sur un problème. Ils forment et sélectionnent leurs cibles en réaction à des injustices perçues, parant souvent leurs actes d'un élément d'autodéfense. Si la majorité des cyberactivités des hacktivistes sont de nature perturbatrice (dégradation de sites web ou DDoS), les hacktivistes les plus doués sont capables d'infliger des dommages plus importants et plus durables à leurs victimes.

**LES INITIÉS**

Les menaces internes continuent de grever les organisations du Royaume-Uni. En effet, les initiés malveillants, salariés à qui une organisation fait confiance et qui ont accès à ses systèmes et données critiques, posent la plus grande menace. Ils peuvent porter atteinte à ses finances et à sa réputation, en volant ses données sensibles et sa propriété intellectuelle. Ils peuvent en outre constituer une cybermenace destructrice, s'ils décident de mettre leurs connaissaces et accès privilégiés, au service d'une attaque visant à perturber ou dégrader les services critiques hébergés par le réseau d'entreprise, ou encore à effacer les données du réseau.

Les initiés ou employés qui provoquent des dommages numériques accidentellement en cliquant par inadvertance sur un email d'hameçonnage, en insérant une clé USB infectée dans un ordinateur ou en ne respectant pas les procédures de sécurité et en téléchargeant des contenus dangereux sur Internet, sont tout aussi préoccupants. Bien qu'ils n'aient pas l'intention de porter préjudice à leur entreprise, leur accès

privilégié à ses systèmes et données rend leurs actes tout aussi nuisibles que ceux d'un employé malveillant. Ces individus sont souvent victimes de l'ingénierie sociale — ils peuvent involontairement donner à un escroc l'accès aux réseaux de leur entreprise ou suivre, en toute bonne foi des instructions qui profitent au fraudeur.

Le cyberrisque global que court une organisation suite à des menaces internes, ne concerne pas seulement l'accès non autorisé aux systèmes informatiques et à leur contenu. Les contrôles de sécurité physique protégeant ces systèmes contre un accès inapproprié, ou le prélèvement de données sensibles ou de renseignements exclusifs sur différentes formes de supports sont tout aussi importants. De même, une culture robuste de la sécurité du personnel, consciente des menaces que représentent les employés mécontents, le vol parmi les effectifs et l'espionnage, industriel ou autre, comptent parmi les éléments importants d'une approche holistique en matière de sécurité.

**« Script kiddies »**

3.14. Les « script kiddies » — nom donné dans les pays anglophones aux individus généralement peu qualifiés, qui exploitent des scripts ou des programmes développés par d'autres pour lancer des cyberattaques — ne sont pas considérés comme présentant une menace significative pour l'économie ou la société au sens large. Ils ont cependant accès à des guides, ressources et outils de piratage informatique sur Internet. En raison des vulnérabilités des systèmes connectés à l'Internet utilisés par un grand nombre d'organisations, les actions des « script kiddies » peuvent, dans certains cas, avoir pour elles des conséquences d'une gravité disproportionnée.

**ÉTUDE DE CAS 1 : PIRATAGE CHEZ TALKTALK**

Le 21 octobre 2015, l'opérateur de services de télécommunications britannique TalkTalk signalait une cyberattaque réussie et la violation possible des données personnelles de ses clients. L'enquête menée à la suite de cette attaque a révélé qu'une base de données contenant les informations sur la clientèle avait été consultée via des serveurs internet publics, compromettant les dossiers d'environ 157 000 clients et notamment leurs noms, adresses et coordonnées bancaires.

Le même jour, plusieurs salariés de TalkTalk ont reçu un email leur demandant une rançon en Bitcoins, les détails fournis par les agresseurs sur la structure de la base de données prouvant apparemment qu'elle avait bel et bien été compromise.

En signalant ce délit à la police, épaulée par les experts de l'Agence britannique de lutte contre le crime organisé, TalkTalk l'a aidé à appréhender les principaux suspects, dont tous étaient domiciliés au Royaume-Uni, en octobre et novembre 2015.

Cette attaque montre que les vulnérabilités peuvent persister, même au sein de grandes organisations sensibilisées à la cybercriminalité. Leur exploitation peut avoir une incidence négative disproportionnée sur la réputation et la continuité des opérations, sans oublier l'intérêt médiatique considérable généré par cet incident. La communication rapide de ce délit par TalkTalk a permis aux services répressifs d'intervenir rapidement, pour permettre au public et à l'administration de limiter les pertes potentielles de données sensibles. L'incident a coûté à TalkTalk environ 60 millions GBP (70 m €) et la perte de 95 000 clients, ainsi qu'une chute brutale du cours de son action.

**ÉTUDE DE CAS 2 : ATTAQUE DU SYSTÈME SWIFT DE LA BANGLADESH BANK**

La Société mondiale de télécommunications financières interbancaires (SWIFT) fournit un

réseau qui permet aux institutions financières du monde entier, d'envoyer et de recevoir en toute sécurité des informations sur les transactions financières. Dans la mesure où SWIFT transmet des ordres de paiement qui doivent être réglés par des comptes correspondants détenus par les institutions entre elles, la possibilité que ce processus soit compromis par des cybercriminels ou d'autres acteurs malveillants qui chercheraient à lancer des ordres de paiement illicites sur le système ou, pire, qui tenteraient de désactiver ou de perturber la fonctionnalité du réseau SWIFT lui-même, a longtemps préoccupé.

Début février 2016, un assaillant a accédé au système de paiement SWIFT de la Bangladesh Bank et donné ordre à la banque fédérale de réserve de New York, de virer de l'argent du compte de la Bangladesh Bank sur des comptes domiciliés aux Philippines. Cette tentative de vol s'élevait à 951 millions USD (environ 873 m €). Le système bancaire a empêché 30 transactions d'une valeur estimée de 850 millions USD (780 m €), mais cinq transactions d'un montant de 101 millions USD (91 m €) ont été effectuées. 20 millions USD (18,36 m €), localisés au Sri Lanka, ont depuis été récupérés. Les 81 millions USD (74,34 m €) restants virés aux Philippines ont été blanchis par des casinos. Une partie de cette somme a par la suite été expédiée à Hong Kong.

L'enquête judiciaire lancée par la Bangladesh Bank a révélé qu'un logiciel malveillant avait été installé sur les systèmes de la banque, pour recueillir des renseignements sur ses procédures de paiement international et de transfert de fonds. Une analyse plus approfondie exécutée par BAE Systems sur le logiciel malveillant lié à cette attaque, a révélé une fonctionnalité élaborée d'interaction avec l'interface SWIFT Alliance Access installée dans l'infrastructure de la Bangladesh Bank. BAE a conclu son enquête en déclarant que « des criminels lancent des attaques de plus en plus élaborées contre les organisations victimes, surtout dans le domaine des intrusions sur les réseaux ».

**ÉTUDE DE CAS 3 : ATTAQUE DU RÉSEAU ÉLECTRIQUE EN UKRAINE**

Le 23 décembre 2015, une cyberattaque lancée sur les compagnies de distribution d'électricité ouest-ukrainiennes Prykarpattya Oblenergo et Kyiv Oblenergo a provoqué une énorme panne d'alimentation, perturbant plus de 50 sous-stations électriques des réseaux de distribution. La région aurait apparemment été touchée par un blackout de plusieurs heures, beaucoup d'autres clients et régions ayant souffert de perturbations du réseau moins importantes, touchant plus de 220 000 consommateurs.

Certains ont imputé cette attaque au logiciel malveillant BlackEnergy3, suite à l'identification d'échantillons sur le réseau. Six mois au moins avant l'attaque, les assaillants avaient envoyé des emails d'hameçonnage contenant des documents Microsoft Office malveillants aux sièges de ces compagnies d'électricité ukrainiennes. Toutefois, il est peu probable que le maliciel ait ouvert les coffrets des disjoncteurs à l'origine de la panne. En revanche, il est probable que le logiciel malveillant ait permis aux assaillants de recueillir des justificatifs d'identité pour contrôler directement à distance certains aspects du réseau, ce qui par la suite leur aurait permis de déclencher la panne.

L'incident ukrainien est le premier cas avéré de perturbation d'un réseau de transport d'électricité par cyberattaque. De tels cas démontrent une fois de plus la nécessité de prévoir de bonnes pratiques de cybersécurité sur l'ensemble de notre infrastructure critique nationale, afin d'empêcher l'occurrence d'incidents similaires au Royaume-Uni.

## VULNÉRABILITÉS

### Un arsenal de dispositifs évolutif

3.15. À l'époque de la publication de ladernière Stratégie nationale de cybersécurité en 2011, la cybersécurité qualifiait pour la plupart d'entre nous, la protection de terminaux comme les ordinateurs de bureaux et portables. Depuis, l'Internet s'est installé de plus en plus fermement dans notre vie quotidienne, sans même que nous nous en rendions toujours compte. L'Internet des objets crée de nouvelles opportunités d'exploitation et augmente l'impact potentiel des attaques, lesquelles peuvent se solder par des dégâts physiques, dommages corporels et, dans le pire des cas, des pertes humaines.

3.16. La mise en œuvre rapide de la connectivité dans les processus de contrôle industriel des systèmes critiques et dans toutes sortes de secteurs (énergétique, minier, agricole, aéronautique, etc.), a entraîné la création de l'Internet des objets industriel. Ce dernier augmente simultanément les possibilités de piratage et d'altération d'appareils et de processus qui auparavant ne craignaient pas ce genre d'intrusions, avec des conséquences potentiellement catastrophiques.

3.17. Ainsi, nous ne sommes plus simplement vulnérables face à des dommages numériques causés par le manque de cybersécurité sur nos propres terminaux, mais par des menaces pesant sur l'interconnexion des systèmes fondamentaux pour notre société, notre santé et notre bien-être.

### Hygiène et conformité informatiques lacunaires

3.18. La sensibilisation aux vulnérabilités techniques des logiciels et des réseaux, au même titre que l'importance vitale de l'hygiène informatique au Royaume-Uni, ont indéniablement augmenté ces cinq dernières années et ce en partie suite à des initiatives comme « 10 Steps to Cyber Security » (10 pas vers la cybersécurité) mise en place par le Gouvernement, mais aussi à la visibilité accrue des cyberincidents majeurs touchant les États et les sociétés. Les cyberattaques ne sont pas forcément élaborées ou inévitables. Elles découlent en outre souvent de l'exploitation de vulnérabilités – pourtant aisément rectifiables et, souvent, évitables. Dans la plupart des cas, la vulnérabilité de la victime est le facteur déterminant du succès d'une cyberattaque, pas l'ingéniosité de l'assaillant. Même si les entreprises et organisations décident où et comment investir dans leur cybersécurité sur la base d'une analyse coût-bénéfice, elles n'en sont pas moins, au final, responsables de la sécurité de leurs données et de leurs systèmes. Les entreprises doivent trouver l'équilibre entre le risque que constituent les cyberattaques pour leurs systèmes vitaux, leurs données sensibles et des investissements suffisants dans leur capital humain, leurs moyens technologiques et leur gouvernance, pour se donner les chances de réduire leur exposition aux préjudices potentiels liés au cyberespace.

« Aucun système de sécurité informatique imaginable ne peut empêcher une personne sur cent d'ouvrir un email d'hameçonnage, et il n'en faut parfois pas plus. »

Ciaran Martin, Directeur général de la cybersécurité, GCHQ, juin 2015

### Insuffisance des formations et compétences

3.19. Nos compétences et nos connaissances ne suffisent pas pour répondre aux besoins de cybersécurité des secteurs public et privé. Dans les entreprises, beaucoup de salariés n'ont aucune notion de cybersécurité et ne

comprennent pas leurs responsabilités à cet égard, du fait en partie d'un manque d'apprentissage formel. Le public n'est quant à lui, pas assez conscient des cyberrisques.

« L'an dernier, un peu moins d'un cinquième des entreprises ont fait suivre à leur personnel une formation à la cybersécurité. »
Enquête sur les atteintes à la cybersécurité, 2016

3.20. Nous devons par ailleurs développer les compétences et les capacités spécialisées, qui nous permettront de rester en phase avec l'évolution rapide des technologies et de gérer les cyberrisques en découlant. Ce déficit de compétences représente une vulnérabilité nationale qui doit être traitée.

**Systèmes hérités et non corrigés**

3.21. Un nombre important d'organisations du Royaume-Uni continuent d'exploiter des systèmes hérités vulnérables, jusqu'à la prochaine mise à niveau informatique. Les logiciels installés sur ces systèmes dépendent souvent de versions anciennes et non corrigées. Or, ces versions plus anciennes souffrent souvent de vulnérabilités recherchées par les pirates, équipés des outils nécessaires pour les exploiter. L'utilisation par certaines organisations de logiciels non pris en charge, pour lesquels ils n'existent pas de régime correctif, est un autre problème.

« Nous avons récemment analysé 115 000 dispositifs Cisco sur Internet et sur les environnements clients, de manière à mettre en évidence les risques sécuritaires que présentent les infrastructures vieillissantes — et le manque d'attention accordée aux vulnérabilités des versions non patchées… Nous avons découvert que, sur ces 115 000 dispositifs, le logiciel exécuté sur 106 000 d'entre eux présentait des vulnérabilités connues. »
Rapport annuel sécurité Cisco 2016

**Disponibilité des ressources de piratage informatique**

3.22. La disponibilité évidente des informations sur le piratage informatique et des outils de piratage conviviaux sur Internet, facilite la tâche des pirates potentiels. Les renseignements dont ils ont besoin pour piéger leurs victimes sont souvent en accès libre et récupérables rapidement. Du salon à la salle de réunion, chacun doit savoir dans quelle mesure ses coordonnées et systèmes sont exposés sur Internet et à quel point cette exposition risque de le rendre vulnérable, en cas de tentative de cyber-exploitation.

« Dans 99,9 % des cas, les vulnérabilités exploitées sur les supports compromis, l'ont été plus d'un an après la publication de la vulnérabilité. »
Rapport d'enquête sur les atteintes aux données Verizon 2015

**CONCLUSIONS**

3.23. Le Royaume-Uni a suivi des politiques et mis en place des institutions qui ont amélioré les défenses du pays et, en partie, atténué la menace indissociable du cyberespace.

3.24. Toutefois, nous ne la maîtrisons pas encore. Les types de cyber-acteurs malveillants auxquels nous avons affaire, et leurs motivations, ont largement persisté, dans un contexte où les logiciels malveillants et ces acteurs nuisibles se sont rapidement multipliés. Nos ennemis les plus techniquement compétents, à savoir un nombre restreint d'États et de cybercriminels d'élite, ont renforcé leurs capacités. Il nous appartient de veiller à ce que nos défenses soient suffisamment évoluées, suffisamment agiles pour les contrer, d'entraver les ambitions d'attaque des acteurs malveillants et de traiter les causes profondes des vulnérabilités évoquées plus haut. Tel est notre défi collectif.

# 4. RIPOSTE NATIONALE

4.1. Pour atténuer les multiples menaces auxquelles nous sommes confrontés et protéger nos intérêts dans le cyberespace, une approche stratégique capable d'étayer les mesures collectives et individuelles prises dans le domaine numérique au cours des cinq prochaines années s'impose. Ce chapitre est consacré à notre vision et à cette approche.

**NOTRE VISION**

4.2. Notre vision à l'horizon 2021 envisage un **Royaume-Uni sécurisé, résilient face aux cyber-menaces, prospère et confiant dans le monde numérique**.

4.3. Afin de concrétiser cette vision, nous nous nous efforcerons d'atteindre les objectifs suivants :

• **DÉFENDRE** Nous disposons des moyens nécessaires pour défendre le Royaume-Uni contre les cybermenaces évolutives, intervenir efficacement en cas d'incident, veiller à la protection et à la résilience des réseaux, données et systèmes britanniques. Les citoyens, les entreprises et le secteur public disposent des connaissances et capacités nécessaires pour se défendre.

• **DISSUADER** Le Royaume-Uni sera une cible difficile pour toutes les formes d'agression dans le cyberespace. Nous détectons, comprenons, enquêtons sur les manœuvres hostiles menées à notre encontre et les perturbons, recherchons et poursuivons en justice leurs auteurs. Nous sommes équipés pour prendre, si nous choisissons de le faire, des mesures offensives dans le cyberespace.

• **DÉVELOPPER** Innovant et en plein essor, notre secteur de la cybersécurité est étayé par des travaux de recherche et de développement scientifiques de rang mondial. Notre vivier de talents autosuffisant, nous fournit les compétences nécessaires pour répondre aux besoins des secteurs public et privé à l'échelle nationale. Nos capacités d'analyse et notre expertise de pointe permettront au Royaume-Uni non seulement de faire face, mais aussi de surmonter les menaces et défis futurs.

4.4. Pour étayer ces objectifs, nous mènerons une **ACTION INTERNATIONALE**. Nous exercerons notre influence en investissant dans les partenariats qui façonnent l'évolution mondiale du cyberespace, de manière à promouvoir nos intérêts économiques et sécuritaires au sens large.

**PRINCIPES**

4.5 Pour réaliser ces objectifs, le Gouvernement appliquera les principes suivants :

• nos actions et nos politiques seront motivées par la double nécessité de protéger nos citoyens et de mieux assurer notre prospérité ;
• nous accorderons la même importance aux cyberattaques déclenchées sur notre territoire, qu'aux attaques conventionnelles équivalentes et nous défendrons en conséquence ;
• nous agirons dans le respect du droit national et international et attendrons des autres qu'ils en fassent autant ;
• nous protégerons et défendrons rigoureusement nos valeurs fondamentales : démocratie, primauté du droit, liberté, ouverture et obligation redditionnelle des administrations publiques et institutions, droits de l'homme et liberté d'expression ;

• nous préserverons et protégerons la vie privée des citoyens britanniques ;
• nous agirons en partenariat. Seule la coopération avec les administrations décentralisées, les diverses branches du secteur public, les entreprises, les institutions et le citoyen individuel nous permettra de sécuriser le Royaume-Uni dans le cyberespace ;
• le Gouvernement assumera ses responsabilités et dirigera la riposte nationale. Les entreprises, organisations et particuliers n'en sont pas moins tenus de prendre des mesures raisonnables pour se protéger en ligne, assurer leur résilience et leur capacité d'assurer la continuité de leurs opérations en cas d'incident ;
• la responsabilité de la sécurité des organisations de l'ensemble du secteur public, y compris de la cybersécurité et de la protection des données et des services en ligne, relève des ministres, secrétaires permanents et conseils d'administration respectifs ;
• nous n'accepterons pas que le public et l'ensemble du pays courent un risque important, parce que des entreprises et des organisations n'auront pas pris les mesures nécessaires pour gérer les cybermenaces ;
• nous travaillerons en étroite collaboration avec les pays qui partagent nos points de vue et avec lesquels nos préoccupations de sécurité se rejoignent, conscients que les menaces informatiques ne connaissent aucune frontière. Nous coopérerons globalement avec nos divers partenaires internationaux, afin d'influencer le grand public, en reconnaissant la valeur des larges coalitions et
• afin de veiller à ce que les interventions de l'État aient une incidence réelle sur la cybersécurité et la résilience nationales globales, nous nous efforcerons de définir, d'analyser et de présenter des données qui mesurent l'état de notre cybersécurité collective et de notre avancement vers la réalisation de nos buts stratégiques.

**RÔLES ET RESPONSABILITÉS**

4.6. La sécurisation du cyberespace national nécéssite un effort collectif. Nous avons tous et sans exception, un rôle important à jouer.

**Particuliers**

4.7. En tant que citoyens, salariés et consommateurs, nous prenons des mesures pratiques, pour protéger les biens auxquels nous sommes attachés dans le monde physique. Le réflexe doit être le même dans le monde virtuel. Ainsi devons-nous assumer notre responsabilité personnelle et prendre toutes les mesures adéquates, pour protéger non seulement notre matériel informatique — nos smartphones et autres terminaux —, mais aussi les données, logiciels et systèmes dont nous tirons la liberté, la souplesse et la commodité auxquels nous nous sommes habitués dans nos vies privée et professionnelle.

**Entreprises et organisations**

4.8. Les entreprises, organisations des secteurs public et privé et autres institutions, détiennent des données personnelles, s'acquittent de prestations et exploitent des systèmes dans le domaine numérique. La connectivité de ces informations a révolutionné leurs opérations. Cette mutation technologique est cependant assortie de la responsabilité de protéger leurs actifs, maintenir leurs services et doter leurs produits duégrer niveau de sécurité qui convient. Le citoyen, le consommateur et l'ensemble de la société, attendent des entreprises et des organisations qu'elles prennent toutes les mesures adéquates pour protéger leurs données à caractère personnel et intègrent la résilience — autrement dit la capacité de résistance et de récupération — aux systèmes et structures auxquels ils se fient. De plus, ces entités doivent comprendre

que les entreprises et organisations victimes d'une cyberattaque, sont responsables de ses conséquences.

**Gouvernement**

4.9. Le premier devoir du Gouvernement est de défendre le territoire contre les attaques déclenchées par d'autres États, protéger les citoyens et l'économie de tout préjudice et d'établir le cadre de travail national et international visant à protéger nos intérêts, nos droits fondamentaux et à traduire en justice les criminels.

4.10. À la fois dépositaire d'importantes données et prestataire de services, le Gouvernement prend des mesures rigoureuses pour protéger les actifs informatiques dont il a la charge. Autre responsabilité importante, il lui appartient également de conseiller et d'informer les citoyens et organisations des mesures à prendre pour se protéger en ligne et si nécessaire, de définir les normes auxquelles les grandes entreprises et organisations sont censées se conformer.

4.11. Bien que certains secteurs clés de notre économie soient privés, le Gouvernement n'en est pas moins responsable d'assurer leur résilience nationale et, avec ses partenaires de toute l'administration, le maintien des services et fonctions essentiels de l'ensemble de l'administration publique.

**Moteur du changement : le rôle du marché**

4.12. La Stratégie et le Programme national de cybersécurité de 2011 cherchaient à multiplier les résultats, accroître les capacités dans les secteurs public et privé et comptait sur le marché pour induire les bons comportements. Nous espérions que les pressions commerciales et les incitations émanant du gouvernement, garantiraient des investissements d'entreprises adéquats dans des moyens de cybersécurité appropriés, stimuleraient le flux d'investissement vers notre secteur industriel et encourageraient la création d'un vivier de compétences dans ce secteur.

4.13. De grands progrès ont été réalisés. L'économie et la société en général, sont plus conscientes du risque et des mesures nécessaires pour atténuer le cyberrisque qu'il y a cinq ans. Toutefois, l'alliance des forces du marché et de l'encouragement de l'État n'a pas suffi en elle-même, pour sécuriser suffisamment rapidement nos intérêts à long terme dans le cyberespace. Trop de réseaux, y compris dans des secteurs critiques, sont encore vulnérables. Le marché n'évalue pas et donc ne gère pas correctement le cyberrisque. Trop d'organisations sont encore victimes d'atteintes et qui plus est, même au niveau le plus élémentaire. Les investisseurs disposés à risquer leur argent pour accompagner les entrepreneurs dans le secteur sont trop rares. Les filières d'enseignement et de formation ne produisent pas suffisamment de diplômés et autres détenteurs des compétences requises.

4.14. Le marché n'en est pas redondant pour autant. À long terme, sa contribution dépassera largement celle du Gouvernement dans ce domaine. Toutefois, compte tenu de l'imminence de la menace qui pèse sur le Royaume-Uni et des vulnérabilités croissantes de notre environnement numérique, le Gouvernement doit prendre des mesures à court terme plus percutantes.

**Moteur du changement : un rôle élargi pour le Gouvernement**

4.15. Le Gouvernement doit donc donner le ton pour répondre aux besoins nationaux en matière de cybersécurité. Lui seul peut tirer parti des renseignements et des autres actifs, nécessaires pour défendre le pays contre les menaces les plus complexes. Lui seul peut

promouvoir la coopération des secteurs public et privé et veiller au partage réciproque de l'information. Le Gouvernement joue un rôle prépondérant, en concertation avec le secteur industriel, pour définir une cybersécurité efficace et garantir sa mise en œuvre.

4.16. Le Gouvernement améliorera considérablement la cybersécurité nationale au cours des cinq prochaines années. Ce programme ambitieux et transformateur s'articulera autour de quatre grands axes :

• **Moyens d'action et mesures d'incitation**. Le Gouvernement investira pour maximiser le potentiel d'un secteur britannique de la cybersécurité véritablement novateur. Pour ce faire, il soutiendra les jeunes entreprises et investira dans l'innovation. Il cherchera à identifier les talents, à favoriser leur épanouissement plus tôt dans l'enseignement et développera des filières plus précises d'entrée dans une profession qui doit être mieux définie. Le Gouvernement utilisera tous les moyens à sa disposition, dont le prochain Règlement général sur la protection des données (sigle anglais GDPR), pour renforcer les normes de cybersécurité dans l'économie, notamment par le biais de la réglementation si nécessaire.
• **Un service des renseignements élargi et des forces de l'ordre attentives à la menace**. Les agences du renseignement, le ministère de la Défense, la police et l'Agence britannique de lutte contre la criminalité, en coordination avec les agences internationales partenaires, élargiront leurs efforts pour identifier, anticiper et perturber les activités hostiles des acteurs étrangers, cybercriminels et terroristes. Cette lutte améliorera le recueil et l'exploitation du renseignement, dans le but d'obtenir un renseignement préventif sur les intentions et capacités de nos ennemis.
• **Développement et déploiement des technologies** en partenariat avec le secteur industriel ; mesures de cyberdéfense active pour approfondir notre compréhension de la menace, renforcer la sécurité des systèmes et réseaux des secteurs public et privé britanniques face à la menace, déstabiliser l'activité malveillante.
• **Le Centre national de la cybersécurité (sigle anglais NCSC)**. Le Gouvernement a créé un organe unique, central, de cybersécurité à l'échelon national. Chargé de la gestion des cyberincidents nationaux, il fera autorité en la matière et jouera le rôle de centre d'expertise en cybersécurité. Il proposera un appui et des conseils sur mesure aux ministères, administrations décentralisées, régulateurs et entreprises. Le NCSC analysera, détectera et comprendra les menaces informatiques. Son expertise en cybersécurité accompagnera le Gouvernement dans ses efforts pour encourager l'innovation, soutenir un secteur de la cybersécurité prospère et stimuler le développement des compétences en la matière. Fait singulier pour un établissement aussi public, son organisation de tutelle est le GCHQ (Centre national des communications). Cette filiation lui permet de tirer parti de l'expertise mondialement réputée et des moyens sensibles de cette organisation, pour apporter à notre économie et à la société au sens large un soutien encore plus efficace. Les ministères conserveront la responsabilité de la mise en œuvre efficace de ces recommandations en matière de cybersécurité.

« Compte tenu de l'échelle industrielle des vols de propriété intellectuelle commis dans nos entreprises et nos universités, ainsi que des nombreuses escroqueries par hameçonnage et logiciels malveillants qui font perdre du temps et de l'argent, le Centre national de la cybersécurité montre que le Royaume-Uni concentre ses efforts pour combattre les menaces qui existent en ligne. »

Robert Hannigan, Directeur de GCHQ, mars 2016

4.17. Nous devrons mobiliser des ressources supplémentaires, pour améliorer nos pratiques de cybersécurité et notre résilience. Dans son Bilan 2015 de la défense stratégique et de la sécurité, le Gouvernement consacre 1,9 milliard GBP (2,25 Mrd €) sur cinq ans à la concrétisation de ces engagements et objectifs.

## CENTRE NATIONAL DE LA CYBERSÉCURITÉ

Inauguré le 1er octobre 2016, le Centre national de la cybersécurité (NCSC) est une plateforme unique de création de partenariats efficaces dans le domaine de la cybersécurité, associant l'administration publique, l'industrie et le public et dont le but est de renforcer la sécurité en ligne du Royaume-Uni. Il interviendra en cas de cyberincident et sera la référence britannique en matière de cybersécurité. Pour la première fois, les secteurs clés pourront contacter directement le personnel du NCSC afin d'obtenir les meilleurs conseils et le meilleur soutien possible, pour protéger leurs réseaux et systèmes des cybermenaces.

Le NCSC est :

• une source unifiée de renseignements et d'assurance de l'information sur les menaces à la cybersécurité mise en place par l'État ;
• la représentation publique puissante de l'action du Gouvernement contre les cybermenaces — action menée de concert avec les industriels, les universitaires et les partenaires internationaux pour protéger le Royaume-Uni contre les cyberattaques et
• une organisation publique, affiliée à GCHQ pour tirer parti de renseignements nécessairement secrets et d'une expertise technique de renommée mondiale.

Les capacités du NCSC seront renforcées progressivement jusqu'à la fin de la période d'exécution de cette stratégie. Le Centre rassemble les capacités déjà développées par CESG — division sécurité de l'information de GCHQ —, le Centre de protection des infrastructures nationales (sigle anglais CPNI), CERT-UK (équipe d'intervention d'urgence informatique) et le Centre de cyber-évaluation (sigle anglais CCA) et nous permet de consolider les moyens les plus efficaces dont nous disposons déjà, tout en simplifiant considérablement les anciennes dispositions. Il se concentrera initialement sur les objectifs suivants :

• développer une capacité de gestion des incidents de rang mondial, pour réagir aux cyberincidents et en réduire les dommages — des attaques ne visant qu'une organisation, aux agressions nationales de grande envergure ;
• communiquer des moyens par lesquels les organisations des secteurs public et privé peuvent traiter les questions de cybersécurité facilitantle partage de l'information et
• continuer de fournir des avis d'expert sectoriel au Gouvernement et aux secteurs critiques tels que les télécommunications, l'énergie et les finances, ainsi que des conseils de cybersécurité à l'ensemble du Royaume-Uni.

Grâce au NCSC, le Gouvernement dispose d'un moyen efficace de concrétiser une grande partie de cette stratégie, sachant qu'au fur et à mesure de son évolution, ses objectifs et capacités devront s'adapter à de nouveaux défis et tenir compte des enseignements tirés.

# PLAN
# DE MISE EN ŒUVRE

Nos objectifs des cinq prochaines années pour développer la cybersécurité du pays sont ambitieux, à juste titre. Pour les atteindre, il nous faudra agir en conséquence et avec détermination sur l'ensemble du paysage numérique. Les mesures prises pour concrétiser la vision de l'État feront progresser les trois principaux objectifs de la stratégie : DÉFENDRE notre cyberespace, DISSUADER nos ennemis et DÉVELOPPER nos capacités, le tout dans le cadre d'une ACTION INTERNATIONALE efficace.

# 5. DÉFENDRE

5.0.1. Les éléments DÉFENDRE de cette stratégie ont pour but de garantir la résilience et la protection contre les cyberattaques, des réseaux, données et systèmes dans les sphères publique, privée et commerciale. Il serait aussi utopique de prétendre empêcher toutes les cyberattaques, que de croire à la possibilité de prevenir tous les délits. Toutefois, la mobilisation des citoyens, des prestataires d'enseignement, des universitaires, des entreprises et des autres gouvernements, permettra au Royaume-Uni de créer des niveaux de défense susceptibles de réduire significativement notre exposition aux cyberincidents, protéger nos actifs les plus précieux et nous permettre à tous d'évoluer avec succès et prospérité dans le cyberespace. D'autre part, notre sécurité collective ne peut que bénéficier d'une démarche visant à promouvoir la coopération entre les États et les bonnes pratiques de cybersécurité.

5.0.2. Le Gouvernement mettra en œuvre des mesures pour garantir aux citoyens, entreprises, institutions, organismes publics et privés l'accès aux informations utiles pour se défendre. Le Centre national de la cybersécurité est une source unifiée de renseignements et d'assurance de l'information sur les menaces, mise en place par l'État pour nous permettre de proposer des conseils personnalisés en matière de cyberdéfense et d'intervenir rapidement et efficacement en cas d'incidents majeurs dans le cyberespace. Le Gouvernement collaborera avec l'industrie et les partenaires internationaux, afin de définir les grands traits d'une cybersécurité efficace pour les secteurs public et privé, pour nos systèmes et services les plus importants et pour l'ensemble de l'économie. Nous intègrerons la sécurité par défaut, à tous les nouveaux systèmes de l'administration publique et vitaux. Les services répressifs travailleront en étroite collaboration avec l'industrie et le Centre national de la cybersécurité, pour fournir des renseignements dynamiques sur les menaces criminelles, donner à l'industrie les moyens de mieux se défendre et promouvoir des recommandations et normes de sûreté.

## 5.1. CYBERDÉFENSE ACTIVE

5.1.1. La cyberdéfense active (ACD) qualifie le principe de mise en œuvre de mesures de sécurité visant à renforcer un réseau ou un système, pour le rendre plus impénétrable en cas d'attaque. La cyberdéfense active évoque habituellement les analystes en cybersécurité qui, ayant compris la nature des menaces pesant sur leurs réseaux, conçoivent et mettent en œuvre des mesures pour les combattre en amont ou s'en protéger. Dans le contexte de cette stratégie, le Gouvernement a choisi d'appliquer le même principe à une plus grande échelle : il mettra à profit son expertise, ses capacités et son influence uniques pour transformer radicalement la cybersécurité nationale et réagir aux cybermenaces. Appliqué à notre statégie de défense, le terme « réseau » désigne l'ensemble du cyberespace britannique. Les activités proposées représentent un plan d'action défensive, fondé sur l'expertise du NCSC en sa qualité d'Autorité technique nationale capable de réagir aux menaces pesant sur le Royaume-Uni au niveau macro.

**Objectifs**

5.1.2. En déployant cette ACD, l'État vise à :

• faire du Royaume-Uni une cible beaucoup plus difficile pour les acteurs soutenus par un État et les cybercriminels, en renforçant la résilience des réseaux britanniques ;

• mettre en échec la vaste majorité des activités malveillantes à volume élevé et à faible complexité sur les réseaux britanniques, en bloquant les communications émanant de logiciels malveillants entre les hackeurs et leurs victimes ;
• adapter et augmenter la portée et l'ampleur des capacités du Gouvernement pour contrecarrer les menaces graves émanant d'États ou de cybercriminels ;
• protéger le trafic sur notre Internet et nos télécommunications contre les tentatives de piratage d'acteurs malveillants ;
• consolider la résistance aux cybermenaces des infrastructures critiques du pays et des services destinés à ses citoyens et
• perturber le modèle économique des assaillants de tous types, afin de les démotiver et réduire les dommages consécutifs aux attentats.

**Approche**

5.1.3. Pour réaliser ces objectifs, le Gouvernement :

• œuvrera avec l'industrie et surtout, avec les prestataires de services de communications, afin de rendre les services et les usagers d'Internet au Royaume-Uni beaucoup plus difficiles à attaquer, tout en réduisant considérablement le potentiel d'incidences durables sur le pays. Il s'agira entre autres de lutter contre l'hameçonnage, de bloquer les domaines et les adresses IP malveillantes et de prendre toute autre mesure capable de perturber les attaques aux maliciels. Des mesures visant à sécuriser l'infrastructure de télécommunications et de routage Internet britanniques, s'imposent également ;
• accroîtra l'échelle et accélérera le développement des moyens de GCHQ, du ministère de la Défense et de la NCA pour perturber les cybermenaces les plus graves pour le Royaume-Uni et notamment, les campagnes lancées par des cybercriminels ingénieux et des acteurs étrangers hostiles et
• protégera mieux les systèmes et les réseaux du gouvernement, aidera l'industrie à intégrer une plus grande sécurité dans la chaîne d'approvisionnement de l'infrastructure critique nationale, rendra l'écosystème des logiciels britanniques plus sûr et fournira des protections automatisées pour les services administratifs proposés en ligne aux citoyens.

5.1.4. Dans la mesure du possible, ces initiatives seront lancées par ou en partenariat avec l'industrie. Dans de nombreux cas, les industriels se chargeront de l'élaboration et de la direction de leur mise en œuvre, avec la contribution critique du Gouvernement sous forme de soutien d'experts, de conseils et de leadership intellectuel.

5.1.5. Pour les mettre en œuvre, le Gouvernement prendra par ailleurs des mesures précises, notamment :

• en coopérant avec les prestataires de services de communication pour bloquer les attaques de logiciels malveillants. Pour y parvenir, il limitera l'accès aux domaines et sites web spécifiques constituant des sources connues de logiciels malveillants : c'est le blocage ou filtrage du système de noms de domaine (DNS) ;
• en empêchant les activités d'hameçonnage par usurpation de domaines (le courriel semble provenir d'un expéditeur précis, d'une banque ou d'un ministère par exemple, alors qu'il est frauduleux), en déployant systématiquement un programme de vérification d'email sur les réseaux de l'administration publique et en encourageant l'industrie à en faire autant ;
• en favorisant l'adoption des meilleures pratiques de sécurité par le biais d'organisations de gouvernance de l'Internet multipartites telles que la Société pour l'attribution des noms de domaine et des

numéros sur Internet (sigle anglais ICANN - elle coordonne le système de noms de domaine), *l'Internet Engineering Task Force* (sigle anglais IETF) et le Registre internet régional européen (sigle anglais RIPE) et la coopération avec les parties prenantes du Forum sur la gouvernance de l'Internet (FGI) des Nations unies ;
• en œuvrant de concert avec les services répressifs afin d'empêcher que les citoyens britanniques ne soient ciblés par des cyberattaques émanant d'infrastructures étrangères non protégées ;
• en travaillant à la mise en œuvre de contrôles visant à sécuriser le routage du trafic internet destiné aux ministères, pour empêcher des acteurs malveillants de le réacheminer illicitement et
• en investissant dans des programmes pour renforcer les capacités du ministère de la Défense, de la NCA et de GCHQ de réagir et perturber les actes graves de cyberactivité soutenue par un État et criminelle ciblant les réseaux britanniques.

Au fur et à mesure de l'évolution de ces menaces, nous développerons ces interventions techniques pour veiller à ce que nos citoyens, nos entreprises bénéficient d'une protection par défaut, contre la majorité des cyberattaques dites « éde commodité » et de grande envergure.

**Évaluation**

5.1.6. Le Gouvernement mesurera le succès de ses initiatives de mise en place d'une cyberdéfence active, en évaluant les progrès réalisés vers les résultats suivants :

• le Royaume-Uni est plus difficile à hameçonner, suite à la mise en place de défenses à grande échelle contre les domaines malveillants, d'une protection anti-phishing plus active à l'échelle requise et parce qu'il est beaucoup plus difficile d'utiliser d'autres formes de communication comme le « vishing » (hameçonnage vocal) et l'usurpation d'identité par SMS, pour lancer des attaques d'ingénierie sociale ;
• les moyens mis en place bloquent un volume largement plus important de communications malveillantes et d'artefacts techniques associés aux cyberattaques et à l'exploitation connexe ;
• le trafic Internet et les télécommunications sont largement moins vulnérables aux tentatives de redirection par des acteurs malveillants ;
• Les capacités de réaction de GCHQ, des forces armées et de la NCA aux menaces graves émanant d'États ou criminelles, ont été significativement renforcées.

**5.2. CONSTRUIRE UN INTERNET PLUS SÛR**

5.2.1. L'évolution des technologies nous donne la possibilité de réduire significativement la capacité de nos ennemis à perpétrer des actes de cybercriminalité au Royaume-Uni, en veillant à ce que les nouveaux produits en ligne soient « sécurisés par défaut ». Les contrôles de sécurité intégrés aux logiciels et au matériel informatique que nous utilisons, doivent donc faire partie des paramètres d'usine définis par le fabricant pour que l'utilisateur bénéficie d'un maximum de sécurité, si toutefois il ne choisit pas lui-même de les désactiver. L'enjeu consiste à réaliser ce changement transformateur pour le bien de l'utilisateur final, tout en lui proposant un produit ou un service commercialement viables certes, mais néanmoins sûrs et en préservant le caractère libre et ouvert de l'Internet.

« Les objets connectés à l'Internet se multiplient rapidement. En 2015, la preuve a été faite du concept et de la réalité des attaques et nous avons identifié de graves vulnérabilités dans les automobiles, les appareils médicaux, entre autres. Les fabricants doivent inscrire la sécurité au cœur de leurs priorités, afin de réduire le risque de

lourdes conséquences personnelles, économiques et sociales.

Rapport Symantec 2016 sur les menaces à la sécurité internet

5.2.2. Le Gouvernement est bien placé pour jouer un rôle déterminant dans l'étude des nouvelles technologies conçues pour mieux protéger nos propres systèmes, aider l'industrie à accorder une place plus importante à la sécurité de leurs chaînes d'approvisionnement, sécuriser l'écosystème des logiciels et fournir des protections automatisées aux citoyens qui utilisent l'Internet dans le cadre de leurs démarches auprès de l'administration. Le Gouvernement doit tester et adopter les nouvelles technologies qui protègent automatiquement les produits et services en ligne de l'État. Dans la mesure du possible, des technologies similaires devront être proposées au secteur privé et aux citoyens.

**Objectif**

5.2.3. La majorité des nouveaux produits et services en ligne seront « sécurisés par défaut » à l'horizon 2021. Les consommateurs pourront choisir des produits et prestations dotés de paramètres de sécurité intégrée par défaut. Ils pourront choisir de les désactiver, mais ceux qui souhaitent profiter du cyberespace en toute sécurité seront automatiquement protégés.

**Notre approche**

5.2.4. Nous mènerons les actions suivantes :

• le Gouvernement donnera l'exemple en exécutant des services en ligne sécurisés, que l'Internet lui-même le soit ou non ;
• le Gouvernement étudiera les possibilités de collaboration avec l'industrie, pour mettre au point des techniques de pointe visant à rendre le matériel informatique et les logiciels plus « sécurisés par défaut » et
• le Gouvernement adoptera des technologies de cybersécurité inédites, ambitieuses et encouragera les administrations décentralisées à l'imiter, afin de réduire les risques perçus d'adoption. Ces mesures fourniront une validation de principe et démontreront les avantages sécurisants des nouvelles technologies et approches. Elles placeront également la sécurité au cœur du développement de nouveaux produits, élimineront les opportunités d'exploitation criminelle et protégeront ainsi l'utilisateur final.

5.2.5. Pour y parvenir :

• nous continuerons d'encourager les fournisseurs de matériel informatique et de logiciels à commercialiser des produits dont les paramètres de sécurité sont activés par défaut et dont la désactivation nécessite l'intervention volontaire de l'utilisateur. Si certains vendeurs le font déjà, certains n'ont pas encore pris cette mesure nécessaire ;
• nous poursuivrons le développement d'un service de réputation Protocole Internet (IP) visant à protéger les services numériques du gouvernement (il permettrait aux services en ligne de se renseigner sur une adresse IP entrante et les aiderait à prendre des décisions de gestion du risque plus éclairées, en temps réel) ;
• nous chercherons à installer sur les réseaux de l'administration publique, des produits garantissant le bon fonctionnement des logiciels et qu'ils n'ont subi aucune interférence malveillante ;
• au-delà du domaine GOV.UK, nous étendrons nos efforts à d'autres mesures portant sur les services numériques, pour signaler aux utilisateurs que leurs navigateurs sont périmés et
• nous investirons dans des technologies comme les *Trusted Platform Modules* (TPM – Modules de plateforme sécurisée) et les

normes industrielles émergentes comme la *Fast Identity Online* (FIDO - Identité rapide en ligne), qui ne dépendent pas des mots de passe pour authentifier l'utilisateur, mais vérifient son identité en se servant de son ordinateur et de ses autres terminaux. Le Gouvernement mettra à l'essai des mécanismes d'authentification innovants pour en montrer les capacités, tant sur le plan de la sécurité que sur celui de l'expérience globale de l'utilisateur.

5.2.6. Nous réfléchirons en outre à la façon d'encourager le marché, en appliquant un système de notation de sécurité aux nouveaux produits, pour que les consommateurs puissent déterminer facilement quels produits et services leur offrent la plus grande sécurité. Nous étudierons par ailleurs les moyens d'associer ces notations de produits aux régulateurs nouveaux et existants, et d'avertir un consommateur qui s'apprête à exécuter une démarche en ligne susceptible de compromettre sa sécurité.

**Évaluation**

5.2.7. Le Gouvernement mesurera le succès de ses initiatives de construction d'un Internet sécurisé, en analysant les progrès réalisés vers les résultats suivants :

• la majorité des produits et services dits « de commodité » disponibles au Royaume-Uni en 2021 rendent le pays plus sûr, parce que leurs paramètres de sécurité sont activés par défaut ou la sécurité a été intégrée en phase de conception et
• le public britannique se fie à tous les services du gouvernement fournis aux échelons national, local et des administrations décentralisées, parce qu'ils ont été mis en œuvre de la façon la plus sûre possible et parce que les niveaux de fraude sont compris dans une fourchette de risque acceptable.

## 5.3. PROTÉGER NOTRE ADMINISTRATION PUBLIQUE

5.3.1. Le Gouvernement britannique, ses administrations décentralisées et plus largement le secteur public, détiennent de vastes quantités de données sensibles. Ils fournissent des services essentiels au public et exploitent des réseaux vitaux pour la sécurité et la résilience nationales. Les systèmes du gouvernement sous-tendent le fonctionnement de notre société. La modernisation des services publics continuera d'être la pierre angulaire de la stratégie numérique du Royaume-Uni — l'ambition du Gouvernement est de faire du pays le chef de file mondial du numérique. Pour que les citoyens puissent continuer à faire confiance aux services et systèmes publics en ligne, les données détenues par l'administration publique doivent être protégées. Toutes les branches du gouvernement doivent mettre en place des niveaux de cybersécurité suffisants, pour faire face aux tentatives constantes d'acteurs hostiles, déterminés à accéder aux réseaux et données de l'administration ou du secteur public.

**Objectifs**

5.3.2. Nous visons les résultats suivants :

• les citoyens utilisent les services publics en ligne sans crainte : ils sont convaincus que leurs informations sensibles ne courent aucun risque et, en contrepartie, sont conscients qu'il leur appartient de les soumettre en ligne de manière sécurisée ;
• le Gouvernement fixera les normes de cybersécurité les plus appropriées et les appliquera, afin de veiller à ce que toutes les branches de l'administration publique comprennent et s'acquittent de leurs obligations relatives à la sécurisation de leurs réseaux, données et services et
• les actifs critiques du gouvernement, y compris ceux de la classification la plus

élevée, sont protégés contre les cyberattaques.

**Notre approche**

5.3.3. Le Gouvernement britannique continuera d'élargir son offre de services en ligne, pour que le Royaume-Uni devienne véritablement « numérique par défaut ». Le Service numérique du gouvernement (sigle anglais GDS), le Service commercial de la Couronne (sigle anglais CCS) et le NCSC veilleront à ce que tous les nouveaux services numériques créés ou achetés par le Gouvernement, soient également « sécurisés par défaut ».

5.3.4. Les réseaux du Gouvernement sont particulièrement complexes et reposent souvent sur des systèmes hérités et autres logiciels du commerce, que le distributeur d'origine ne prend plus en charge. Nous veillerons à ce que ces systèmes hérités et logiciels non pris en charge, ne présentent aucun risque non maîtrisé.

5.3.5. Nous améliorerons la résilience de l'administration publique et de l'ensemble du secteur public face aux cyberattaques. Nous devrons par conséquent disposer d'informations précises et à jour sur tous les systèmes, sur les données et sur ceux qui peuvent y accéder. La mise en œuvre des meilleures pratiques définies par le NCSC, nous permettra de réduire au minimum la probabilité et l'impact d'un cyberincident. Le Gouvernement se donnera également les moyens d'intervenir efficacement en cas de cyberincident, en suivant un programme d'exercices de simulation d'incidents et en contrôlant régulièrement ses réseaux. Nous inviterons les administrations décentralisées et les pouvoirs locaux à participer à ces exercices, si nécessaire. Le recours au balayage automatisé nous permettra de mieux connaître l'état de la sécurité en ligne du Gouvernement.

5.3.6. La cybersécurité n'est pas une simple question de technologie. La quasi-totalité des cyberattaques réussies comporte un facteur humain favorisant. En conséquence, nous continuerons à investir dans nos collaborateurs, pour veiller à ce que chaque fonctionnaire du gouvernement soit parfaitement conscient du cyberrisque. Nous développerons une cyberexpertise spécifique dans les domaines à haut risque et nous doterons des processus adéquats pour les gérer efficacement.

5.3.7. Le NCSC formulera des orientations phares en matière de cybersécurité, en phase avec l'évolution de la menace et des nouvelles technologies. Nous prendrons les mesures qui s'imposent pour veiller à ce que les organismes publics puissent accéder facilement aux renseignements sur les menaces, renforcer leur compréhension de leurs propres cyberrisques et prendre les mesures qui s'imposent.

5.3.8. Nous continuerons d'améliorer nos réseaux à classification maximale, pour protéger les communications les plus sensibles du Gouvernement.

5.3.9. Les systèmes de soins de santé posent des défis uniques dans le contexte de la cybersécurité. Le secteur emploie quelque 1,6 million de personnes dans plus de 40 000 organisations, dont les ressources et capacités individuelles de sécurité de l'information varient énormément. Parallèlement à un nouveau modèle de consentement/refus pour les patients, le Gardien des données nationales pour la santé et les soins (National Data Guardian for Health and Care) a fixé de nouvelles normes de sécurité des données à destination des systèmes de santé et d'aide sociale en Angleterre. Le Gouvernement collaborera avec les organisations de la santé et de l'aide sociale pour les mettre en œuvre.

« La Grande-Bretagne est un leader mondial dans le domaine de la cybersécurité et face à la montée en puissance des menaces, ce nouveau Centre des opérations de cybersécurité donnera à nos forces armées les moyens de continuer d'opérer en toute sécurité. L'augmentation de notre budget de défense nous aidera à garder une longueur d'avance sur nos ennemis dans le cyberespace, tout en investissant également dans les moyens conventionnels. »

Michael Fallon, député
Ministre de la Défense, avril 2016

5.3.10. La cybersécurité est vitale pour notre défense. Nos forces armées dépendent des systèmes d'information et de communications, tant sur le territoire britannique que dans le cadre de leurs missions à l'étranger. Les infrastructures et le personnel du ministère de la Défense (MoD) sont des cibles bien en vue. Les systèmes de défense sont régulièrement visés par les criminels, services du renseignement étrangers et autres acteurs malveillants qui cherchent à exploiter leur personnel, à déstabiliser leurs activités et opérations, à endommager et voler leurs informations. Nous améliorerons les fonctions de sensibilisation, de détection et de réaction aux menaces grâce au développement d'un Centre des opérations de cybersécurité (sigle anglais CSOC), doté de moyens de cyberdéfense de pointe pour protéger le cyberespace du MoD et combattre les menaces. Le CSOC travaillera en étroite collaboration avec le NCSC pour, d'une part, relever les défis auxquels est confronté le MoD et de l'autre, contribuer à la cybersécurité nationale au sens large du terme.

**Évaluation**

5.3.11. Le Gouvernement mesurera le succès de ses initiatives de protection des réseaux, systèmes et données publics, en évaluant les progrès réalisés vers les résultats suivants :

• le Gouvernement comprend parfaitement le niveau de risque de cybersécurité que courent l'ensemble de l'administration et le secteur public au sens large du terme ;
• les ministères individuels et autres organes se protègent proportionnellement à leur niveau de risque et conformément à une norme minimale convenue avec l'administration publique ;
• les ministères et l'ensemble du secteur public sont résilients et savent réagir efficacement aux cyberincidents, maintenir la continuité de leurs fonctions et récupérer rapidement ;
• les nouvelles technologies et services numériques déployés par l'administration publique seront cybersécurisés par défaut ;
• nous sommes conscients des vulnérabilités des systèmes et services publics connectés et œuvrons activement pour les atténuer et
• tous les fournisseurs de l'administration publique respectent les normes de cybersécurité appropriées.

## 5.4. PROTÉGER LES INFRASTRUCTURES CRITIQUES ET LES AUTRES SECTEURS PRIORITAIRES DU PAYS

**Contexte**

5.4.1 La cybersécurité de certaines organisations britanniques est particulièrement importante, dans la mesure où une cyberattaque réussie à ce niveau aurait les pires conséquences pour notre sécurité nationale. Ces conséquences risqueraient de se répercuter sur la vie des citoyens britanniques, la stabilité et la puissance de l'économie ou encore, la réputation et le statut du Royaume-Uni à l'étranger. Ce groupe d'entreprises et d'organisations de premier plan des secteurs public et privé, comprend l'infrastructure vitale nationale (sigle anglais CNI), chargée de

fournir des services essentiels à la Nation. Le Gouvernement inscrira de la sécurisation de ces infrastructures et de leur résilience face aux cyberattaques potentielles, parmi ses priorités. Au-delà de la CNI, ce groupe de première importance inclut d'autres entreprises et organisations nécessitant un soutien plus conséquent. Citons notamment :

• les sociétés britanniques les plus performantes, fleurons de notre économie et celles dont la recherche et la propriété intellectuelle constitueront les bases de notre prospérité économique future ;
• les détenteurs de données — non seulement les organisations qui détiennent de grandes quantités de données personnelles, mais aussi celles qui possèdent des données sur les citoyens vulnérables ici et ailleurs, comme c'est le cas des associations caritatives ;
• les cibles privilégiées – les médias notamment, contre lesquels une attaque risquerait de ternir la réputation du Royaume-Uni, de nuire à la confiance des citoyens dans le Gouvernement ou de porter atteinte à la liberté d'expression ;
• les fournisseurs de services numériques. Piliers de notre économie numérique, rouages essentiels du commerce électronique et de notre économie numérique, ils dépendent de la confiance des consommateurs en leurs prestations et
• les organisations qui, par le biais des forces et de l'autorité des marchés, peuvent exercer une influence sur l'ensemble de l'économie et contribuer à leur cybersécurité : assureurs, investisseurs, régulateurs et conseillers professionnels.

5.4.2. Davantage d'efforts doivent être consentis, pour protéger ces composantes vitales de notre économie et accompagner les organismes influents. Notre CNI - dans les secteurs public et privé - continue d'être prise pour cible. Le cyberrisque que courent cette infrastructure et un grand nombre d'autres secteurs prioritaires, est encore mal compris et mal géré, alors même que les menaces continuent de se diversifier et de s'intensifier.

**Objectif**

5.4.3. Le Gouvernement britannique, en collaboration avec les administrations décentralisées et les autres autorités responsables si nécessaire, veillera à ce que les organisations et entreprises les plus importantes du pays, CNI incluse, soient suffisamment sécurisées et résilientes face aux cyberattaques. Ni le Gouvernement ni les autres organes publics n'assumeront la responsabilité de gérer ce risque pour le compte du secteur privé. Cette tâche incombe, à juste titre, aux conseils d'administration, aux propriétaires et aux opérateurs.
Le Gouvernement n'en proposera pas moins un appui et une assurance proportionnels aux menaces auxquelles sont confrontées ces entreprises et organisations et aux conséquences de ces attaques.

« La cybersécurité est la clé qui ouvrira la porte à l'innovation et à l'expansion. L'adoption d'un schéma d'organisation sur mesure et d'une approche centrée sur le risque, permet aux organisations de se recentrer sur les opportunités et l'exploration. Renforcer la confiance dans une entreprise très performante au sein de l'Internet des objets (IdO), qui accompagne et protège les individus et leurs terminaux mobiles personnels (du simple téléphone à l'appareil de soins de santé, en passant par les voitures et les appareils intelligents), constitue un différenciateur concurrentiel clé et doit être traité comme une priorité. »
Enquête 2015 sur la sécurité de l'information mondiale EY

**Notre approche**

5.4.4. Il incombe aux conseils d'administration des organisations et des sociétés de faire en sorte que leurs réseaux soient sécurisés, d'identifier les systèmes critiques et d'évaluer régulièrement leur vulnérabilité par rapport à un paysage technologique et des menaces en constante évolution. Ils doivent investir dans la technologie et leurs ressources humaines, pour réduire les vulnérabilités des systèmes existants, futurs et de leur chaîne d'approvisionnement, afin de maintenir un niveau de cybersécurité proportionnel au risque. Ils doivent également se doter de moyens éprouvés pour réagir en cas d'attaque. S'agissant de l'infrastructure CNI, ils doivent œuvrer avec les organismes publics et les régulateurs, pour que nous soyons sûrs que les risques du cyberespace sont correctement gérés et — dans le cas contraire — pour que nous puissions intervenir dans l'intérêt de la sécurité nationale.

5.4.5. Le Gouvernement comprendra alors le niveau de cybersécurité sur l'ensemble de l'infrastructure CNI et disposera de moyens prêts à intervenir en cas de besoin, pour dynamiser les améliorations jugées comme étant dans l'intérêt national.

5.4.6. Le Gouvernement :

• partagera avec l'industrie des informations sur les menaces qu'il est le seul à pouvoir obtenir, afin qu'ils puissent définir celles contre lesquelles ils doivent se protéger ;
• formulera des conseils et des orientations sur la façon de gérer le cyberrisque et, en collaboration avec les entreprises et les universités, définira les grandes caractéristiques d'une cybersécurité efficace ;
• stimulera la mise en place d'une sécurité haut de gamme nécessaire pour protéger l'infrastructure CNI, faisant notamment appel aux centres de formation, laboratoires d'analyse, normes de sécurité et services de conseil et

• mènera, avec les sociétés de l'infrastructure CNI, des exercices pour les aider à gérer leurs cyberrisques et vulnérabilités.

5.4.7. Le NCSC fournira ces services aux entreprises et aux organismes britanniques les plus importants, dont la CNI. Il s'y emploiera en partenariat avec les ministères et les régulateurs, qui s'assureront que le niveau de gestion du cyberrisque dans leurs secteurs, est conforme aux exigences de l'intérêt national.

5.4.8. En outre, le Gouvernement fera en sorte que la cybersécurité soit associée à un cadre réglementaire approprié et à ce que ce cadre :

• veille à ce que l'industrie réagisse pour se protéger contre les menaces ;
• soit orienté vers les résultats et suffisamment souple pour ne pas se faire dépasser par la menace, ou entraîner une mise en conformité administrative plutôt qu'une gestion saine des risques ;
• soit suffisamment agile pour encourager la croissance et l'innovation, au lieu de les diriger ;
• s'harmonise avec les régimes d'autres juridictions afin que les entreprises britanniques ne soient pas victimes d'une approche fragmentée et fastidieuse et
• constitue, avec le concours solide du Gouvernement, un avantage compétitif pour le Royaume-Uni.

5.4.9. Pour un grand nombre de nos secteurs industriels, la question de la cybersécurité fait déjà l'objet d'une réglementation. Nous n'en devons pas moins veiller à ce que les mesures appropriées soient prises sur l'ensemble de l'économie, CNI comprise, pour gérer les risques en ligne.

**Évaluation**

5.4.10. Le Gouvernement mesurera le succès de ses initiatives de protection de notre CNI et des autres secteurs prioritaires, en évaluant les progrès réalisés vers les résultats suivants :

• nous comprenons le niveau de cybersécurité de notre CNI et avons mis en place des mesures pour intervenir en cas de besoin et dynamiser les améliorations, dans l'intérêt national et
• nos entreprises et organisations les plus importantes comprennent le niveau de menace et mettent en œuvre des pratiques de cybersécurité proportionnelles aux risques.

## 5.5. TRANSFORMER LES COMPORTEMENTS DU PUBLIC ET DES ENTREPRISES

5.5.1 La prospérité de l'économie numérique britannique dépend aussi de la confiance qu'accordent les entreprises et le public aux services en ligne. Le Gouvernement a coopéré avec l'industrie et d'autres branches du secteur public, dans une optique de sensibilisation et pour mieux faire comprendre la menace. Il a également mis à la disposition du public et des entreprises les outils nécessaires pour se protéger. Si de nombreuses organisations s'acquittent d'un excellent travail — passé référence mondial dans certains cas — pour se protéger et fournir des services en ligne, la majorité des entreprises et des particuliers ne gèrent toujours pas correctement le cyberrisque.

« L'année dernière, les atteintes à la sécurité subies par les grandes entreprises leur ont coûté, en moyenne, 36 500 GBP (environ 42 400 euros). La facture moyenne des petites entreprises victimes d'attaques s'élevait à 3 100 GBP (3 653 euros). 65 % des grandes organisations ont signalé l'occurrence d'une atteinte à la sécurité de leurs informations au cours des 12 derniers mois et 25 % d'entre elles ont subi au moins une attaque par mois. Dans près de sept attaques sur dix, le pirate s'est servi d'un virus, espiogiciel ou logiciel malveillant que le programme « L'essentiel de la cybersécurité » (Cyber Essentials Scheme) du Gouvernement aurait permis d'éviter. »
Bilan cyber-santé 2016 du Gouvernement et enquête sur les atteintes à la cybersécurité

**Objectif**

5.5.2. Notre objectif est de faire en sorte que les particuliers et les organisations, tous secteurs ou tailles confondus, prennent les mesures qui conviennent pour se protéger, eux et leur clientèle, contre les préjudices consécutifs aux cyberattaques.

**Notre approche**

5.5.3. Le Gouvernement fournira les conseils dont a besoin l'économie pour se protéger. Nous améliorerons la façon dont ils sont communiqués, pour en maximiser les effets. Pour le public, le Gouvernement fera appel à des « voix fiables » afin d'étendre la portée de notre message, de le rendre à la fois plus crédible et plus pertinent. Nous fournirons des conseils faciles à suivre et utiles aux particuliers, aux points d'accès aux services susceptibles de les exposer aux risques. Nous impliquerons les administrations décentralisées et d'autres autorités si nécessaire.

5.5.4. S'agissant des entreprises, nous œuvrerons par l'intermédiaire d'organisations telles que les assureurs, régulateurs et investisseurs, qui peuvent influencer les entreprises pour veiller à ce qu'elles gèrent le cyberrisque. Ce faisant, nous soulignerons les avantages économiques manifestes et le prix du cyberrisque fixé par les influenceurs du marché. Nous chercherons à mieux comprendre pourquoi de nombreuses organisations ne se protègent pas encore

suffisamment. Nous œuvrerons avec des partenaires tels que les organismes de normalisation professionnelle, dans le but d'aller au-delà de la sensibilisation, pour persuader les entreprises qu'une action s'impose. Par ailleurs, nous veillerons à ce que le cadre réglementaire qui convient soit mis en place, pour gérer les cyberrisques auxquels le marché ne répond pas. Dans le cadre de cet effort, nous tenterons d'exploiter certains leviers comme le règlement général sur la protection des données (sigle anglais GDPR), afin de renforcer les normes de cybersécurité et de protéger nos citoyens.

5.5.5. Les particuliers et les organisations du Royaume-Uni auront accès à l'information, à la formation et aux outils nécessaires pour se protéger. Afin d'aboutir à une transformation radicale du comportement du public, le Gouvernement et ses partenaires pérenniseront un ensemble de messages cohérents et logiques d'orientation en matière de cybersécurité. Le NCSC donnera des conseils techniques pour étayer ces orientations. Facilement accessibles, clairs, cohérents allant de pair avec les menaces, ils correspondront aux priorités et pratiques des entreprises et du public. En étroite collaboration avec le secteur industriel et le NCSC, les services répressifs partageront les renseignements les plus récents sur les activités criminelles, pour aider l'industrie à se défendre contre les menaces et atténuer l'impact des attaques sur les victimes britanniques.

**Évaluation**

5.5.6. Le Gouvernement mesurera le succès de ses initiatives de protection de notre infrastructure CNI et des autres secteurs prioritaires, en évaluant les progrès réalisés vers les résultats suivants :

• le niveau de cybersécurité de l'économie britannique est aussi élevé, voire plus élevé, que celui d'économies avancées comparables ;
• le nombre, la gravité et l'impact des cyberattaques réussies contre des entreprises au Royaume-Uni, ont diminué suite à l'amélioration des normes d'hygiène informatique et
• la culture de la cybersécurité s'est améliorée au Royaume-Uni, parce que les organisations et le public comprennent leurs niveaux de cyberrisque et les mesures d'hygiène informatique à prendre pour le gérer.

**CYBER AWARE**

La campagne *Cyber Aware* (« Conscient des cyberrisques »), anciennement *Cyber Streetwise*, donne au public les conseils dont il a besoin pour se protéger contre les cybercriminels. Des messages ciblés, transmis par les réseaux sociaux et publicitaires en partenariat avec les entreprises, l'encourage à :

• utiliser trois mots pris au hasard pour créer un mot de passe efficace et
• à toujours télécharger les dernières mises à jour logicielles.

Les spécialistes s'accordent à dire que l'adoption de ces comportements protègeront les petites entreprises et particuliers contre la cybercriminalité. *Cyber Aware* compte actuellement 128 partenaires intersectoriels, dont la police et des entreprises des secteurs de la vente au détail, des loisirs, du voyage et des services professionnels.
En 2015-2016, quelque 10 millions d'adultes et un million de petites entreprises ont avoué êtreplus susceptibles de maintenir ou d'adopter des comportements de

cybersécurité clés, suite à la campagne *Cyber Aware*.

Pour en savoir plus, consulter le site cyberaware.gov.uk

**CYBER ESSENTIALS**

Le programme *Cyber Essentials* (« L'essentiel de la cybersécurité ») a été développé pour montrer aux organisations comment se protéger des menaces de faible niveau dites « de commodité ». Il recense cinq contrôles techniques (contrôle d'accès ; pare-feu de cloisonnement et passerelles internet ; protection contre les logiciels malveillants ; gestion des patches (correctifs) et configuration sécurisée) que les organisations doivent avoir mis en place. La vaste majorité des cyberattaques utilise des méthodes relativement simples, exploitant les vulnérabilités de base des logiciels et systèmes informatiques. Des outils et techniques en accès libre sur Internet permettent même à des acteurs peu compétents d'en profiter. La mise en œuvre correcte du programme Cyber Essentials protège contre la vaste majorité des menaces Internet les plus courantes.

## 5.6. GÉRER LES INCIDENTS ET COMPRENDRE LA MENACE

5.6.1. Les cyberincidents qui touchent les organisations des secteurs public et privé, risquent de se multiplier et de s'aggraver. D'où la nécessité de définir les modes d'interaction entre le secteur privé, le public et les pouvoirs publics lors d'un cyberincident. Nous ferons en sorte que le niveau de soutien du Gouvernement britannique pour chaque secteur — compte tenu de sa cybermaturité — soit clairement défini et compris. La collecte et la diffusion par les pouvoirs publics des informations sur la menace, doivent s'effectuer d'une manière et à un rythme convenant à toutes sortes d'organisations. Au jour d'aujourd'hui, le secteur privé, l'administration publique et le public peuvent accéder à une multitude de sources d'information, de recommandations et d'assistance en matière de cybersécurité. Cet aspect doit être simplifié.

5.6.2. Nous devons veiller à ce que l'offre du Gouvernement, tant dans sa manière dont il réagit aux incidents que dans la formulation d'orientations, n'existe pas isolément, mais dans le cadre d'un partenariat avec le secteur privé. Nos procédures de gestion d'incidents devraient refléter une approche globale en la matière, par laquelle nous profiterons de l'expérience de nos partenaires et partagerons les techniques d'atténuation. Nous continuerons par ailleurs de mettre à profit nos relations avec d'autres équipes d'interventions en cas d'urgence informatique (sigle anglais CERT) et avec nos alliés, dans le cadre de notre fonction de gestion d'incidents.

5.6.3. Dans sa forme actuelle, la gestion d'incidents reste quelque peu fragmentée dans les ministères. Cette stratégie lui donnera une forme unifiée. Le NCSC mettra en œuvre une fonction d'intervention en cas d'incident rationalisée, efficace et dirigée par le gouvernement.
En cas de cyberincident grave, nous ferons en sorte que les forces armées puissent apporter une assistance, soit sous une forme conventionnelle traitant l'impact physique de l'incident, soit sous forme d'appui assuré par un personnel régulier ou de réserve, spécialiste de la cyberdéfense. Tout en fournissant un soutien adapté à nos ressources, le Gouvernement insiste une fois de plus sur l'importance de la contribution de l'industrie, de la société et du public dans la protection de leur cybersécurité de base.

**Objectifs**

5.6.4. Nos objectifs sont les suivants :

• le Gouvernement appliquera une approche unique, décloisonnée en matière de gestion d'incidents, fondée sur une compréhension et une prise de conscience améliorées de la menace et des mesures prises à notre encontre. Le NCSC jouera un rôle moteur, à l'instar des partenariats avec le secteur privé, des forces de l'ordre et des autres ministères, autorités et agences ;
• le NCSC définit des procédures claires de signalement des incidents, adaptées au profil de la victime et
• nous empêcherons les cyberincidents les plus courants et disposerons de structures de partage de l'information efficaces et utiles à la planification « pré-incident ».

**Notre approche**

5.6.5. Il incombe aux directions des organisations et des entreprises des secteurs public et privé, de veiller à ce que leurs réseaux soient sécurisés et de mettre en place des plans d'intervention en cas d'incident. Dans l'éventualité d'un incident important, la procédure de gestion d'incidents des pouvoirs publics portera sur les trois éléments distincts d'un cyberincident : les précurseurs, l'incident proprement dit et l'intervention après l'incident.

5.6.6. Afin de mettre en œuvre une gestion d'incidents efficace pour le Gouvernement et le secteur privé, nous travaillerons en étroite collaboration pour examiner et définir la portée de l'intervention du Gouvernement, dans une optique de renforcement de la coopération. Nous renforcerons notre plan de cyber-exercice national, en tirant parti d'une compréhension et de connaissances de la menace améliorées, pour améliorer notre offre de soutien à nos partenaires des secteurs public et privé.

5.6.7. Nous créerons une identité fiable et crédible pour le Gouvernement, source de conseils en matière d'incidents, d'assistance et d'assurance. La communauté numérique du Royaume-Uni étant alors plus sensible à la cybersécurité, nous pourrons mieux identifier les tendances, prendre des mesures proactives et au final, empêcher les incidents.

5.6.8. En évoluant vers un partage de l'information automatisé (par lequel les systèmes de cybersécurité s'alertent automatiquement les uns les autres en cas d'incident ou d'attaque), nous améliorerons l'efficacité de notre service. Il permettra aux organisations d'agir rapidement, sur la base d'informations sur la menace pertinentes.

**Évaluation**

5.6.9. Le Gouvernement mesurera le succès de son initiative de gestion d'incidents, en évaluant les progrès réalisés vers les résultats suivants :

• un nombre plus important d'incidents sont signalés aux autorités, d'où une meilleure compréhension de l'étendue et de l'ampleur de la menace ;
• les cyberincidents sont gérés plus efficacement, de manière plus efficiente et plus complète, suite à la création du NCSC, mécanisme centralisé de signalement d'incidents et d'intervention et
• nous traiterons les causes profondes des attaques à l'échelon national, réduisant l'occurrence des récidives contre une multitude de victimes et de secteurs.

## 6. DISSUADER

6.0.1. En vertu de la Stratégie de sécurité nationale, la défense et la protection commencent par la dissuasion. Le cyberespace n'échappe pas plus à cette règle que n'importe quelle autre sphère. Afin de concrétiser notre volonté de vivre dans un pays sécurisé et résilient face aux menaces, prospère et confiant dans l'univers numérique, nous devons dissuader et décourager ceux qui veulent nuire à nos intérêts. C'est pourquoi nous devons tous continuer à améliorer notre cybersécurité, pour qu'une attaque dans le cyberespace – pour nous voler ou nous faire du mal – soit matériellement rhédibitoire et très difficile à exécuter. Nos ennemis doivent savoir qu'ils ne peuvent agir en toute impunité : nous disposons des moyens nécessaires pour les identifier et ils le seront. Nous sommes prêts à riposter, en sélectionnant les outils de notre vaste panoplie les mieux adaptés à la situation. Nous continuerons à former des alliances mondiales et à promouvoir l'application du droit international dans le cyberespace. De plus, nous perturberons plus activement les opérations de ceux qui nous menacent dans le cyberespace et les infrastructures sur lesquelles ils comptent pour mener leurs actions. La mise en œuvre de cette ambition requiert des moyens souverains de rang mondial.

### 6.1. LE RÔLE DE LA CYBERSÉCURITÉ DANS LA DISSUASION

6.1.1. Le cyberespace n'est qu'une des sphères dans lesquelles nous devons défendre nos intérêts et notre souveraineté. Tout comme nos actions dans la sphère physique sont importantes pour la cybersécurité et la dissuasion, nos actions et notre attitude dans le cyberespace doivent contribuer à notre sécurité nationale au sens large.

6.1.2. Les principes de dissuasion sont aussi applicables dans le cyberespace que dans la sphère physique. Le Royaume-Uni déclare sans équivoque, qu'il fera appel à l'intégralité de son arsenal de capacités pour dissuader ses ennemis et les priver d'opportunités de l'attaquer. Nous n'en reconnaissons pas moins que la cybersécurité et la résilience sont, en elles-mêmes, des moyens d'enrayer les attaques visant l'exploitation de vulnérabilités.

6.1.3. Nous appliquerons une approche nationale globale en matière de cybersécurité et de dissuasion, pour faire du Royaume-Uni une cible plus difficile à viser, en réduisant les avantages et en augmentant les coûts pour nos ennemis — qu'ils soient politiques, diplomatiques, économiques ou stratégiques. Nous devons faire en sorte que nos ennemis potentiels comprennent nos capacités et notre intention de riposte, pour influencer leur processus décisionnel. Nous nous doterons des outils et des capacités nécessaires : pour priver nos ennemis d'occasions faciles de compromettre nos réseaux et systèmes ; comprendre leurs intentions et leurs moyens ; déjouer à grande échelle les menaces liées aux maliciels dits « de commodité » et enfin, pour intervenir et protéger la Nation dans le cyberespace.

### 6.2. RÉDUIRE LA CYBERCRIMINALITÉ

6.2.1. Nous devons augmenter le coût, accroître le risque et réduire les gains découlant des activités des cybercriminels. Si nous devons endurcir le Royaume-Uni aux cyberattaques et réduire les vulnérabilités, il nous faut aussi poursuivre sans relâche les délinquants qui continuent de cibler notre territoire.

6.2.2. Les services répressifs concentreront leurs efforts sur la poursuite des criminels qui

persistent à attaquer les citoyens et les entreprises britanniques. Nous coopérerons avec nos partenaires nationaux et internationaux, pour cibler les criminels où qu'ils soient et démanteler leurs infrastructures et réseaux de facilitation. Les services répressifs poursuivront également leurs efforts de sensibilisation aux et d'amélioration des critères de cybersécurité, en collaboration avec le NCSC.

6.2.3. Cette stratégie s'inscrit en complément de la Stratégie 2013 afférente aux crimes graves et à la criminalité organisée (Serious and Organised Crime Strategy), qui présente la réponse stratégique du Gouvernement britannique à la cybercriminalité, parallèlement à d'autres formes graves de criminalité organisée. La *Cellule nationale de cybercriminalité* (sigle anglais NCCU), qui siège au sein de l'Agence britannique de lutte contre le crime organisé (sigle anglais NCA), a été établie pour diriger et coordonner la réponse nationale à la cybercriminalité. *Action Fraud* est un centre national de signalement des manœuvres frauduleuses et de la cybercriminalité. Un réseau de cellules de lutte contre la cybercriminalité au sein des Unités régionales de lutte contre la criminalité organisée (sigle anglais ROCU) donne accès, à l'échelon régional, à des cybercapacités spécialisées soutenant la NCCU et les forces de police locales.

**Objectif**

6.2.4. Nous réduirons l'impact de la cybercriminalité sur le Royaume-Uni et ses intérêts, en dissuadant les cybercriminels de cibler notre pays et en poursuivant sans relâche ceux qui persistent à nous attaquer.

**Notre approche**

6.2.5. Pour diminuer l'impact de la cybercriminalité :

• nous renforcerons les capacités et les compétences des services répressifs aux échelons national, régional et local afin de détecter, poursuivre et dissuader les cybercriminels sur le territoire britannique et à l'étranger ;
• nous améliorerons notre compréhension du modèle économique de la cybercriminalité, afin de savoir où nous devons orienter nos interventions et de déstabiliser le plus posible les activités criminelles. Nous mettrons aussi à profit ces connaissances pour :

- faire du Royaume-Uni un environnement opérationnel au coût et au risque rhédibitoires en visant le cœur de la criminalité du pays et en œuvrant de concert avec l'industrie pour réduire la possibilité pour les criminels d'exploiter les infrastructures britanniques et
- combattre la cybercriminalité en amont, en déstabilisant le modèle économique criminel, en démantelant leurs infrastructures et leurs réseaux financiers et en saisissant toutes les occasions de traduire les criminels en justice.

• nous tisserons des partenariats internationaux pour mettre fin à l'impunité perçue par les cybercriminels agissant contre le Royaume-Uni, en traduisant en justice les criminels situés dans des juridictions étrangères ;
• nous dissuaderons les individus de se laisser tenter par la cybercriminalité ou de s'y impliquer, en renforçant nos mesures d'intervention précoce ;
• nous améliorerons notre collaboration avec l'industrie afin de lui fournir des renseignements sur les menaces à titre de précaution et pour obtenir les renseignements en amont dont elle dispose et ainsi, renforcer nos efforts de déstabilisation ;
• nous mettrons en place au sein *d'Action Fraud* une nouvelle capacité de signalement et de triage 24 heures sur 24, 7 jours sur 7 liée au NCSC, à la *National Cyber Crime Unit* de la

NCA et à l'ensemble des services répressifs, pour améliorer le soutien aux victimes de la cybercriminalité, réagir plus rapidement aux délits signalés et dispenser de meilleurs conseils en matière de sûreté. Un système de signalisation inédit sera établi, pour diffuser l'information sur la cybercriminalité et les menaces en temps réel sur l'ensemble des services répressifs ;
• nous collaborerons avec le NCSC et le secteur privé pour réduire les vulnérabilités des infrastructures britanniques susceptibles d'être exploitées à grande échelle par les cybercriminels et
• travaillerons avec le secteur financier pour faire du Royaume-Uni un environnement plus hostile pour ceux qui cherchent à monétiser les usurpations d'identité, en perturbant leurs réseaux, par exemple.

**Évaluation**

6.2.6. Le Gouvernement mesurera le succès de ses initiatives de réduction de la cybercriminalité, en évaluant les progrès réalisés vers les résultats suivants :

• nous parvenons mieux à déstabiliser les cybercriminels qui attaquent le Royaume-Uni ; le nombre d'arrestations et de condamnations augmente au même titre que celui des réseaux criminels démantelés suite à l'intervention des forces de l'ordre ;
• les moyens des services répressifs se sont améliorés, cette amélioration se traduisant notamment par le renforcement des capacités et compétences des spécialistes et des agents de base et par le perfectionnement des ressources des services répressifs de nos partenaires étrangers ;
• l'efficacité et l'ampleur des mesures d'intervention précoce, prises pour dissuader et réformer les délinquants se sont manifestement améliorées et
• le nombre de cyber-infractions de faible niveau a diminué, les services des cybercriminels ayant perdu leur facilité d'accès et une grande part de leur efficacité.

**QUE FAIRE SI VOUS ÊTES VICTIME DE CYBERCRIMINALITÉ**

Vous êtes un membre du public et pensez être victime d'une cyber-infraction, ou d'une manœuvre frauduleuse en ligne ? Contactez *Action Fraud*.

Vous pouvez signaler l'incident à l'aide de l'outil de signalement en ligne d'*Action Fraud* à tout moment de la journée ou de la nuit, ou en appelant le 0300 123 2040. Pour en savoir plus, visitez
www.actionfraud.police.uk

Le service *Action Fraud* est géré par la City of London Police.

## 6.3. LUTTER CONTRE LES ACTIONS ÉTRANGÈRES HOSTILES

6.3.1. Nous devons utiliser la panoplie complète des capacités du Gouvernement, pour lutter contre la menace que présentent les acteurs étrangers hostiles et qui pèse de plus en plus sur notre sécurité politique, économique et militaire. La coopération avec nos partenaires internationaux sera déterminante pour notre succès et nous redoublerons d'efforts pour les impliquer et collaborer avec eux, afin de contrer cette menace. Une grande partie de cette action ne sera pas dans le domaine public. Notre investissement dans les capacités souveraines et dans les partenariats avec les industriels et le secteur privé, continuera de soutenir notre capacité à détecter, observer et identifier cette activité ennemie en constante évolution.

**Objectif**

6.3.2. Pour chaque ennemi, nous aurons mis en place des stratégies, politiques et priorités, dont le but sera de veiller à ce qu'une approche proactive, bien calibrée et efficace, soit adoptée pour contrer la menace et faire baisser le nombre et la gravité des cyberincidents.

**Notre approche**

6.3.3. Afin de réduire les menaces émanant d'acteurs étrangers hostiles :

• nous renforcerons l'application du droit international dans le cyberespace, tout en favorisant l'adoption de normes non contraignantes de comportement d'État responsable, ainsi que le développement et la mise en œuvre de mesures de renforcement de la confiance ;
• nous travaillerons avec nos partenaires internationaux, notamment dans les domaines de la défense collective, de la sécurité coopérative et de la dissuasion renforcée, dans le cadre de notre adhésion à l'OTAN ;
• nous identifierons les aspects à la fois uniques et génériques de la cyberactivité de nos ennemis ;
• nous chercherons et étudierons toutes les options disponibles pour dissuader et contrer cette menace, en nous appuyant sur tout l'éventail des capacités du Gouvernement. Nous tiendrons pleinement compte d'autres facteurs connexes, y compris les stratégies propres à chaque pays, les priorités internationales et les objectifs de cybercriminalité et de prospérité ;
• nous utiliserons les réseaux et les relations existants avec nos principaux partenaires internationaux, pour partager les informations sur les menaces actuelles et naissantes, enrichissant notre réflexion et notre expertise et
• nous attribuerons publiquement des cyber-identités spécifiques, à chaque fois qu'une telle mesure nous paraîtra être dans l'intérêt national.

**Évaluation**

6.3.4. Le Gouvernement mesurera le succès de ses initiatives de lutte contre les actions d'acteurs étrangers hostiles, en évaluant les progrès réalisés vers les résultats suivants :

• les réseaux de partage de l'information consolidés établis conjointement avec nos partenaires internationaux, ainsi que les accords multilatéraux formulés pour encourager l'adoption par les États d'un comportement légitime et responsable, contribuent de manière substantielle à notre capacité à comprendre et réagir à la menace, se traduisant par une défense plus efficace du Royaume-Uni et
• nos mesures de défense et de dissuasion, ainsi que nos stratégies nationales spécifiques, font du Royaume-Uni une cible plus difficile à atteindre pour les acteurs étrangers hostiles.

## 6.4. PRÉVENIR LE TERRORISME

6.4.1. Pour l'instant, les moyens techniques des terroristes sont encore limités. Ils n'en continuent pas moins d'aspirer à mener contre le Royaume-Uni des opérations préjudiciables via les réseaux informatiques, principalement dans un but publicitaire et déstabilisateur. Le Gouvernement identifiera et perturbera l'activité des terroristes qui exploitent le cyberespace ou envisagent de le faire dans ce but. Nous minimiserons ainsi leur impact et empêcherons que l'amélioration de leurs capacités n'augmente la menace qui pèse déjà sur les réseaux britanniques et la sécurité nationale.

**Objectif**

6.4.2. Atténuer le risque d'utilisation du cyberespace par les terroristes, en repérant et en déstabilisant les cyberterroristes qui détiennent actuellement les capacités de menacer la sécurité nationale du Royaume-Uni de et les renforcer.

**Notre approche**

6.4.3. Afin de garantir que la menace cyber-terroriste reste faible :

• nous détecterons les menaces cyber-terroristes et identifierons les auteurs potentiels qui cherchent à lancer, contre le Royaume-Uni et nos alliés, des opérations nuisibles sur les réseaux ;
• nous enquêterons sur ces cyber-terroristes et les déstabiliserons afin de les empêcher d'exploiter leurs cyber-capacités contre le Royaume-Uni et ses alliés et
• nous travaillerons en étroite collaboration avec nos partenaires internationaux, pour mieux combattre la menace du cyber-terrorisme.

**Évaluation**

6.4.4. Le Gouvernement mesurera le succès de ses initiatives de prévention du terrorisme, en évaluant les progrès réalisés vers les résultats suivants :

• compréhension approfondie du risque posé par le cyberterrorisme, par l'identification et l'analyse des menaces cyberterroristes pesant sur le Royaume-Uni et
• surveillance rapprochée et perturbation des capacités cyberterroristes à la première occasion, dans le but d'empêcher leur intensification à long terme.

## 6.5. AMÉLIORER LES CAPACITÉS SOUVERAINES — CYBEROFFENSIVE

6.5.1. Les cybercapacités offensives impliquent des intrusions délibérées dans les systèmes ou les réseaux adverses, pour les endommager, les perturber ou les détruire. Les cyberoffensives font partie de l'arsenal complet des capacités que nous développons, pour dissuader nos ennemis et les priver d'opportunités de nous attaquer, tant dans le cyberespace que dans la sphère physique. Notre Programme national de cyberoffensive (sigle anglais NOCP), nous donne une capacité d'action dédiée dans le cyberespace. Nous engagerons les ressources nécessaires pour la développer et l'améliorer.

**Objectif**

6.5.2. Nous ferons en sorte de disposer de capacités de cyber-offensive susceptibles d'être déployées au moment et à l'endroit qui nous conviennent, à des fins dissuasives, opérationnelles et dans le respect du droit national et international.

**Notre approche**

6.5.3. Pour y parvenir :

• nous investirons dans notre NOCP — partenariat entre le ministère de la Défense et GCHQ, qui mobilise les compétences et les talents des deux organisations pour mettre en œuvre les outils, les techniques et l'expérience requis ;
• nous développerons notre maîtrise des outils informatiques offensifs et
• nous développerons la capacité de nos forces armées à déployer des cybercapacités offensives dans le cadre de leurs opérations, renforçant ainsi l'impact global de notre action militaire.

**Evaluation**

6.5.4. Le Gouvernement mesurera le succès de ses initiatives d'établissement de cybercapacités offensives, en évaluant les progrès réalisés vers les résultats suivants :

• le Royaume-Uni compte parmi les chefs de file mondiaux du domaine des cybercapacités offensives et
• le Royaume-Uni a établi un vivier de compétences et d'expertise, pour développer et déployer ses cybercapacités offensives souveraines.

## 6.6. AMÉLIORER LES CAPACITÉS SOUVERAINES — CRYPTOGRAPHIE

6.6.1. La capacité cryptographique est fondamentale, pour protéger nos informations les plus sensibles et décider de la manière de déployer nos forces armées et nos capacités de sécurité nationale. Afin de maintenir cette capacité, nous devrons faire appel à des compétences et technologies du secteur privé, assurées par GCHQ. Ce travail devra vraisemblablement être exécuté au Royaume-Uni, par des ressortissants britanniques possédant l'habilitation de sécurité requise, travaillant pour des entreprises prêtes à discuter ouvertement avec GCHQ des détails de conception et de mise en œuvre. Le MoD et GCHQ s'efforcent de bien appréhender les budgets à long terme associés à l'entretien de telles capacités cryptographiques souveraines, en se basant sur les conditions de marché actuelles et en coopérant avec les sociétés capables de fournir de telles solutions.

**Objectif**

6.6.2. Nous sommes confiants que le Royaume-Uni aura toujours la maîtrise politique des capacités cryptographiques essentielles à la sécurité du pays et par conséquent, les moyens de protéger les secrets de la Nation.

**Notre approche**

6.6.3. Nous sélectionnerons les moyens qui nous permettront de partager efficacement l'information avec nos alliés et veillerons à ce que des renseignements et des systèmes informatiques fiables soient disponibles en temps et lieu voulus. En collaboration étroite avec d'autres ministères et agences, GCHQ et le MoD définiront les conditions souveraines et la meilleure façon de les satisfaire pour les fournisseurs nationaux. Un nouveau cadre commun sera créé pour déterminer les conditions en matière d'avantage opérationnel et de liberté d'action.

**Évaluation**

6.6.4. Le Gouvernement mesurera le succès de ses initiatives d'entretien de ses capacités cryptographiques, en évaluant les progrès réalisés vers le résultat suivant :

• nos capacités cryptographiques souveraines protègent efficacement nos secrets et nos informations sensibles, contre les divulgations non autorisées.

**CHIFFREMENT**

Le chiffrement est le processus d'encodage de données ou d'informations visant à les protéger contre le risque d'accès non autorisé.

Le Gouvernement est favorable au chiffrement, pierre angulaire d'une économie Internet puissante : il protège les données personnelles des citoyens et la propriété

intellectuelle, tout en sécurisant le commerce en ligne.

Or, tandis que les technologies continuent d'évoluer, nous devons veiller à ce qu'aucun « espace sûr » ne permette aux terroristes et aux criminels d'opérer hors d'atteinte de la justice.

Au fil de l'évolution des technologies, les pouvoirs publics souhaitent œuvrer avec l'industrie pour faire en sorte que, fortes d'un cadre juridique solide et d'une supervision claire, la police et les agences du renseignement puissent accéder au contenu des communications des terroristes et des criminels. La législation actuelle autorise l'interception des communications des criminels et des terroristes, avec un mandat judiciaire. Les entreprises ont le devoir de donner suite à ces mandats et de soumettre les communications demandées aux autorités compétentes. En cas de présentation d'un mandat judiciaire, les entreprises doivent désactiver le chiffrement, qu'il ait été activé par l'entreprise elle-même ou par un tiers en leur nom, pour que le matériel soumis soit lisible. La loi stipule que les entreprises sont tenues de prendre des mesures raisonnables pour donner suite aux mandats judiciaires ; l'analyse du caractère raisonnable de leur démarche en ce sens, passe notamment par l'évaluation des mesures que l'entreprise doit prendre pour désactiver le chiffrement.

# 7. DÉVELOPPER

7.0.1. L'axe « DÉVELOPPER » de la stratégie porte sur la manière dont nous nous procurerons et consoliderons les outils et capacités dont doit se munir le Royaume-Uni, pour se protéger des menaces informatiques.

7.0.2. Le Royaume-Uni doit augmenter ses effectifs de professionnels compétents et qualifiés dans les métiers de la cybersécurité. Le Gouvernement agira immédiatement pour combler le fossé entre la demande et l'offre de postes clés dans ce domaine, tout en redonnant de la vigueur aux programmes d'éducation et de formation dédiés à cette filière. Il s'agit d'un objectif transformateur à long terme. Cette stratégie posera les premières pierres de cet important chantier, qui se poursuivra nécessairement au-delà de 2021. Une main-d'œuvre compétente est l'élément moteur d'un écosystème commercial de cybersécurité dynamique et mondialement réputé. Cet écosystème veillera à ce que les start-ups du cyberespace prospèrent et bénéficient des investissements et du soutien dont elles ont besoin. Cette innovation et cette vigueur ne peuvent venir que du secteur privé ; toutefois, les pouvoirs publics l'accompagneront dans son développement et dans la promotion active du secteur de la cybersécurité sur le marché mondial. Un secteur de la recherche scientifique dynamique et florissant, est la condition sine qua non de l'épanouissement de personnes hautement qualifiées et de la concrétisation d'idées novatrices en produits de pointe.

## 7.1. RENFORCER LES COMPÉTENCES DE CYBERSÉCURITÉ

7.1.1. Le Royaume-Uni doit traiter les problématiques systémiques au cœur de la pénurie de cyber-compétences : insuffisance du contingent de jeunes choisissant la filière, manque de spécialistes de la cybersécurité à jour de leurs compétences, couverture insuffisante des concepts de cybersécurité et de sécurité de l'information par les cours d'informatique, pénurie d'enseignants qualifiés et absence de plans de carrière et de parcours de formation vers la profession.

7.1.2. Ces insuffisances nécessitent une intervention rapide du Gouvernement, afin de lutter contre la pénurie actuelle et de formuler une stratégie cohérente à long terme, susceptible de capitaliser ces interventions pour combler le déficit de compétences. Toutefois, force est de reconnaître que pour avoir un effet radical, cet effort doit être collaboratif et entrepris avec le concours de divers participants, d'influenceurs des administrations décentralisées, du secteur public, de l'enseignement, des milieux universitaires et de l'industrie.

**Objectif**

7.1.3. L'ambition du Gouvernement est d'assurer l'approvisionnement soutenu des meilleurs talents britanniques possible dans le domaine de la cybersécurité et dans l'immédiat, de financer des interventions ciblées visant à combler les déficits de compétence connus. D'autre part, nous définirons et développerons, au sein de la population et des effectifs actifs, les compétences de cybersécurité requises pour profiter de l'Internet en toute sécurité.

7.1.4. Il ne s'agit pas d'un projet sur cinq, mais sur vingt ans. Nous définirons l'ensemble de mesures à long terme, coordonnées dont auront besoin les pouvoirs publics, l'industrie, les enseignants et les universitaires, pour

établir une source durable de professionnels des métiers de la cybersécurité, en adéquation avec les normes et certifications requises pour exercer avec confiance et en toute sécurité.

7.1.5. Nous comblerons le déficit de compétences dans la Défense. Le Gouvernement recrutera des cyber-spécialistes efficacement formés, prêts à protéger notre sécurité nationale. La compréhension de l'impact du cyberespace sur les opérations militaires s'impose donc.

**Notre approche**

7.1.6. Nous développerons et mettrons en œuvre une stratégie de formation autonome, visant à consolider l'effort actuel d'intégration de la cybersécurité dans le système éducatif. Cette stratégie contribuera aussi à l'amélioration de l'état général de l'enseignement de l'informatique et à l'incorporation de la cybersécurité dans les programmes scolaires. Les étudiants en informatique, en technologie ou en compétences numériques, apprendront les principes fondamentaux de la cybersécurité pour apporter leurs qualifications au marché du travail. Dans le cadre de cet effort, nous traiterons la question du déséquilibre hommes-femmes dans les professions du cyberespace et nous tournerons vers les personnes issues de milieux plus divers, afin de pouvoir compter sur le plus large possible des viviers de talents. Nous travaillerons en étroite collaboration avec les administrations décentralisées, pour favoriser l'adoption d'une démarche cohérente sur l'ensemble du territoire.

7.1.7. Nous formulerons plus clairement les rôles respectifs des pouvoirs publics, de l'industrie et la manière dont ils pourraient évoluer dans le temps. Le Gouvernement britannique et les administrations décentralisées, ont un rôle clé à jouer dans la création d'un environnement favorable au développement des compétences de cybersécurité et l'actualisation du système éducatif, afin de refléter les besoins changeants de l'industrie et de l'administration publique. Les employeurs n'en ont pas moins la responsabilité importante d'exprimer clairement leurs besoins, de former et développer leurs salariés et les jeunes qui entrent dans la profession. L'industrie a un rôle important à jouer dans la mise en place de plans de carrière et de parcours de formation variés et attrayants, en partenariat avec les universités, organismes agréés et associations professionnelles.

7.1.8. Conscients que la réduction du déficit de compétences représente un enjeu collectif, nous créerons un groupe consultatif sur les compétences formé d'agents de la fonction publique, d'employeurs, d'organismes professionnels, de centres de formation, de prestataires de services éducatifs et d'universitaires. Il renforcera la cohérence entre ces secteurs clés, tout en favorisant le développement d'une stratégie à long terme, qui tiendra compte des innovations dans le vaste domaine des compétences numériques et veillera à l'alignement et à l'incorporation permanents des préoccupations de cybersécurité. Ce groupe coopérera avec des organes similaires sur tout le territoire britannique.

7.1.9. En parallèle, le Gouvernement investira dans diverses initiatives porteuses d'améliorations immédiates et qui serviront de base au développement d'une stratégie de formation à long terme. Ces initiatives sont les suivantes :

• établir un programme scolaire pour transformer radicalement l'enseignement et les formations spécialisées dans le domaine de la cybersécurité, à destination des jeunes talents de 14 à 18 ans (programme à base

d'activités en classe, de tutorats spécialisés après l'école, de projets mobilisateurs et de stages d'été) ;
• créer des apprentissages aux niveaux avancé et universitaire dans les secteurs de l'énergie, des finances et des transports, pour lutter contre les déficits de compétences dans ces domaines essentiels ;
• créer un fonds de reclassement des candidats qui travaillent déjà et qui présentent un potentiel prometteur pour les métiers de la cybersécurité ;
• identifier et épauler les programmes de cybersécurité de qualité aux niveaux licence et master, identifier et remédier aux pénuries de compétences spécialisées — en reconnaissant le rôle déterminant que jouent les universités dans le développement des compétences ;
• soutenir l'accréditation de la formation professionnelle des enseignants en cybersécurité. Cette initiative permettra aux enseignants et aux autres soutiens d'apprentissage de mieux comprendre la pédagogie de la cybersécurité et leur proposera une méthode d'accréditation externe ;
• développer la profession de la cybersécurité, notamment grâce au statut Royal Chartered (Charte royale) d'ici 2020, pour renforcer la reconnaissance du corpus d'excellence en cybersécurité au sein de l'industrie et fournir un point focal capable de conseiller, influer sur et façonner la politique nationale ;
• développer une Académie de la cyberdéfense, servant de centre d'excellence pour la formation et les exercices en cybersécurité sur l'ensemble du ministère de la Défense, traiter les compétences spécialisées et l'éducation au sens large ;
• chercher les opportunités de collaboration en matière de formation et d'enseignement, entre les pouvoirs publics, les forces armées, l'industrie et les milieux universitaires, ainsi que des installations pour entretenir et pratiquer les compétences acquises ;
• œuvrer avec l'industrie pour étendre le programme *CyberFirst*, afin d'identifier et d'alimenter le riche vivier de jeunes talents pour défendre notre sécurité nationale et
• imbriquer la cybersécurité et les compétences numériques dans les cours du système éducatif qui conviennent, de l'école primaire au troisième cycle universitaire, en fixant des normes, en améliorant la qualité et en fournissant une base solide d'évolution de carrière dans cette filière.

L'éducation étant un dossier décentralisé, certaines de ces initiatives s'appliqueront principalement à l'Angleterre. Nous collaborerons toutefois avec les administrations décentralisées pour favoriser le développement d'une approche cohérente sur l'ensemble des systèmes éducatifs britanniques.

**Évaluation**

7.1.10. Le Gouvernement mesurera le succès de ses initiatives de renforcement des compétences de cybersécurité, en évaluant les progrès réalisés vers les résultats suivants :

• les filières efficaces et claires d'accès aux métiers de la cybersécurité attirent des candidats très divers ;
• à l'horizon 2021, la cybersécurité sera enseignée efficacement dans le cadre de cours pertinents, de l'école primaire au troisième cycle universitaire ;
• la cybersécurité est largement reconnue comme étant une profession établie, associée à des parcours de carrière précis et par le Royal Chartered Status ;
• les connaissances appropriées en cybersécurité font partie intégrante de la formation continue des professionnels non spécialisés dans la cybersécurité, tous secteurs de l'économie confondus et
• le Gouvernement et les forces armées disposent de spécialistes de la cyberdéfense,

capables de préserver la sécurité et la résilience du Royaume-Uni.

## 7.2. STIMULER LA CROISSANCE DANS LE SECTEUR DE LA CYBERSÉCURITÉ

7.2.1. Notre économie numérique moderne doit impérativement pouvoir compter sur un secteur de la cybersécurité innovant et en plein essor. Les sociétés britanniques de cybersécurité comptent parmi les leaders mondiaux des technologies, formations et conseils à destination de l'industrie et des gouvernements. Toutefois, même si le Royaume-Uni fait figure de chef de file, il doit faire face à une concurrence redoutable pour conserver son avance. En outre, le Gouvernement devra franchir certains obstacles. Les entreprises et milieux universitaires britanniques développent des technologies de pointe, mais certains d'entre eux ont besoin d'être épaulés pour développer les aptitudes commerciales et entrepreneuriales nécessaires pour prospérer. Les déficits de financement freinent la croissance des PME et les empêchent de conquérir de nouveaux marchés et territoires. Les produits et services les plus révolutionnaires, qui pourraient nous permettre de garder notre avance sur la menace, ont du mal à trouver des clients disposés à jouer le rôle d'adopteurs précoces. Pour surmonter ces difficultés, les pouvoirs publics, l'industrie et les milieux universitaires doivent collaborer efficacement.

### Objectif

7.2.2. Le Gouvernement favorisera la création d'un secteur dynamique, novateur et prospère de la cybersécurité au Royaume-Uni afin de créer un écosystème où :

• les sociétés de sécurité s'épanouissent et bénéficient des investissements dont elles ont besoin pour le faire ;
• les cerveaux les plus brillants issus des administrations, des milieux universitaires et du secteur privé travaillent en étroite collaboration pour stimuler l'innovation et
• la clientèle du Gouvernement et de l'industrie est suffisamment confiante et disposée à adopter des services de pointe.

### Notre approche

7.2.3. Afin de créer cet écosystème :

• nous commercialiserons l'innovation dans le milieu de la recherche, en proposant aux universitaires des solutions de formation et de mentorat ;
• nous établirons deux centres d'innovation, pour dynamiser le développement de cyberproduits de pointe et de jeunes entreprises de cybersécurité dynamiques. Ces centres s'inscriront au cœur d'un programme d'initiatives pour aider les start-ups à trouver leurs premiers clients et à attirer d'autres investisseurs ;
• nous affecterons une part des 165 millions GBP (environ 195 m €) du Fonds pour la défense et la cyber-innovation au soutien d'une passation de marchés innovante dans la défense et la sécurité ;

• nous mettrons à la disposition des entreprises des centres d'essai pour développer leurs produits, ainsi qu'une forme d'évaluation en voie accélérée pour la prochaine génération de produits et services de cybersécurité émergents, pour que les clients puissent avoir confiance en leur utilisation ;
• nous tirerons parti de l'expertise collective du partenariat industrie-gouvernement pour la cyber-croissance (Cyber Growth Partnership), pour continuer à façonner et focaliser la croissance et les interventions innovantes ;

• nous faciliterons l'expansion et l'accès aux marchés internationaux des entreprises, toutes tailles confondues et
• nous favoriserons l'adoption de normes internationales communes propices à l'accès au marché britannique.

7.2.4. Nous profiterons également du poids des marchés publics pour stimuler l'innovation. Les défis et menaces de cybersécurité auxquels le Gouvernement est confronté, comptent respectivement parmi les plus difficiles à traiter et les plus lourdes. Non seulement nous pouvons chercher les solutions les plus efficaces à ces problèmes, mais nous devons le faire. D'où la nécessité de faciliter la coopération entre les petites entreprises et les pouvoirs publics. D'autre part, le Gouvernement doit être moins réticent à l'idée d'essayer et d'adopter les nouveaux produits. La solution est gagnant-gagnant : le Gouvernement en tirera les services les plus performants, les technologies innovantes pourront compter sur un adopteur précoce et auront moins de mal à attirer les investisseurs et élargir leur clientèle. Nous encouragerons toutes les branches de l'administration publique, dont les administrations décentralisées, à adopter une approche similaire.

« Nous souhaitons créer un cyber-écosystème où les start-ups de la cybersécurité prolifèrent, bénéficient des investissements et du soutien dont elles ont besoin pour tirer parti des marchés du monde entier et fournir un vivier d'innovations favorable à la circulation des idées entre le secteur privé, les pouvoirs publics et les milieux universitaires. »

Matt Hancock, député,
Ministre adjoint chargé du numérique et de la culture

**Évaluation**

7.2.5. Le Gouvernement mesurera le succès de ses initiatives de dynamisation de la croissance dans le secteur de la cybersécurité, en évaluant les progrès réalisés vers les résultats suivants :

• croissance globale plus forte que la moyenne en glissement annuel, de la taille du secteur britannique de la cybersécurité ;
• accroissement significatif des investissements dans les sociétés en phase de démarrage ;
• adoption par les administrations publiques de technologies de cybersécurité plus novatrices et plus efficaces.

## 7.3. PROMOUVOIR LES SCIENCES ET LES TECHNOLOGIES DANS LE DOMAINE DE LA CYBERSÉCURITÉ

7.3.1. Le secteur florissant des sciences et des technologies du Royaume-Uni et sa recherche de pointe, étayent nos capacités de cybersécurité de classe mondiale. Afin de maintenir et de renforcer notre réputation de leader mondial dans la recherche de pointe, nos établissements de recherche universitaire doivent continuer d'attirer les cerveaux les plus brillants des métiers de la cybersécurité. Pour y parvenir, nous devrons favoriser le développement de centres d'excellence capables d'attirer les scientifiques et les chercheurs les plus dynamiques et les plus doués, approfondir le partenariat actif entre les universités, le Gouvernement et l'industrie. Cette promotion passera, pour le Gouvernement, par un rôle de jumelage visant à stimuler ces collaborations. Le succès nous permettrait d'établir un écosystème autonome facilitant la circulation des idées et des personnes, entre les trois secteurs et de manière symbiotique.

**Objectif**

7.3.2. D'ici à 2021, le Royaume-Uni aura renforcé sa position de leader mondial dans le domaine des cybersciences et cybertechnologies. Des partenariats souples entre les universités et le secteur industriel traduiront la recherche en produits et services commercialement viables. Les capacités d'innovation du Royaume-Uni préserveront leur réputation d'excellence, notamment dans les domaines comptant parmi ses atouts les plus puissants, comme le secteur financier.

**Notre approche**

7.3.3. Pour y parvenir, le Gouvernement encouragera la collaboration, les modèles de financement de la recherche souples et innovants et la commercialisation des activités de recherche. Il veillera à ce que les aspects humains et comportementaux de la cybernétique soient suffisamment pris en compte et à ce que les systèmes non techniques, comme les processus d'entreprise et structures organisationnelles par exemple, soient inclus dans les cybersciences et cybertechnologies.

7.3.4. Cette approche soutiendra la création de produits, systèmes et services « sécurisés par défaut », la sécurité nécessaire étant prise en compte *ab initio*, dans un scénario où la décision du « rejet » est l'effet d'un choix conscient de la part de l'utilisateur.

7.3.5. Nous publierons une Stratégie de cybersciences et cybertechnologies détaillée, issue d'une concertation exhaustive avec nos partenaires et parties prenantes. Nous devrons notamment identifier les domaines scientifiques et technologiques que le Gouvernement, l'industrie et les universitaires jugent importants et recenser les capacités lacunaires actuelles du Royaume-Uni, pour y remédier.

7.3.6. Le Gouvernement continuera de financer et soutenir les centres d'excellence universitaire, instituts de recherche et centres de formation doctorale. Nous créerons également un nouvel Institut de recherche dans une discipline d'importance stratégique. Par ailleurs, nous financerons des recherches plus poussées dans les domaines où la prochaine Stratégie de cybersciences et cybertechnologies identifie des manques de capacité. La recherche portera notamment sur les domaines importants suivants : analytique du Big Data ; systèmes autonomes ; systèmes de contrôle industriels fiables ; systèmes cyber-physiques et Internet des objets ; villes intelligentes ; vérification des systèmes automatisée ; science de la cybersécurité.

7.3.7. Nous continuerons de parrainer les doctorants britanniques dans les centres universitaires d'excellence, pour pouvoir compter sur des réserves de ressortissants cyberexperts.

7.3.8. Le Gouvernement collaborera avec des organismes pertinents et notamment avec *Innovate UK* et les Conseils de la recherche (Research Councils), pour encourager la coopération entre l'industrie, le Gouvernement et les milieux universitaires. Afin de soutenir cette collaboration, nous ferons le point sur les meilleures pratiques de classification de sécurité et identifierons les experts, universitaires inclus, ayant satisfait aux exigences d'habilitation de sécurité. Cette intiative permettra de faire en sorte que le travail accompli dans l'espace non classifié et au-delà du secret, soit aussi collaboratif que possible.

7.3.9. Le Gouvernement financera un « grand défi » pour trouver et apporter des solutions inédites aux problèmes de cybersécurité les plus urgents. *CyberInvest*, nouveau partenariat entre l'industrie et le

Gouvernement pour soutenir la recherche de pointe en cybersécurité et protéger le Royaume-Uni dans le cyberespace, fera partie de notre approche visant à consolider le partenariat universités-administration publique-industrie.

**Évaluation**

7.3.10. Le Gouvernement mesurera le succès de ses initiatives de promotion des cybersciences et cybertechnologies, en évaluant les progrès réalisés vers les résultats suivants :

• augmentation considérable du nombre de sociétés britanniques ayant réussi à commercialiser les fruits de la cyber-recherche universitaire, diminution du nombre de capacités lacunaires convenues et identifiées à l'échelle nationale dans le domaine de la recherche en cybersécurité et application de mesures efficaces pour y remédier et
• le Royaume-Uni est considéré comme un leader mondial de la recherche et de l'innovation en cybersécurité.

## 7.4. POUR UNE ANALYSE PROSPECTIVE EFFICACE

7.4.1. Le Gouvernement doit s'assurer que l'élaboration des politiques tient compte de l'évolution du paysage virtuel, géopolitique et technologique. D'où la nécessité de recourir efficacement à l'analyse prospective et à l'évaluation étendues. Nous devons investir dans notre protection contre les menaces futures, tout en anticipant une évolution des marchés susceptibles d'avoir une incidence sur notre cyber-résilience au cours des cinq à dix prochaines années. Nous avons besoin de programmes d'analyse prospective capables d'émettre les recommandations qui serviront de base à la politique et à la planification des programmes du gouvernement, aujourd'hui comme demain.

**Objectif**

7.4.2. Le Gouvernement veillera à ce que nos programmes d'analyse prospective comportent une évaluation rigoureuse du cyberrisque, intégrée à l'élaboration des domaines de développement de politiques de cybersécurité et d'autres technologies, parallèlement à l'évaluation de toutes les sources et aux autres preuves disponibles. Nous coordonnerons l'analyse prospective entre la sécurité nationale et les autres domaines de politique, pour être sûrs de bénéficier d'une évaluation holistique des enjeux et opportunités émergents.

**Notre approche**

7.4.3. Nous :

• recenserons les lacunes des travaux actuels et coordonnerons les activités sur une base interdisciplinaire, dans le but d'élaborer une approche holistique en matière d'analyse prospective appliquée à la cybersécurité ;
• favoriserons l'intégration plus systématique des aspects techniques de la cybersécurité à la science du comportement ;
• soutiendrons une surveillance rigoureuse du marché de la cybercriminalité, afin de repérer les nouveaux outils et services susceptibles de faciliter les transferts de technologie vers des États hostiles, des terroristes ou des criminels ;
• analyserons les technologies émergentes de contrôle de processus connectés ;
• anticiperons les vulnérabilités des monnaies électroniques et
• suivrons les tendances du marché des technologies des télécommunications, afin de déployer des moyens de défense précoces contre les attaques anticipées.

7.4.4. Nous sommes conscients qu'au-delà du cadre technique, l'analyse prospective englobe les dimensions politique, économique, législative, sociale et environnementale. La cybersécurité n'est qu'une facette des questions qu'une analyse prospective efficace peut aider à traiter. En conséquence, nous veillerons à ce que tout exercice d'analyse prospective orienté vers ces autres domaines de politique, tienne compte de ses éventuelles conséquences pour la cybersécurité.

7.4.5. En outre, nous ferons en sorte que la prise de décisions de cybersécurité se base sur une approche fondée sur des données probantes, tenant compte des analyses de toutes les sources disponibles. Il s'agira entre autres :

• de données techniques précises sur l'Internet des objets ou le futur rôle des matériaux, par exemple et
• de tendances stratégiques et sociétales internationales et de leurs effets sur la cybernétique.

7.4.6. Nous veillerons à ce que la cybersécurité soit considérée comme relevant de la Cellule interministérielle d'analyse des technologies émergentes et de l'innovation (sigle anglais ETIAC), qui sera créée pour détecter les menaces et opportunités technologiques pertinentes pour la sécurité nationale. Nous veillerons en outre à ce que la cybersécurité soit prise en compte par les mécanismes de veille prospective existants, dont le *Government Futures Group* (sigle anglais GFG), et le Groupe consultatif du Conseil des ministres sur la veille prospective (sigle anglais CSAG).

**Évaluation**

7.4.7. Le Gouvernement mesurera le succès de ses initiatives d'établissement d'une capacité de veille prospective efficace, en évaluant les progrès réalisés vers les résultats suivants :

• la veille prospective interministérielle et l'évaluation de toutes les sources sont intégrées à l'élaboration de la politique de cybersécurité et
• les effets de la cybersécurité sont pris en compte dans toutes les analyses prospectives interministérielles.

# 8. ACTION INTERNATIONALE

8.1. Notre prospérité économique et notre bien-être social, dépendent de plus en plus de l'ouverture et de la sécurité de réseaux dont la portée dépasse largement nos propres frontières. Nous devons impérativement travailler en étroite collaboration avec nos partenaires internationaux, pour garantir la pérennité d'un cyberespace libre, ouvert, paisible et sûr, propice au maintien de ces avantages. L'arrivée du prochain milliard d'Internautes à l'échelle planétaire, ne peut qu'accentuer l'importance de cette collaboration.

8.2. La coopération internationale pour traiter les questions de cybersécurité, fait désormais partie des éléments essentiels d'un débat plus général sur l'économie et la sécurité mondiales. Ce domaine politique évolue rapidement, sans faire l'objet de la moindre vision internationale commune. Le Royaume-Uni et ses alliés ont réussi à mettre en place certains éléments d'un système international fondé sur des règles : il a été convenu que le droit international s'applique dans le cyberespace ; que les droits de l'homme doivent être respectés en ligne comme dans le monde réel. D'autre part, un consensus largement majoritaire convient qu'une approche multipartite est le meilleur moyen de gérer les complexités liées à la gouvernance de l'Internet. Néanmoins, au vu des opinions de plus en plus divisées sur la façon de relever le défi commun lié à la conciliation de la sécurité nationale, les droits et libertés individuelles, tout consensus mondial demeure fragile.

« Nous devons œuvrer à l'échelle internationale pour convenir des règles de la voie à suivre pour garantir la sécurité et la prospérité à venir du Royaume-Uni dans le cyberespace. »

M. Boris Johnson, député,
Ministre des Affaires étrangères et du Commonwealth

**Objectifs**

8.3. L'objectif du Royaume-Uni est de garantir la pérennité d'un cyberespace libre, ouvert, paisible et sûr, moteur de la croissance économique et pilier de la sécurité nationale de notre Nation. Sur cette base, le Royaume-Uni continuera à prôner le modèle multipartite de gouvernance de l'Internet, à s'opposer à la localisation des données et s'efforcera de renforcer la capacité de nos partenaires à améliorer leur propre cybersécurité. Afin de réduire la menace qui pèse sur notre pays, nos intérêts et vient en grande partie de l'étranger, nous chercherons à influencer le processus décisionnel des auteurs d'actes de cybercriminalité, de cyberespionnage et se livrant à des activités déstabilisatrices ou destructrices en ligne, tout en renforçant les cadres de soutien de la coopération internationale.

**Notre approche**

8.4. Pour y parvenir :

• nous renforcerons et intégrerons une conception commune du comportement responsable des États dans le cyberespace ;
• nous bâtirons sur l'accord selon lequel le droit international s'applique dans le cyberespace ;• nous continuerons à promouvoir l'adoption de normes volontaires, non contraignantes pour encadrer le comportement responsable des États ;

• nous soutiendrons la conception et la mise en œuvre de mesures de renforcement de la confiance ;
• nous renforcerons nos moyens de déstabiliser et de poursuivre les cybercriminels opérant de l'étranger, surtout dans les juridictions difficilement accessibles ;
• nous encouragerons un environnement propice à la coopération mutuelle des services répressifs, pour réduire le nombre d'endroits où les cybercriminels peuvent agir sans craindre de faire l'objet d'enquêtes et de poursuites ;
• nous augmenterons la résilience du cyberespace en façonnant les normes techniques régissant les technologies émergentes à l'échelle internationale (chiffrement inclus), pour faire du cyberespace un environnement plus « intrinsèquement sécurisé » et favoriser l'adoption des meilleures pratiques ;
• nous chercherons des approches communes entre pays partageant des valeurs similaires, notamment sur le plan de capacités comme le chiffrement puissant, par exemple, dont les corollaires dépassent les frontières ;
• nous renforcerons les moyens de lutte dont disposent les autres pays contre les menaces visant le Royaume-Uni et ses intérêts à l'étranger ;
• nous continuerons d'aider nos partenaires à développer leur propre cybersécurité : partageant le même cyberespace, nous sommes plus forts collectivement lorsque chaque pays améliore ses propres moyens de défense ;
• nous ferons en sorte que l'OTAN soit prête à faire face aux conflits du XXI$^{e}$ siècle, aussi bien dans le cyberespace que sur les champs de bataille ;
• nous travaillerons avec nos alliés pour permettre à l'OTAN d'opérer aussi efficacement dans le cyberespace que sur terre, en mer et dans les airs et
• nous veillerons à ce que le « Processus de Londres », cycle de conférences internationales sur le cyberespace, continue de promouvoir le consensus mondial en faveur d'un cyberespace libre, ouvert, paisible et sûr.

8.5. Conscients que nous n'y parviendrons pas en nous isolant, nous continuerons d'investir dans divers partenariats et outils afin de réaliser et d'étayer nos objectifs cybernétiques internationaux. Nous nous efforcerons donc notamment :

• d'œuvrer de concert avec nos alliés traditionnels et de nouveaux partenaires, pour nouer et entretenir des relations politiques et opérationnelles solides, tout en créant les conditions politiques propices à la construction d'alliances mondiales puissantes ;
• d'exercer notre influence auprès d'instances multilatérales comme les Nations Unies, le G20, l'Union européenne, l'OTAN, l'OSCE, le Conseil de l'Europe, le Commonwealth et au sein de la communauté internationale du développement et
• de renforcer nos relations avec les acteurs non étatiques — l'industrie, la société civile, les milieux universitaires et la communauté technique. Capables d'influencer et de remettre en question la formulation des politiques internationales, ces acteurs jouent un rôle essentiel dans la consolidation des messages politiques portant sur un large éventail de problématiques cybernétiques. Nos liens universitaires de renommée mondiale sont une plateforme neutre, favorable à la collaboration avec nos partenaires internationaux.

**Évaluation**

8.6 Le Gouvernement mesurera le succès de ses initiatives de défense de nos intérêts cybernétiques internationaux, en évaluant les progrès réalisés vers les résultats suivants :

• la collaboration internationale renforcée réduit la menace cybernétique qui pèse sur le Royaume-Uni et sur ses intérêts à l'étranger ;
• le comportement responsable des États dans le cyberespace, fait l'objet d'une compréhension commune ;
• les partenaires internationaux ont augmenté leurs moyens de cybersécurité et
• le consensus international relatif aux avantages d'un cyberespace libre, ouvert, paisible et sûr, a été renforcé.

# 9. MÉTRIQUES

9.1. S'agissant de mesurer ses résultats et impacts — en appliquant des « métriques » selon le terme habituel, la cybersécurité reste un domaine relativement nouveau. La science de la cybersécurité souffre déjà du voile de l'hyperbole et du manque de données étalonnées. Cette réalité est frustrante pour les décideurs et les entreprises, qui tentent tant bien que mal de mesurer l'investissement par rapport aux résultats obtenus. Selon le Gouvernement, l'utilisation efficace de métriques est primordiale, pour concrétiser cette stratégie et concentrer ses ressources porteuses.

9.2. Nous ferons en sorte que la présente stratégie repose sur un ensemble rigoureux et complet de métriques, servant à mesurer les progrès réalisés vers les résultats visés. Livrable déterminant à part entière de cette stratégie, le NCSC jouera également un rôle crucial dans l'effort visant à aider d'autres secteurs du Gouvernement, l'industrie et la société à réaliser la totalité de ses objectifs stratégiques.

9.3. L'annexe 3 de ce document explique comment les mesures du succès définies dans le cadre de la stratégie contribueront aux résultats stratégiques, lesquels feront l'objet d'un bilan annuel vérifiant leur adéquation précise avec nos buts et impératifs nationaux. Les principaux résultats stratégiques sont les suivants :

1. Le Royaume-Uni dispose des capacités de détecter, d'analyser et de contrer efficacement la menace émanant des cyberactivités de nos ennemis.

2. L'impact de la cybercriminalité au Royaume-Uni et sur ses intérêts est considérablement réduit et les cybercriminels sont dissuadés de cibler le territoire britannique.

3. Le Royaume-Uni dispose de capacités efficaces pour gérer les cyberincidents et réagir en conséquence, réduire les dommages subis par le pays et contrer ses ennemis cybernétiques.

4. Nos partenariats de cyberdéfense active avec l'industrie neutralisent les attaques de grande envergure par hameçonnage et maliciels.

5. Le Royaume-Uni est plus sûr depuis que les produits et services technologiques sont munis, dès la conception, de mesures de cybersécurité intrinsèque, activées par défaut.

6. Les réseaux et services du Gouvernement seront aussi sécurisés que possible dès leur mise en œuvre. Le public pourra utiliser les services numériques de l'administration publique en toute confiance, sachant que ses informations sont protégées.

7. Les organisations du Royaume-Uni, petites et grandes, gèrent efficacement leur cyberrisque et bénéficient des conseils de grande qualité du NCSC, associés à un mélange équilibré de réglementation et de mesures incitatives.

8. Le Royaume-Uni dispose d'un écosystème propice au développement et à la pérennisation d'un secteur de la

cybersécurité capable de répondre à ses exigences en matière de sécurité nationale.

9. Le Royaume-Uni possède un vivier durable de professionnels de la cybernétique britanniques, qualifiés pour répondre à la demande croissante d'une économie de plus en plus numérisée, dans les secteurs public, privé et dans celui de la défense.

10. Le Royaume-Uni est universellement reconnu comme comptant parmi les chefs de file mondiaux de la recherche et du développement dans la cybersécurité, soutenus par l'expertise de haut niveau de l'industrie et des milieux universitaires britanniques.

11. À l'épreuve du temps, le gouvernement britannique planifie et prépare déjà la mise en œuvre de sa politique avant l'émergence des technologies et menaces futures.

12. L'élargissement du consensus et des capacités internationaux favorables à l'adoption par les États d'un comportement responsable dans un cyberespace libre, ouvert, paisible et sûr, réduit la menace à l'encontre du Royaume-Uni et de ses intérêts à l'étranger.

13. Les politiques, organisations et structures du Gouvernement britannique sont simplifiées, pour maximiser la cohérence et l'efficacité de la réaction du Royaume-Uni face aux cybermenaces.

9.4. Un certain nombre des ambitions de cette stratégie se projettent au-delà de son échéance quinquennale. Soucieux de veiller à ce que les prochains investissements dans la cybersécurité dont l'échéance dépasse 2021 expriment tout leur potentiel transformateur, nous souhaitons que l'industrie, les régulateurs, auditeurs, assureurs et autres acteurs des secteurs public et privé, continuent de bénéficier de ces résultats à plus long terme, au-delà de 2021, suite à l'intégration de la gestion efficace des risques de cybersécurité à l'activité type de gestion généralisée.

# CONCLUSION : LA CYBERSÉCURITÉ AU-DELÀ DE 2021

10.1. L'évolution rapide du paysage cybernétique catalysée par des progrès technologiques que nos ennemis s'acharnent à exploiter, nous obligera constamment à relever de nouveaux défis. Cela étant, le but de cette stratégie est de fournir une panoplie de politiques, outils et moyens susceptibles de nous permettre de réagir rapidement et avec souplesse à chaque occurrence d'un nouveau défi.

10.2. Sauf action efficace de notre part, la menace continuera de devancer notre capacité de protection. L'explosion des capacités de menace est une probabilité réelle, à tous les niveaux.

10.3. En revanche si nous réalisons ces ambitions, tous les organes du Gouvernement, de l'industrie et de la société contribueront à assurer la cybersécurité globale de notre pays. Si nous parvenons à faire en sorte que la sécurité soit conçue et intégrée par défaut dans les technologies dites « de commodité », les consommateurs et les entreprises auront moins de raisons de s'inquiéter de la cybersécurité. La consolidation de sa réputation de milieu transactionnel connecté sécurisé, encouragerait davantage de multinationales et d'investisseurs à s'implanter au Royaume-Uni. La sécurité des réseaux CNI et des secteurs prioritaires serait plus efficace. Les agresseurs potentiels cherchant à mettre au point des outils et méthodes d'attaque contre les systèmes hébergeant des fonctions et des données vitales, auraient à leur tour plus de mal à traverser les couches de sécurité prévues pour les protéger. Ces mesures modifieraient l'équation risque contre récompense aux yeux des cybercriminels et des entités malveillantes, qui s'attendraient à devoir faire face au même risque de poursuite internationale, qu'en cas de délit conventionnel. La réussite de nos inititiatives d'intégration de la cybersécurité, tous secteurs de la société confondus, permettrait au Gouvernement lui-même de se retirer du rôle de premier plan pour laisser le marché, et les technologies catalyser l'évolution de la cybersécurité pour l'ensemble de l'économie et de la société.

10.4. Même dans le cas de figure le plus optimiste et autant pour des raisons d'ampleur que de complexité, cinq années risquent de ne pas suffire pour traiter les défis à relever par le Royaume-Uni dans l'univers cybernétique. Cette stratégie nous dote néanmoins des moyens de transformer notre sécurité future et de garantir notre prospérité dans l'ère numérique.

# ANNEXES

## ANNEXE 1 : SIGLES ET ACRONYMES

**CCA** – Centre for Cyber Assessment [Centre de cyber-évaluation]. Siégeant au sein du NCSC, il se charge des analyses des cybermenaces utilisées dans la formulation de la politique des ministères britanniques.

**CERT** – Computer Emergency Response Team [équipe d'intervention d'urgence informatique].

**CERT-UK** – Équipe d'intervention d'urgence informatique au Royaume-Uni.

**CESG** – Autorité technique nationale pour l'assurance de l'information au Royaume-Uni. Elle fournit un service expert fiable et indépendant, fondé sur la recherche et le renseignement dans le domaine de la sécurité informatique pour le compte du Gouvernement britannique.

**CNI** – Critical National Infrastructure [infrastructure critique nationale]. Éléments critiques de l'infrastructure (actifs, installations, systèmes, réseaux, processus et travailleurs essentiels à leur fonctionnement et à leur facilitation) et dont la perte ou la détérioration pourraient :

a. nuire considérablement à la disponibilité, à l'intégrité ou à la fourniture de services essentiels — notamment des services dont l'intégrité éventuellement compromise pourrait se solder par un nombre important de pertes humaines ou de blessés — sans oublier de lourdes conséquences économiques ou sociales et/ou
b. avoir un impact grave sur la sécurité nationale, la défense nationale ou le fonctionnement de l'État.

**CPNI** – Centre pour la protection de l'infrastructure nationale. Il donne des conseils visant à réduire la vulnérabilité des organisations de l'infrastructure nationale face au terrorisme et à l'espionnage. Il collaborera également avec le NCSC, pour fournir des conseils holistiques en matière de sûreté applicable aux menaces issues du cyberespace.

Le CPNI a tissé des partenariats solides avec les organismes du secteur privé de l'ensemble de l'infrastructure nationale, créant ainsi un milieu fiable où l'information peut être partagée dans l'intérêt mutuel. Un réseau étendu comprenant d'autres ministères et organismes prestataires de services professionnels, complète ces relations directes.

**DDoS** — Attaque par déni de service distribué. Le système informatique est inondé d'un nombre de demandes dépassant ses capacités de réponse, d'où l'impossibilité pour les utilisateurs autorisés d'y accéder.

**GCHQ** – Government Communications Headquarters, centre des activités du renseignement électronique du gouvernement britannique et autorité nationale technique de cybersécurité (sigle anglais NTA).

**MoD** — Ministère de la Défense

**NCA** – National Crime Agency ; organisme gouvernemental non-ministériel.

**NCSC** – National Cyber Security Centre [Centre national de la cybersécurité].

**OSCE** – Organisation pour la sécurité et la coopération en Europe.

**OTAN** – Organisation du traité de l'Atlantique nord.

**PME** – Petites et moyennes entreprises.

**TIC** – Technologies de l'information et des communications.

## ANNEXE 2 : GLOSSAIRE

**Action Fraud** — Centre national britannique de signalement des fraudes et des infractions sur Internet, point central de contact pour le public et les entreprises.

**Authentification** — Procédure de vérification de l'identité ou d'autres attributs d'un utilisateur, d'une procédure ou d'un appareil.

**Vérification des systèmes automatisée** — Mesures permettant de vérifier que les logiciels et le matériel informatique fonctionnent comme prévu et sans erreurs.

**Système autonome** — Ensemble de réseaux IP dont le routage est sous contrôle d'une entité ou d'un domaine spécifiques.

**Big data ou mégadonnées** – Fichiers trop volumineux pour être traités et gérés en temps utile avec des outils logiciels de commodité, ces données nécessitent le recours à des moyens de traitement sur mesure, capables d'en gérer le volume, la vitesse de livraison et la multiplicité des sources.

**Bitcoin** — Monnaie et système de paiement électroniques.

**Exploitation de réseau informatique (CNE)** — cyber-espionnage ; exploitation d'un réseau informatique pour infiltrer un réseau d'ordinateurs cibles et recueillir du renseignement.

**Chiffrement** — Transformation cryptographique de données (le texte en clair) en une forme (le texte chiffré) qui dissimule le sens original de ces données, afin d'empêcher d'en déceler le sens ou de les exploiter.

**Cryptographie** — Science ou étude de l'analyse et du déchiffrement de codes et de chiffres ; cryptanalyse.

**Cyberattaque** — Exploitation délibérée de systèmes informatiques, d'entreprises et de réseaux dépendant du numérique en vue de leur nuire.

**Cybercriminalité (acte de)** — Infraction cyber-dépendante (infraction qui ne peut être commise qu'au moyen de périphériques TIC, ces périphériques étant à la fois l'instrument et la cible de l'infraction) ou infraction facilitée par le cyberespace (infraction pouvant être commise sans périphérique TIC, comme la fraude financière, mais que le recours aux TIC modifie considérablement en termes d'échelle et de portée).

**Cyberdéfense active (ACD)** – Principe de mise en œuvre de mesures de sécurité dans le but de renforcer la sécurité d'un réseau ou d'un système, pour le rendre plus impénétrable.

**Anonymisation** — Utilisation d'outils d'anonymat cryptographiques pour dissimuler ou masquer son identité sur Internet.

**Cyber-écosystème** — Totalité des infrastructures, personnes, procédures, données, technologies de l'information et de la communication interconnectées, ainsi que l'environnement et les conditions qui influencent ces interactions.

**Cyberincident** — Événement qui pose réellement ou potentiellement une menace pour un ordinateur, un appareil ou réseau connectés à l'Internet, à des données traitées,

stockées ou transmises sur ces systèmes — susceptible d'obliger à intervenir pour en atténuer les conséquences.

**CyberInvest** — Programme public et privé de 6,5 millions GBP (env. 7,7 m €), visant à soutenir la recherche de pointe en cybersécurité et à protéger le Royaume-Uni dans le cyberespace.

**Cyber-résilience** — Capacité globale des systèmes et organisations à supporter des cyberincidents et à récupérer en cas de dommages.

**Cybersécurité** — Protection des systèmes interconnectés (matériel informatique, logiciels et infrastructures connexes compris), des données hébergées et des services qu'ils fournissent, contre une tentative d'accès non autorisé, le risque de dommage ou d'usage abusif. Il peut s'agir d'un préjudice causé délibérément par l'opérateur du système ou accidentellement, suite au non-respect des procédures de sécurité ou d'une manipulation par une tierce personne.

**Challenge de cybersécurité** – concours encourageant les individus à tester leurs compétences et à envisager une carrière dans le domaine de la cybernétique.

**Cyberespace** — Réseau interdépendant d'infrastructures technologiques informatiques comprenant l'Internet, les réseaux de télécommunications, systèmes informatiques, appareils interconnectés, processeurs et contrôleurs intégrés. Le cyberespace peut également désigner le monde ou domaine virtuel en tant que phénomène vécu ou concept abstrait.

**Cybermenace** – Toute activité capable de compromettre la sécurité des systèmes informatiques et des appareils interconnectés (matériel informatique, logiciels et infrastructures connexes), les données qu'ils contiennent et les services qu'ils fournissent, ou capable de leur nuire, principalement par des moyens cybernétiques.

**Cyber-offensive** — Utilisation de cyber-capacités pour perturber, bloquer, détériorer ou détruire des réseaux informatiques et des appareils interconnectés.

**Domaine** – Un nom de domaine situe une organisation ou autre entité sur Internet et correspond à une adresse IP (protocole internet).

**Doxing** – Pratique consistant à rechercher ou à pirater les informations personnellement identifiables d'un individu sur Internet, puis à les rendre publiques.

**E-commerce** — Commerce électronique. Échanges commerciaux effectués sur ou facilité par l'Internet.

**Essai de pénétration** — Activités conçues pour tester la résilience d'un réseau ou d'une installation au piratage informatique, autorisées ou sponsorisées par l'organisation qui fait l'objet de l'essai.

**Filoutage ou usurpation d'identité SMS** — Cette technique masque l'origine d'un message SMS en substituant un texte alphanumérique au numéro de portable d'origine (identité de l'expéditeur). Elle peut être utilisée en toute légitimité par un expéditeur pour remplacer son numéro de portable par son propre nom ou le nom de son entreprise, par exemple. Elle peut aussi être utilisée de façon illicite, pour se faire passer frauduleusement pour une autre personne, par exemple.

**Gestion d'incidents** –Gestion et coordination d'activités visant à évaluer et rémédier à la survenue potentielle ou réelle d'un événement cybernétique malveillant,

susceptible de compromettre ou détériorer un système ou un réseau.

**Hameçonnage ou phishing**– Utilisation d'emails provenant apparemment d'une source fiable, pour tromper les destinataires et les inciter à cliquer sur des liens ou pièces jointes malveillants armés de maliciels, ou à partager des informations sensibles avec un tiers inconnu.

**Ingénierie sociale** — Méthode utilisée par les assaillants pour tromper et manipuler leurs victimes, dans le but de leur faire exécuter une action ou divulguer des informations confidentielles.
Ce type d'action passe habituellement par l'ouverture de pages web malveillantes ou d'une pièce jointe contenant un fichier indésirable.

**Initié** — Personne à qui l'on a confié l'accès aux données et aux systèmes informatiques d'une organisation et qui, délibérement, accidentellement ou inconsciemment, l'expose à une cybermenace.

**Intégrité** — Propriété d'une information qui n'a pas été modifiée accidentellement ou délibérément et qui est exacte et complète.

**Internet** — Réseau mondial informatique fournissant divers moyens d'accès à l'information et de communication, il se compose de réseaux interconnectés utilisant des protocoles de communication standardisés.

**Internet des objets** — Ensemble des dispositifs, véhicules, bâtiments et autres objets dotés de composants électroniques, logiciels et capteurs servant à la communication et à l'échange de données sur Internet.

**Internet des objets industriel** (sigle anglais IIoT) — Recours aux technologies de l'Internet des objets dans les secteurs manufacturier et industriel.

**Réponse aux incidents** – Activités traitant les effets directs et à court terme d'un incident et pouvant également favoriser la récupération à court terme.

**Logiciel malveillant dit « de commodité »** — Logiciel malveillant largement disponible à la vente, ou pouvant être téléchargé gratuitement, qui n'a pas été fabriqué sur mesure et est utilisé par un large éventail d'acteurs malveillants.

**Maliciel** — logiciel ou code malveillants. Les virus, vers, chevaux de Troie (CDT) et espiogiciels sont des maliciels (ou logiciels malveillants).

**Marché de la cybercriminalité** — Totalité des produits et services qui soutiennent l'écosystème de la cybercriminalité.

**Patching** – On entend par « patching » ou mise à jour corrective, le processus de mise à jour de logiciels pour corriger les bogues et vulnérabilités.

**Processus de Londres** — Mesures découlant de la conférence de Londres sur le cyberespace organisée en 2011.

**Ransomware ou rançonlogiciel** — Maliciel qui interdit à l'utilisateur d'accéder à ses fichiers, son ordinateur ou son appareil tant qu'une rançon n'a pas été versée.

**Reconnaissance** — Phase d'une attaque où un assaillant recueille des informations, cartographie les réseaux et les explore pour rechercher des vulnérabilités exploitables afin de les pirater.

**Réseau** (d'ordinateurs) — ensemble de serveurs, accompagné de leurs sous-réseau

ou inter-réseau, via lesquels ils peuvent échanger des données.

**Risque** — Capacité potentielle d'une cybermenace donnée d'exploiter les vulnérabilités d'un système informatique et de lui causer des dommages.

**Routeur** — Appareil chargé d'interconnecter les réseaux logiques, en réexpédiant l'information à d'autres réseaux sur la base de leur adresse IP.

**Script kiddie** — Individu peu qualifié qui utilise des scripts ou des programmes prêts à l'emploi trouvés sur Internet afin de lancer des cyberattaques, notamment pour dégrader des sites Web.

**Sécurisé par défaut** — Ce terme évoque la désactivation des paramètres de sécurisation des technologies dites « de commodité », par lesquelles la sécurité est proposée par défaut à l'utilisateur.

**Sécurisé par conception** — Se dit d'un logiciel, de matériel informatique ou d'un système conçus dans une optique de sécurisation dès le départ.

**Système de contrôle industriel (ICS)** — Système informatique utilisé pour contrôler les procédures industrielles telles que la fabrication, la manutention des produits, la production et la distribution ou les actifs des infrastructures.

**Systèmes cyber-physiques** — systèmes intégrant des éléments électroniques et physiques ; systèmes « intelligents ».

**Système de noms de domaine (DNS)** — Système de dénomination pour les ordinateurs et services des réseaux, fondé sur une hiérarchie de domaines.

**Trusted Platform Module (TPM)** – Norme internationale de crypto-processeur sécurisé, microprocesseur dédié conçu pour sécuriser le matériel informatique en intégrant des clés cryptographiques aux périphériques.

**Utilisateur** — Personne, organisation, entité ou processus automatisé d'accès autorisé ou non à un système.

**Analyse prospective** — Examen systématique d'informations visant à identifier d'éventuels menaces, risques, problématiques et opportunités émergentes, améliorant la préparation et l'incorporation de mesures d'atténuation et d'exploitation au processus d'élaboration de politiques.

**Violation de données** — Transmission ou divulgation non autorisées d'informations sur un réseau, à l'intention d'un tiers n'étant pas supposé y accéder ou pouvoir les consulter.

**Virus** — Programme informatique malveillant pouvant contaminer d'autres fichiers.

**Vishing** – Le terme vishing ou « hameçonnage vocal » désigne l'utilisation trompeuse de technologies vocales (téléphones fixes, portables, messagerie vocale, etc.), pour extorquer aux victimes des informations financières ou personnelles sensibles, au profit d'entités non autorisées et en général, à des fins d'escroquerie.

**Vulnérabilité** — Bogues de programmes informatiques susceptibles d'être exploités par des criminels.

# ANNEXE 3 : PRINCIPAL PROGRAMME DE MISE EN ŒUVRE

## STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2016-2021

### Notre vision : le Royaume-Uni est sécurisé et résilient face aux cybermenaces, prospère et confiant dans le monde numérique

| Résultats stratégiques | Indicateurs de succès (échéance 2021) | Contribue à |
|---|---|---|
| 1. Le Royaume-Uni dispose des capacités de détecter, d'analyser et de contrer efficacement la menace émanant des cyberactivités de nos ennemis. | • Les réseaux de partage de l'information consolidés établis conjointement avec nos partenaires internationaux, ainsi que les accords multilatéraux formulés pour encourager l'adoption par les États d'un comportement légitime et responsable, contribuent de manière substantielle à notre capacité à comprendre et réagir à la menace, se traduisant par une défense plus efficace du Royaume-Uni.<br>• Nos mesures de défense et de dissuasion, ainsi que nos stratégies nationales spécifiques, font du Royaume-Uni une cible plus difficile à atteindre pour les acteurs étrangers hostiles et les cyberterroristes.<br>• Meilleure compréhension de la cybermenace émanant d'entités étrangères hostiles et de terroristes, grâce à la détection et à l'évaluation des menaces cyberterroristes contre le Royaume-Uni.<br>• Veiller à ce que les cybercapacités des terroristes restent faibles à long terme, en les surveillant de près, en perturbant leur potentiel et leurs cyberactivités à la première occasion.<br>• Le Royaume-Uni compte parmi les chefs de file mondiaux du domaine des cybercapacités offensives.<br>• Le Royaume-Uni a établi un vivier de compétences et d'expertise pour développer et déployer ses cybercapacités offensives souveraines.<br>• Nos capacités cryptographiques souveraines protègent efficacement nos secrets et nos informations sensibles des divulgations non autorisées. | DISSUADER |
| 2. L'impact de la cybercriminalité au Royaume-Uni et sur ses intérêts est considérablement réduit et les cybercriminels sont dissuadés de cibler le territoire britannique. | • Nous parvenons mieux à déstabiliser les cybercriminels qui attaquent le Royaume-Uni ; le nombre d'arrestations et de condamnations augmente au même titre que celui des réseaux criminels démantelés suite à l'intervention des forces de l'ordre.<br>• Les moyens des services répressifs se sont améliorés, cette amélioration se traduisant notamment par le renforcement des capacités et compétences des spécialistes et des agents de base et par le perfectionnement des ressources des services répressifs de nos partenaires étrangers.<br>• L'efficacité et l'ampleur des mesures d'intervention | DISSUADER |

| | | |
|---|---|---|
| | précoce (« PRÉVENIR ») prises pour dissuader et réformer les délinquants, se sont manifestement améliorées.<br>• Le nombre de cyber-infractions de faible niveau a diminué, les services des cybercriminels ayant perdu leur facilité d'accès et une grande part de leur efficacité. | |
| 3. Le Royaume-Uni dispose de capacités efficaces pour gérer les cyberincidents et réagir en conséquence, réduire les dommages subis par le pays et contrer ses ennemis cybernétiques. | • Un nombre plus important d'incidents sont signalés aux autorités, d'où une meilleure compréhension de l'étendue et de l'ampleur de la menace.<br>• Les cyberincidents sont gérés plus efficacement, de manière plus efficiente et plus complète, suite à la création du NCSC, mécanisme centralisé de signalement d'incidents et d'intervention.<br>• Nous traiterons les causes profondes des attaques à l'échelon national, réduisant l'occurrence des récidives contre une multitude de victimes et de secteurs. | DÉFENDRE |
| 4. Nos partenariats de cyberdéfense active avec l'industrie neutralisent les attaques de grande envergure par hameçonnage et maliciels. | • Le Royaume-Uni est plus difficile à hameçonner, suite à la mise en place de défenses à grande échelle contre les domaines malveillants, d'une protection anti-phishing plus active à l'échelle requise et parce qu'il est beaucoup plus difficile d'utiliser d'autres formes de communication comme le « vishing » (hameçonnage vocal) et l'usurpation d'identité par SMS, pour y lancer des attaques d'ingénierie sociale.<br>• Les moyens mis en place bloquent un volume largement plus important de communications malveillantes et d'artefacts techniques associés aux cyberattaques et à l'exploitation connexe.<br>• Le trafic Internet et les télécommunications sont largement moins vulnérables aux tentatives de redirection par des acteurs malveillants.<br>• Les capacités de réaction de GCHQ, des forces armées et de la NCA aux menaces graves émanant d'États ou criminelles, ont été significativement renforcées. | DÉFENDRE |
| 5. Le Royaume-Uni est plus sûr depuis que les produits et services technologiques sont munis, dès la conception, de mesures de cybersécurité intrinsèque, activées par défaut. | • La majorité des produits et services dits « de commodité » disponibles au Royaume-Uni en 2021 rendent le pays plus sûr, parce que leurs paramètres de sécurité sont activés par défaut ou la sécurité a été intégrée en phase de conception.<br>• Le public britannique se fie aux services de l'administration publique fournis aux échelons national, local et des administrations décentralisées, parce qu'ils ont été mis en œuvre de la façon la plus sûre possible et parce que les niveaux de fraude sont compris dans une fourchette de risque acceptable. | DÉFENDRE |
| 6. Les réseaux et services du Gouvernement seront aussi sécurisés que possible dès leur mise en œuvre. Le public pourra utiliser les services numériques de l'administration | • Le Gouvernement comprend parfaitement le niveau de risque de cybersécurité que courent l'ensemble de l'administration et le secteur public au sens large du terme.<br>• Les ministères individuels et autres organes se | DÉFENDRE |

| | | |
|---|---|---|
| publique en toute confiance, sachant que ses informations sont protégées. | protègent proportionnellement à leur niveau de risque et conformément à une norme minimale convenue avec l'administration publique.<br>• Les ministères et l'ensemble du secteur public sont résilients et savent réagir efficacement aux cyberincidents, maintenir la continuité de leurs fonctions et récupérer rapidement.<br>• Les nouvelles technologies et services numériques déployés par l'administration publique seront cybersécurisés par défaut.<br>• Nous sommes conscients des vulnérabilités des systèmes et services publics connectés et oeuvrons activement pour les atténuer.<br>• Les fournisseurs de l'administration publique respectent les normes de cybersécurité appropriées. | |
| 7. Les organisations du Royaume-Uni, petites et grandes, gèrent efficacement leur cyberrisque et bénéficient des conseils de grande qualité du NCSC, associés à un mélange équilibré de réglementation et de mesures incitatives. | • Nous comprenons le niveau de cybersécurité de notre CNI et avons mis en place des mesures pour intervenir en cas de besoin et dynamiser les améliorations dans l'intérêt national.<br>• Nos entreprises et organisations les plus importantes comprennent le niveau de menace et mettent en œuvre des pratiques de cybersécurité proportionnelles aux risques.<br>• Le niveau de cybersécurité de l'économie britannique est aussi élevé, voir plus élevé, que celui d'économies avancées comparables.<br>• Le nombre, la gravité et l'impact des cyberattaques réussies contre des entreprises au Royaume-Uni ont diminué, suite à l'amélioration des normes d'hygiène informatique.<br>• La culture de la cybersécurité s'est améliorée au Royaume-Uni, parce que les organisations et le public comprennent leurs niveaux de cyberrisque et les mesures d'hygiène informatique à prendre pour le gérer. | DÉFENDRE |
| 8. Le Royaume-Uni dispose d'un écosystème propice au développement et à la pérennisation d'un secteur de la cybersécurité capable de répondre à ses exigences en matière de sécurité nationale. | • Croissance globale plus forte que la moyenne en glissement annuel, de la taille du secteur britannique de la cybersécurité.<br>• Accroissement significatif des investissements dans les sociétés en phase de démarrage. | DÉVELOPPER |
| 9. Le Royaume-Uni possède un vivier durable de professionnels de la cybernétique britanniques, qualifiés pour répondre à la demande croissante d'une économie de plus en plus numérisée, dans les secteurs public, privé et dans celui de la défense. | • Des filières efficaces et claires d'accès aux métiers de la cybersécurité attirent des candidats très divers.<br>• À l'horizon 2021, la cybersécurité sera enseignée efficacement dans le cadre de cours pertinents, de l'école primaire au troisième cycle universitaire.<br>• La cybersécurité est largement reconnue comme étant une profession établie, associée à des parcours de carrière précis et par le Royal Chartered Status.<br>• Les connaissances appropriées en cybersécurité font partie intégrante de la formation continue des professionnels non spécialisés dans la cybersécurité, tous secteurs de l'économie confondus.<br>• Le Gouvernement et les forces armées disposent de spécialistes de la cyberdéfense, capables de préserver | DÉVELOPPER |

| | | |
|---|---|---|
| | la sécurité et la résilience du Royaume-Uni | |
| 10. Le Royaume-Uni est universellement reconnu comme comptant parmi les chefs de file mondiaux de la recherche et du développement dans la cybersécurité, soutenus par l'expertise de haut niveau de l'industrie et des milieux universitaires britanniques. | • Augmentation considérable du nombre de sociétés britanniques ayant réussi à commercialiser les fruits de la cyber-recherche universitaire, diminution du nombre de capacités lacunaires convenues et identifiées à l'échelle nationale dans le domaine de la recherche en cybersécurité et application de mesures efficaces pour y remédier.<br>• Le Royaume-Uni est considéré comme un leader mondial de la recherche et de l'innovation en cybersécurité. | DÉVELOPPER |
| 11. À l'épreuve du temps, le gouvernement britannique planifie et prépare déjà la mise en œuvre de sa politique avant l'émergence des technologies et menaces futures. | • L'analyse prospective interministérielle et l'évaluation de toutes les sources sont intégrées à l'élaboration de la politique de cybersécurité.<br>• Les effets de la cybersécurité sont pris en compte dans toutes les analyses prospectives interministérielles. | DÉVELOPPER |
| 12. L'élargissement du consensus et des capacités internationaux favorables à l'adoption par les États d'un comportement responsable dans un cyberespace libre, ouvert, paisible et sûr, réduit la menace à l'encontre du Royaume-Uni et de ses intérêts à l'étranger. | • La collaboration internationale renforcée réduit la menace cybernétique qui pèse sur le Royaume-Uni et sur ses intérêts à l'étranger.<br>• Le comportement responsable des États dans le cyberespace fait l'objet d'une compréhension commune.<br>• Les partenaires internationaux ont augmenté leurs moyens de cybersécurité.<br>• Le consensus international relatif aux avantages d'un cyberespace libre, ouvert, paisible et sûr, a été renforcé. | ACTION ET INFLUENCE INTERNATIONALES |
| 13. Les politiques, organisations et structures du Gouvernement britannique sont simplifiées, pour maximiser la cohérence et l'efficacité de la réaction du Royaume-Uni face aux cybermenaces. | • Les responsabilités du Gouvernement en matière de cybersécurité sont comprises et ses services sont accessibles.<br>• Nos partenaires savent comment optimiser l'interaction avec le Gouvernement sur les questions de cybersécurité. | QUESTION TRANSVERSALE |