HM Government

Cyberstratégie nationale 2022

Vision novatrice d'un cyberavenir à l'échelle du Royaume-Uni

Cyberstratégie nationale 2022

Vision novatrice d'un cyberavenir à l'échelle du Royaume-Uni

Sommaire

Avant-propos 8

Introduction 10

Opportunités et défis de l'ère numérique 10
Notre vision : le cyberpouvoir à l'appui des objectifs nationaux 11
Les cinq axes de notre stratégie 13

1re partie : Stratégie 16

Contexte stratégique 17

Global Britain in a Competitive Age (Une Grande-Bretagne globale à l'ère de la concurrence) 17
Le cyberpaysage 17
Cyberpouvoir 20
Le Royaume-Uni parmi les cyberpuissances modernes 20
Cybercriminels utilisant les rançongiciels pour attaquer les services publics 26
Exploitation par les États des vulnérabilités stratégiques et des chaînes d'approvisionnement 27
Moteurs du changement 29

Notre réponse nationale 32

Notre vision, nos objectifs, nos principes 32
Principaux changements dans notre approche 34
Rôles et responsabilités à l'échelle du Royaume-Uni 36

2e partie : Mise en œuvre 46

Axe 1 : l'écosystème cyber du Royaume-Uni 48

Renforcer l'écosystème cyber du Royaume-Uni 49

Objectif 1 : soutenir une approche basée sur la dimension pansociétale 50
Objectif 2 : améliorer les compétences et la diversité 54
Objectif 3 : favoriser la croissance et l'innovation 58

Axe 2 : Cyberrésilience 64

Construire un Royaume-Uni numérique résilient et prospère 65

Objectif 1 : comprendre le cyberrisque 68
Objectif 2 : prévenir et résister aux cyberattaques 70
Objectif 3 : préparer, répondre et s'en remettre 74

Axe 3 : Avantage technologique 78

Prendre l'initiative par rapport aux technologies essentielles au cyberpouvoir 79

Objectif 1 : anticiper, évaluer et agir par rapport aux progrès technologiques 81
Objectif 2 : favoriser et maintenir l'avantage technologique 82
Objectif 2a : préserver les capacités Crypt-Key nationales 85
Objectif 3 : sécuriser les technologies connectées 86
Objectif 4 : façonner les normes technologiques mondiales 88

Axe 4 : leadership mondial 90

Promouvoir le leadership et l'influence du Royaume-Uni sur la scène internationale pour un ordre international sûr et prospère. 91

Objectif 1 : renforcer l'action collective et la cyberrésilience mutuelle 92
Objectif 2 : façonner la gouvernance mondiale du cyberespace 94
Objectif 3 : tirer parti et exporter les cybercapacités du Royaume-Uni 95

Axe 5 : lutter contre les menaces 98

Détecter, perturber et dissuader nos adversaires afin d'améliorer la sécurité du Royaume-Uni dans et à travers le cyberespace. 99

Objectif 1 : détecter, enquêter et partager des informations sur les menaces 101
Objectif 2 : dissuader et perturber les menaces 104
Objectif 3 : agir dans et à travers le cyberespace pour lutter contre la menace 106

Concrétiser notre ambition 112

Rôles et responsabilités de l'ensemble du gouvernement 112
Investir dans notre cyberpouvoir 115
Mesurer le succès 115
Prochaines étapes 116

Annexe A : La cybernétique intégrée au programme plus général du gouvernement 118

Annexe B : NIS Regulations (Règlementation relative aux réseaux et systèmes d'information) – stratégie nationale 121

Principaux rôles et responsabilités 122

Liste des principales autorités de mise en œuvre de la règlementation NIS 124

Annexe C : Glossaire 125

Contenu supplémentaire

Récentes études de cas de cyberattaques 26

National Cyber Security Centre 40

National Cyber Force 42

Réseau national de lutte contre la cybercriminalité des services répressifs 44

UK Cyber Security Council (Conseil de cybersécurité du Royaume-Uni) 56

Vous avez envie de rejoindre les cybereffectifs ou de créer votre propre entreprise ? 60

Technologies essentielles au cyberpouvoir 80

Digital Security by Design (Sécurité numérique native) 84

Mettre fin aux cybercrimes signifie également s'attaquer à d'autres types d'activités criminelles. 103

Grandes enquêtes des services répressifs sur les cybercrimes 108

Agir dans le cyberespace pour lutter contre le terrorisme 110

Avant-propos

Le Royaume-Uni est une société ouverte et démocratique. Son passé de collaboration et d'innovation sous-tend le succès de cette nation mondiale tournée vers l'extérieur. Sa réponse aux urgences sanitaires internationales et ses actions pour promouvoir la concrétisation des objectifs zéro émission nette en sont l'illustration éloquente. Quoi qu'il en soit, les avantages de cette approche sont surtout particulièrement évidents dans la cybernétique.

Qu'il s'agisse d'en exploiter positivement les vastes avantages pour nos citoyens et notre économie afin de réduire les inégalités et d'unifier le pays, de collaborer avec nos partenaires pour créer un cyberespace à l'image de nos valeurs nationales ou de mobiliser l'intégralité de nos cybercapacités pour influencer les événements planétaires, le Royaume-Uni considère la cybernétique comme un moyen de protéger et de promouvoir ses intérêts dans un paysage largement remodelé par la technologie.

D'où l'élaboration de notre nouvelle National Cyber Strategy, cyberstratégie nationale par laquelle nous projetons de veiller à ce que le Royaume-Uni reste confiant, capable et résilient dans ce monde numérique évolutif, à ce qu'il continue de s'adapter, d'innover et d'investir afin de protéger et de promouvoir ses intérêts dans le cyberespace.

Prenant le relais de la première Stratégie nationale de cybersécurité publiée en 2016, ce nouveau volet nous mène vers un avenir où le Royaume-Uni sera encore plus résilient aux cyberattaques. En ma capacité de ministre responsable, j'en cerne clairement deux principaux objectifs : nous devrions premièrement consolider notre maîtrise des technologies essentielles à la cybernétique et deuxièmement, limiter notre dépendance à l'égard de fournisseurs ou de technologies individuelles, élaborées sous le contrôle de régimes qui ne partagent pas nos valeurs.

La science et la technologie du Royaume-Uni seront les moteurs de ce changement. Elles veilleront à ce que la cybernétique soit préservée au rang des actifs économiques et stratégiques nationaux, à ce que notre technologie soit plus digne de confiance et mieux équipée pour repousser toutes sortes de cyberadversaires dont les capacités étaient, jusqu'à récemment, l'apanage exclusif des États-nations.

Le gouvernement s'est engagé à consacrer 22 milliards GBP à la recherche et au développement, à placer la technologie au cœur de nos stratégies de sécurité nationale. Nous avons tous pu constater le potentiel transformateur des technologies numériques, mais aussi, comme dans le cas de la 5G, leur pouvoir perturbateur. Nos projets en matière d'intelligence artificielle et de politique des données nous aideront à rester à l'avant-garde de ces technologies. Les mesures prises dans le cadre de la cyberstratégie nous rassurerons sur la sécurité et la résilience de nos fournisseurs et partenaires.

La création de la cyberforce nationale National Cyber Force en 2021 témoigne de l'intensification significative de nos capacités de cyberoffensive. Cela étant, la cybersécurité de base reste essentielle à nos efforts pour fortifier notre réponse face à ceux qui attaquent le Royaume-Uni et ses citoyens. Nos efforts viseront également à améliorer la résilience du secteur public, en aidant les municipalités à protéger leurs systèmes et les données personnelles des citoyens contre les rançongiciels et autres cyberattaques.

Dans une société, tout le monde est concerné par la cybernétique. En adoptant cette stratégie, le gouvernement intensifie ses efforts de protection des citoyens, des entreprises du Royaume-Uni et de ses partenaires internationaux et se rapproche de la concrétisation de sa vision d'un cyberespace fiable, résilient, favorable à la prospérité de ses citoyens et de ses entreprises.

Le très honorable Steve Barclay MP,
Chancelier du duché de Lancastre,
ministre chargé du « Cabinet Office »

Introduction

Opportunités et défis de l'ère numérique

1. Associés à la diminution des coûts, les progrès exponentiels de la technologie ont fait du monde un univers plus connecté que jamais et stimulent la création d'opportunités extraordinaires, l'innovation et le progrès. Et même si la pandémie de coronavirus (COVID-19) a indéniablement accéléré cette tendance, nous n'en sommes probablement encore qu'aux premières étapes d'un bouleversement structurel à long terme. L'expansion mondiale du cyberespace change la manière dont nous vivons, travaillons et communiquons. Elle transforme les systèmes critiques sur lesquels nous comptons dans des domaines tels que la finance, l'énergie, la distribution alimentaire, les soins de santé et les transports. Bref, le cyberespace fait désormais partie intégrante de notre sécurité et de notre prospérité futures. Cet état de chose met des pays aussi avancés sur le plan technologique que le Royaume-Uni dans une position extraordinaire pour exploiter de nouveaux moyens de poursuivre leurs objectifs nationaux.

2. L'ampleur et la rapidité de ce changement, qui souvent dépasse nos normes sociales, nos lois et institutions démocratiques, nous met également face à des niveaux de complexité, d'instabilité et de risque sans précédent. L'année dernière a été ponctuée de cyberattaques contre des hôpitaux et des oléoducs, des écoles et des entreprises, dont certaines ont même été paralysées par des rançongiciels et espiogiciels commerciaux ciblant militants, journalistes et politiciens. Compte tenu de la transnationalisation du cyberespace, relever ces défis demande une collaboration internationale dans une arène de concurrence systémique dont l'importance augmente de plus en plus et où s'opposent les intérêts, valeurs et visions de l'avenir antagonistes de notre monde.

Notre vision : le cyberpouvoir à l'appui des objectifs nationaux

3. Dans ce contexte, le cyberpouvoir s'impose progressivement parmi les leviers de plus en plus vitaux du pouvoir national, comme une source d'avantages stratégiques. **Le cyberpouvoir, c'est la capacité de protéger et de promouvoir les intérêts nationaux dans et à travers le cyberespace.** Demain, les pays les mieux placés pour négocier les opportunités et relever les défis de l'ère numérique seront plus sûrs, plus résilients et plus prospères. Le Royaume-Uni est l'un des pays du monde les plus avancés sur le plan numérique et ce gouvernement a élaboré un programme technologique national et international ambitieux. Nous sommes donc d'une part particulièrement exposés aux défis du cyberespace et de l'autre, exceptionnellement bien placés pour prendre l'initiative en saisissant ses opportunités pour nos citoyens et le bien commun de l'humanité.

4. Au cours de la prochaine décennie, nos intérêts et ceux de nos alliés et adversaires dépendront de plus en plus de l'Internet, de la technologie numérique et de l'infrastructure sur laquelle elle repose. Parallèlement à nos efforts pour construire le nouveau rôle du Royaume-Uni au sein d'une ère plus concurrentielle, la consolidation de notre cyberpouvoir nous permettra de montrer la voie à l'industrie et à d'autres pays, d'anticiper l'évolution des technologies, d'atténuer les menaces et d'acquérir un avantage stratégique par rapport à nos adversaires et à nos concurrents. Elle placera le Royaume-Uni parmi les économies numériques les plus sûres et les plus attrayantes pour vivre, faire des affaires et investir.

5. Notre vision du **Royaume-Uni en 2030 est celle d'un pays qui continue à faire partie des cyberpuissances mondiales de premier plan, responsable, démocratique, capable de protéger et de promouvoir ses intérêts dans et à travers le cyberespace, en adéquation avec ses objectifs nationaux** :

- une nation à la fois plus sûre et plus résiliente, mieux équipée pour faire face aux menaces et aux risques évolutifs, utiliser ses cybercapacités pour protéger ses citoyens contre la criminalité, la fraude et les menaces étatiques ;
- une économie numérique novatrice, prospère où les opportunités sont mieux réparties sur l'ensemble du pays et de notre population diversifiée ;
- une superpuissance scientifique et technologique, maîtrisant en toute sécurité les technologies transformatrices au profit d'une société plus verte et plus saine ;
- un partenaire plus influent, plus estimé sur la scène mondiale, façonnant les futures frontières d'un ordre international ouvert, stable tout en préservant sa liberté d'action dans le cyberespace.

6. Au cours de la dernière décennie, nous avons établi le Royaume-Uni parmi les cyberpuissances mondiales en développant des capacités de cybersécurité et de cyberopération de pointe ainsi qu'un secteur de la cybersécurité de premier plan. Cette stratégie s'appuie sur les importants progrès réalisés dans le cadre de la Stratégie nationale de cybersécurité 2016-2021 et les trois conclusions importantes énoncées dans le document du gouvernement intitulé Integrated Review of Security, Defence, Development and Foreign Policy (Revue intégrée de la sécurité, de la défense, du développement et de la politique étrangère). À savoir en premier lieu qu'à l'ère numérique, le cyberpouvoir du Royaume-Uni jouera un rôle de levier de plus en plus important pour concrétiser nos objectifs nationaux. Deuxièmement, que l'entretien de notre cyberpouvoir exige une stratégie plus complète, intégrée tenant compte de tous nos cyberobjectifs et cybercapacités. Troisièmement, que la société doit adopter uniformément cette approche. Autrement dit d'une part, que l'activité des entreprises et des établissements d'enseignement doit autant compter pour le cyberpouvoir national que les démarches des experts techniques et fonctionnaires d'État et de l'autre, que nos partenariats seront essentiels à notre succès.


CHELTENHAM
Science
Festival
18.2 Cyber Skills a
@CyNam

Les cinq axes de notre stratégie

7. La Revue intégrée définit cinq « actions prioritaires ». Adoptées comme axes du cadre de notre stratégie, **elles nous guideront et étayeront l'organisation des actions spécifiques que nous mettrons en œuvre, ainsi que les résultats visés à l'horizon 2025**:

- **Axe 1 : renforcer l'écosystème cyber du Royaume-Uni**, en investissant dans notre capital humain, dans les compétences et en approfondissant le partenariat entre le gouvernement, le monde universitaire et l'industrie.
- **Axe 2 : construire un Royaume-Uni numérique résilient et prospère**, en réduisant les cyberrisques pour permettre aux entreprises de maximiser les avantages économiques de la technologie numérique, que les citoyens se sentent moins menacés en ligne et qu'ils ne doutent plus que leurs données sont protégées.
- **Axe 3 : prendre l'initiative par rapport aux technologies essentielles au cyberpouvoir,** en renforçant notre capacité industrielle et en développant les structures nécessaires pour sécuriser les technologies futures.
- **Axe 4 : promouvoir le leadership et l'influence du Royaume-Uni sur la scène internationale, pour un ordre international plus sûr, prospère et ouvert**, en collaborant avec les partenaires du gouvernement et de l'industrie et en partageant l'expertise étayant le cyberpouvoir du Royaume-Uni.
- **Axe 5 : détecter, perturber et dissuader nos adversaires afin d'améliorer la sécurité du Royaume-Uni dans et à travers le cyberespace**, en recourant de manière plus intégrée, plus créative et plus régulière à l'ensemble des leviers du Royaume-Uni.

8. La première partie du présent document décrit le contexte stratégique dans lequel nous évoluons, les objectifs de notre stratégie et l'approche stratégique que nous adopterons au cours de la prochaine décennie. La seconde présente les actions précises que nous mettrons en œuvre pour atteindre nos objectifs à l'horizon 2025, sur la base de nos cinq axes directeurs.

Vision

En 2030, le Royaume-Uni sera toujours une cyberpuissance responsable et démocratique de premier plan, capable de protéger et de promouvoir ses intérêts dans et à travers le cyberespace pour concrétiser ses objectifs nationaux.

Axes et objectifs

Axe 1

Renforcer l'écosystème cyber du Royaume-Uni

1. Renforcer les structures, partenariats et réseaux nécessaires pour soutenir une approche basée sur la dimension pansociétale de la cybernétique.
2. Améliorer et élargir les cybercompétences nationales à tous les niveaux, notamment par le biais d'une cyberprofession de calibre mondial et diversifiée, capable d'inspirer et d'équiper les futurs talents.
3. Favoriser la croissance d'un secteur de la cybersécurité et de la sécurité de l'information durable, novateur et concurrentiel à l'échelle internationale, source de produits et de services de qualité répondant aux besoins du gouvernement et de l'ensemble de l'économie.

Axe 2

Construire un Royaume-Uni numérique résilient et prospère

1. Améliorer la compréhension des cyberrisques pour favoriser une action plus efficace en matière de cybersécurité et sur le plan de la résilience.
2. Prévenir et résister plus efficacement aux cyberattaques en améliorant la gestion des cyberrisques au sein des organisations britanniques et en protégeant mieux les citoyens.
3. Renforcer la résilience aux niveaux national et organisationnel afin de se préparer aux cyberattaques, d'y répondre et de s'en remettre.

Axe 3

Prendre l'initiative par rapport aux technologies essentielles au cyberpouvoir

1. Améliorer notre capacité d'anticiper, d'évaluer et d'agir par rapport aux progrès scientifiques et technologiques les plus essentiels à notre cyberpouvoir.
2. Favoriser et maintenir l'avantage souverain et allié dans le domaine de la sécurité des technologies essentielles au cyberespace.
2a. Préserver des capacités cryptographiques « Crypt-Key » nationales robustes et résilientes répondant aux besoins des clients du gouvernement britannique, de ses partenaires et de ses alliés et ayant adéquatement atténué nos risques les plus importants, dont la menace de nos adversaires les plus compétents.
3. Sécuriser la prochaine génération de technologies et d'infrastructures connectées, en atténuant les risques de cybersécurité liés à la dépendance à l'égard des marchés mondiaux et en veillant à ce que les utilisateurs britanniques aient accès à un approvisionnement fiable et diversifié.
4. Œuvrer avec la communauté multi-parties prenantes, pour façonner l'élaboration de normes techniques numériques mondiales dans les domaines prioritaires qui comptent le plus pour préserver nos valeurs démocratiques, garantir notre cybersécurité et favoriser la progression de l'avantage stratégique du Royaume-Uni à travers la science et la technologie.

Axe 4

Promouvoir le leadership et l'influence du Royaume-Uni sur la scène internationale

1. Renforcer la cybersécurité et la cyberrésilience des partenaires internationaux et accroître l'action collective pour perturber et dissuader nos adversaires.
2. Façonner la gouvernance mondiale pour promouvoir un cyberespace libre, ouvert, pacifique et sécurisé.
3. Tirer parti des cybercapacités et de l'expertise du Royaume-Uni et les exporter pour accroître notre avantage stratégique, promouvoir notre politique étrangère plus générale et les intérêts propices à notre prospérité.

Axe 5

Détecter, perturber et dissuader nos adversaires

1. Détecter, enquêter et partager des informations sur les cyberacteurs et cyberactivités malveillants étatiques, criminels et autres afin de protéger le Royaume-Uni, ses intérêts et ses citoyens.
2. Dissuader et perturber les cyberacteurs et cyberactivités malveillants étatiques, criminels et autres menaçant le Royaume-Uni, ses intérêts et ses citoyens.
3. Prendre des mesures dans et à travers le cyberespace pour étayer notre sécurité nationale, la prévention et la détection des crimes graves.

Soutien aux objectifs nationaux

- Sécurité et résilience
- Superpuissance scientifique et technologique
- Prospérité économique
- Façonner l'ordre international

1re partie :
Stratégie

Contexte stratégique

Global Britain in a Competitive Age (Une Grande-Bretagne globale à l'ère de la concurrence)

9. Publié en mars 2021, le document Integrated Review of Security, Defence, Development and Foreign Policy décrit la vision du gouvernement quant au rôle du Royaume-Uni sur la scène mondiale au cours des dix prochaines années, ainsi que l'action par laquelle il entend la concrétiser à l'horizon 2025. Il reconnaît que pour être mieux équipé pour évoluer dans un monde concurrentiel, le Royaume-Uni doit favoriser l'innovation scientifique et technologique afin de stimuler notre prospérité nationale et notre avantage stratégique. La cyberstratégie nationale s'appuie sur cette approche. Sa publication est l'un des engagements pris dans le cadre de l'objectif stratégique de la Revue intégrée visant à « maintenir l'avantage stratégique par la science et la technologie ».

Le cyberpaysage

10. Les défis politiques associés au cyberespace n'ont pas seulement une dimension technologique. Le cyberdomaine est un environnement d'origine humaine, fondamentalement façonné par les comportements humains. Les répercussions de ces comportements amplifiés, pour le meilleur ou pour le pire, sont habituellement également ressenties dans le monde physique. Le cyberespace est détenu et exploité par des entreprises privées, des gouvernements, des organisations à but non lucratif, des particuliers, mais aussi par des individus et organisations aux intentions criminelles. Toute réponse stratégique à un tel contexte doit par conséquent établir un lien entre la géostratégie et la sécurité nationale, la justice pénale et la réglementation civile, les politiques économique et industrielle. Elle exige une compréhension approfondie des différents contextes culturels ou sociaux, ainsi que des systèmes de valeurs interagissant en ligne.

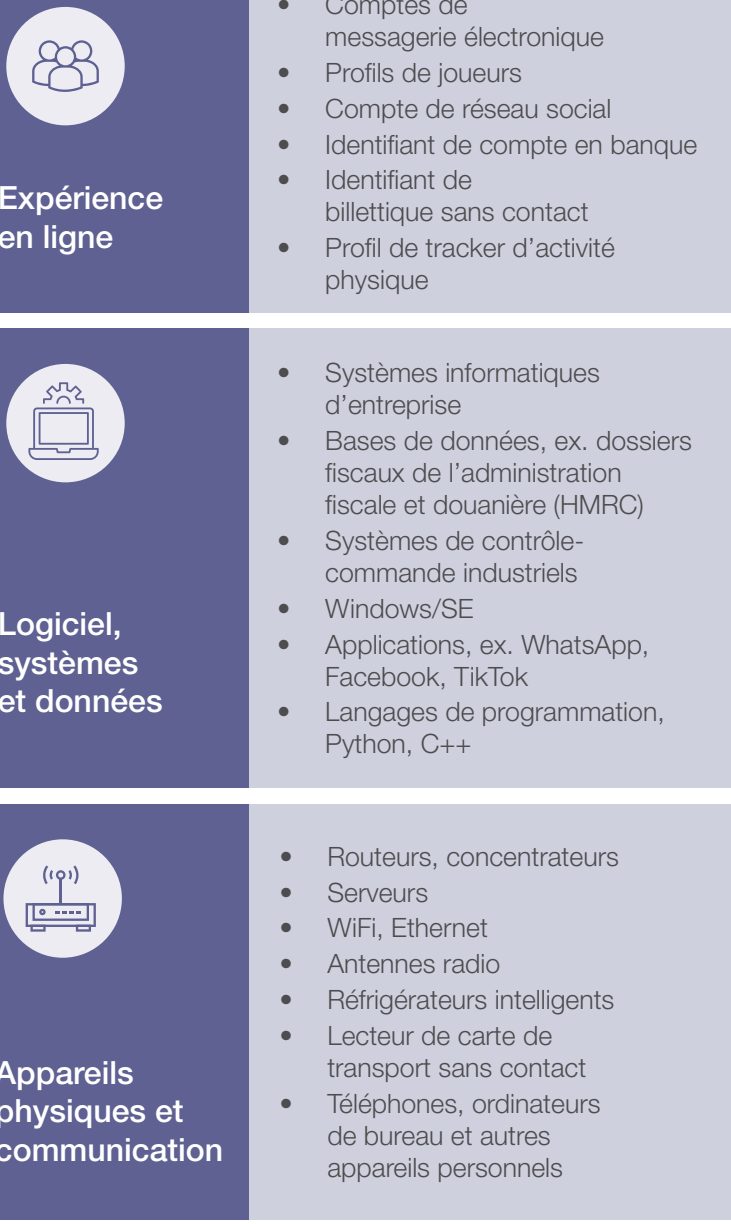
11. Par ailleurs, le cyberespace transcende les frontières nationales. Les chaînes d'approvisionnement technologiques et dépendances critiques sont de plus en plus mondiales. Les cybercriminels et acteurs étatiques proviennent des quatre coins de la planète. Les puissantes entreprises technologiques exportent des produits et établissent leurs normes. Les règles et les normes régissant le cyberespace et l'Internet sont décidées dans les forums internationaux. L'évolution continue du cyberespace au rythme de celle de la technologie et de l'usage qu'en font les utilisateurs, nous oblige à faire preuve d'agilité et de réactivité.

Les couches du cyberespace

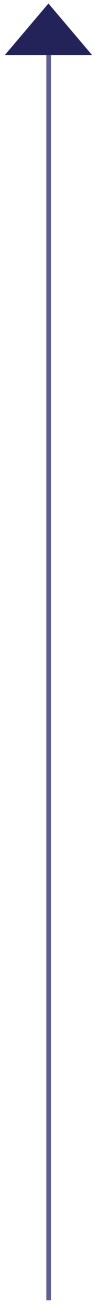
Qu'est-ce que le cyberespace ?

Pour beaucoup d'entre nous, le cyberespace est le monde virtuel dans lequel nous nous déplaçons en ligne, pour communiquer, travailler et accomplir nos tâches quotidiennes. En termes techniques, le cyberespace est le réseau interdépendant de technologies de l'information composé de l'Internet, des réseaux de télécommunications, des systèmes informatiques et des appareils connectés à l'Internet. Pour les militaires et en ce qui concerne nos efforts pour contrer les menaces dans le cyberespace, il s'agit d'un domaine opérationnel au même titre que la terre, la mer, l'air et l'espace.

Comment vit-on le cyberespace ?
Par définition, le cyberespace est un espace « partagé » dont l'ampleur et la complexité sont telles que chaque utilisateur le vit différemment et à sa façon. Les citoyens accèdent au cyberespace quand ils vérifient leur compte bancaire en ligne ou regardent un film en streaming chez eux. Les entreprises l'utilisent pour mettre leurs employés en contact avec les ressources dont ils ont besoin, qu'il s'agisse d'accéder à des informations ou de contrôler un processus de fabrication. Les gouvernements fournissent des services publics à leurs citoyens par le biais de portails en ligne. Les professionnels de la cybernétique traitent la technologie en regardant « sous le capot ». Ils examinent les normes et protocoles qui garantissent la parfaite fluidité des systèmes au profit des utilisateurs. Chacun de ces groupes utilise le cyberespace de différentes façons et à des fins différentes, mais tous l'utilisent de plus en plus.



Le cyberespace peut être défini par rapport à ses trois couches :



L'EXPÉRIENCE DU CYBERESPACE

Virtuelle

Partie du cyberespace qu'utilise la plupart des internautes. Elle se compose de représentations de personnes et d'organisations à travers une identité virtuelle, dans un espace partagé virtuel également. Ces représentations virtuelles peuvent prendre la forme d'adresses électroniques, d'identifications utilisateur, de comptes de réseaux sociaux ou d'alias. Une personne ou une organisation peuvent avoir plusieurs identités en ligne. Inversement, plusieurs personnes ou organisations peuvent créer une seule identité partagée.

Logique

Partie du cyberespace constituée de code ou de données, comme les systèmes d'exploitation, protocoles, applications et autres logiciels. La couche logique ne peut pas fonctionner sans la couche physique. L'information circule à travers des réseaux câblés ou le spectre électromagnétique. La couche logique, en association avec la couche physique, permet aux identités virtuelles de communiquer et d'agir.

Physique

La couche physique du cyberespace inclut le matériel servant à la transmission des données, des routeurs, fils et concentrateurs dont vous disposez chez vous aux systèmes de télécommunication vastes et complexes exploités par les grandes sociétés de technologie. En plus de l'infrastructure physique, elle inclut le spectre électromagnétique sur lequel les données sont transmises et dont dépendent le WiFi et la radio.

Cyberpouvoir

12. Le concept du cyberpouvoir, que nous définissons comme étant la capacité d'un état de protéger et de promouvoir ses intérêts dans et à travers le cyberespace, est une des notions essentielles de notre stratégie. Nous identifions cinq dimensions générales du cyberpouvoir, qui s'alignent sur les axes de cette stratégie :

- les personnes, connaissances, compétences, structures et partenariats servant de base à notre cyberpouvoir, qui sous-tendent les autres composantes et les intègrent à une approche nationale ;
- la capacité de protéger nos actifs grâce à la cybersécurité et à la résilience, afin de réaliser l'intégralité des avantages qu'offre le cyberespace à nos citoyens et à notre économie ;
- les capacités techniques et industrielles pour continuer à participer à l'évolution des principales technologies cybernétiques et déployer les extrants de nouveaux progrès, dans l'intérêt de la société ;
- l'influence mondiale, les relations et les normes éthiques pour façonner les règles et les normes dans le cyberespace conformément à nos valeurs et à nos intérêts et pour promouvoir la sécurité et la stabilité internationales ;
- la capacité d'agir dans et à travers le cyberespace pour étayer la sécurité nationale, le bien-être économique et la prévention de la criminalité. Cette dimension comprend les cyberopérations visant à produire des effets concrets et pour contribuer à l'acquisition d'un avantage stratégique, ainsi que les opérations de répression et l'application de cybersanctions visant à traduire en justice les cybercriminels malveillants et à perturber leurs activités.

13. Le cyberpouvoir se distingue d'autres formes de pouvoir plus traditionnelles. Il découle d'un mélange homogène de capacités dures et de leviers d'influence plus souples. Il est plus réparti et les gouvernements doivent travailler avec des partenaires pour l'acquérir et l'exercer. Étant donné le rythme de l'évolution technologique par lequel les nouveaux progrès rendent obsolètes et remplacent les capacités précédemment dites « de pointe », il se gagne et se perd plus rapidement.

14. Notre stratégie en tient compte et décrit la façon dont nous nous efforcerons de ne manquer aucune occasion de travailler avec des partenaires dans le cadre d'un effort concerté et pansociétal. Nous nous mobiliserons davantage pour régler les problèmes en amont et corriger les causes profondes, anticiper les tendances futures, mettre en place des réponses à long terme et favoriser une action visant à façonner l'environnement géopolitique contesté au lieu d'y répondre.

Le Royaume-Uni parmi les cyberpuissances modernes

15. Le Royaume-Uni compte déjà parmi les cyberpuissances mondiales de référence.[1] Depuis dix ans, le gouvernement mène un effort national soutenu pour renforcer la cybersécurité du Royaume-Uni, sensibiliser le public aux cyberrisques, développer le secteur de la cybersécurité et un large éventail de capacités à travers le cyberespace afin de répondre aux menaces d'acteurs hostiles. Malgré nos progrès très encourageants et la position solide dans laquelle nous nous trouvons, nous continuons de faire face à des défis importants sur l'ensemble des cinq axes de cette stratégie.

[1] Classé au deuxième rang de l'Indice mondial de cybersécurité (GCI) de l'Union internationale des télécommunications, au troisième rang du Cyber Power Index (Indice des cyberpuissances) du Harvard Belfer Center et au deuxième niveau de l'évaluation des capacités des cyberpuissances de l'International Institute of Strategic Studies (IISS).

Écosystème cyber et leadership technologique du Royaume-Uni

16. L'approche adoptée par le Royaume-Uni pour construire son cyberpouvoir intègre des efforts concertés pour développer la base de cybercompétences et les capacités commerciales du pays, dans le cadre d'un partenariat et du partage de connaissances entre le gouvernement britannique et les gouvernements décentralisés d'Irlande du Nord, d'Écosse et du Pays de Galles. Comptant plus de 1 400 entreprises génératrices d'un chiffre d'affaires global de 8,9 milliards GBP l'an dernier, soutenant 46 700 emplois qualifiés et attirant d'importants investissements exogènes, le secteur de la cybersécurité du Royaume-Uni est en pleine croissance. Ce secteur qui contribue largement à notre sécurité, à notre influence internationale et à notre croissance économique est essentiel à notre cyberpouvoir. Nous avons consolidé la réputation du Royaume-Uni parmi les leaders mondiaux de la recherche en cybersécurité, position qu'illustrent 19 centres d'excellence universitaires et quatre instituts de recherche dont les travaux traitent nos défis les plus urgents en matière de cybersécurité.

17. La main-d'œuvre du secteur de la cybersécurité a augmenté d'environ 50 % au cours des quatre dernières années, dans un contexte où la demande de compétences dépasse souvent l'offre. Nous avons considérablement échangé avec l'industrie, les organisations professionnelles, les étudiants, les employeurs, les professionnels actuels de la cybersécurité et le monde universitaire pour mieux comprendre la nature du défi des compétences en cybersécurité. Nous avons mis à la disposition des jeunes une vaste gamme d'initiatives parascolaires pour les inciter à faire carrière dans le domaine de la cybersécurité. De 2019 à 2020, nous avons fait participer près de 57 000 jeunes à nos programmes d'apprentissage CyberFirst et Cyber Discovery. Nous avons élargi nos formations pour atteindre les élèves plus jeunes. Le concours CyberFirst Girls en ligne a attiré 11 900 jeunes filles, les meilleures équipes concourant simultanément à 18 endroits du Royaume-Uni. Notre programme de bourses CyberFirst a attiré des étudiants de premier cycle très motivés et pleins de talent. L'an dernier, 750 étudiants ont participé au programme et parmi eux, 56 diplômés occupaient des postes à temps plein dans le domaine de la cybersécurité.

18. En dépit de ces interventions, le pipeline de compétences plus général continue de poser un défi considérable. Sur les 1,32 million d'entreprises de l'ensemble de l'économie, environ 50 % font encore état d'un déficit de cybercompétences techniques de base.[2] Et malgré la croissance rapide du secteur de la cybersécurité du Royaume-Uni, la plupart des entreprises sont des start-up et le développement de grands fournisseurs nationaux reste difficile face à la consolidation internationale. Comme l'a illustré l'expérience de la 5G, le Royaume-Uni et nos alliés ne figurent pas parmi les leaders dans certains domaines clés de l'industrie technologique plus générale. Les pays qui parviennent à établir un rôle de premier plan dans les technologies essentielles au cyberpouvoir seront mieux placés pour influencer la façon dont elles sont conçues et déployées, plus en mesure de protéger leur sécurité et leur avantage économique et d'exploiter plus rapidement les possibilités de percées dans les cybercapacités.

Cyberrésilience du Royaume-Uni

19. Au cours de la dernière décennie, nous avons mis en œuvre un large éventail d'interventions visant à renforcer la cyberrésilience du Royaume-Uni. Nous le devons à l'investissement important et soutenu dans certaines de nos capacités cybernétiques de base et notamment dans le National Cyber Security Centre (NCSC - Centre national de la cybersécurité), la répression, nos professionnels de la sécurité et des politiques à l'échelle du gouvernement, mais aussi à l'expansion de nos partenariats nationaux et internationaux.

[2] DCMS, Cyber security skills in the UK labour market 2021 (2021) (État des compétences de cybersécurité du marché du travail du Royaume-Uni en 2021)

20. Nos efforts les plus novateurs et révolutionnaires se sont manifestés sous forme d'actions à l'échelle nécessaire, dont le développement et le déploiement plus systématique du programme de cyberdéfense active Active Cyber Defence (ACD). L'an dernier, il a permis d'éliminer 2,3 millions de campagnes malveillantes dont 442 campagnes d'hameçonnage déguisées sous la marque NHS et 80 applications NHS illégitimes hébergées et disponibles en téléchargement en dehors des boutiques d'applications officielles.[3] Nous avons également pris l'initiative à l'échelle mondiale en faisant pression pour que les produits de consommation connectables soient « secure by design » (sécurisé de façon native), élaborant au Royaume-Uni en 2018 un code de pratique qui depuis, a été émulé et a servi de base à l'élaboration de la première norme de l'industrie relative aux appareils grand public connectés à l'Internet applicable à l'échelle mondiale.[4] [5]

21. La nouvelle réglementation a eu un impact positif sur la cybersécurité, 82 % des organisations déclarant que leurs améliorations ont été influencées par l'introduction en 2018 du Règlement général sur la protection des données au Royaume-Uni.[6] Et 77 % des entreprises, soit 12 % de plus qu'en 2016, considèrent désormais la cybersécurité comme une haute priorité.[7] D'autre part l'introduction des NIS Regulations (Règlementation relative aux réseaux et systèmes d'information) en 2018 a forcé les organisations désignées à prendre des mesures pour renforcer la sécurité de leurs réseaux et systèmes d'information, aboutissant à une réduction des cyberrisques posés par les services essentiels et services numériques importants.[8] Notons parmi les bons exemples de collaboration entre les quatre nations du Royaume-Uni, les améliorations apportées à l'ensemble du secteur de la santé et notamment, la mise en œuvre de la réglementation NIS.

22. Nous avons fourni des conseils et des directives très complètes en matière de cybersécurité aux organisations de l'ensemble de l'économie, tout en adaptant notre soutien aux secteurs essentiels pendant la pandémie de coronavirus (COVID-19). Quant aux particuliers, notre campagne Cyber Aware a fourni des conseils sur les mesures pouvant être prises pour se protéger en ligne. Dans les cas où les cyberattaqueurs sont parvenus à s'infiltrer, nous avons mobilisé nos capacités de référence mondiale de réponse aux incidents, pour assurer un soutien direct dans les cas les plus graves. Notre investissement dans les spécialistes locaux de la répression nous permet désormais de répondre au moindre signalement d'incident.

23. Nous avons mis sur pied des cellules cybernétiques spécialisées dans la répression sur l'ensemble du Royaume-Uni, parallèlement au réseau Cyber PROTECT, à la cellule de soutien aux victimes de la criminalité économique Economic Crime Victims Care Unit et aux centres régionaux de cyberrésilience Cyber Resilience Centres. Grâce à ces initiatives, les citoyens comme les petites et moyennes entreprises savent qu'ils peuvent compter sur un contact à proximité ou facilement joignable, disposant des compétences et des connaissances locales nécessaires pour les soutenir, les conseiller et leur donner les moyens d'améliorer leur cyberrésilience.

24. L'existence de lacunes dans notre résilience nationale est néanmoins de plus en plus évidente. Les niveaux de cybercriminalité et de violation touchant le gouvernement, les entreprises et les particuliers continuent d'augmenter, au même titre que la criminalité

[3] NCSC, NCSC Annual Review 2021 (2021) (Bilan annuel)
[4] DCMS, Code of Practice for Consumer IoT Security (2018) (Code de pratique de sécurité IdO grand public)
[5] DCMS, ETSI industry standard based on the Code of Practice (2019) (Norme industrielle ETSI basée sur le Code de conduite)
[6] DCMS/RSM, The impact of GDPR on cyber security outcomes (2020) (Impact du RGPD sur les extrants de la cybersécurité). Le Règlement général sur la protection des données (RGPD) incorporé à la loi du Royaume-Uni en 2018 a désormais été remplacé par le UK GDPR)
[7] DCMS, Cyber Security Breaches Survey 2021 (2021) (Enquête sur les atteintes à la cybersécurité)
[8] DCMS, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020) (Bilan post-mise en œuvre de la règlementation relative aux réseaux et systèmes d'information).

facilitée par la cybernétique, comme la fraude informatique.[9] [10] Les systèmes informatiques hérités, vulnérabilités de la chaîne d'approvisionnement et la pénurie de professionnels de la cybersécurité sont des domaines de plus en plus préoccupants. Près de quatre entreprises sur dix (39 %) et un quart des associations caritatives (26 %) signalent avoir subi des atteintes à la cybersécurité ou des cyberattaques au cours des 12 derniers mois. Un grand nombre d'organisations (surtout les PME) n'ont pas la capacité de se protéger et de répondre aux incidents.[11] Selon l'industrie, beaucoup d'entreprises ne comprennent pas les cyberrisques auxquels elles sont confrontées, les incitatifs commerciaux susceptibles de les pousser à investir dans la cybersécurité manquent de clarté et elles sont souvent insuffisamment motivées pour signaler les atteintes et les attaques.

Leadership et influence du Royaume-Uni sur la scène internationale

25. À l'international, la cyberexpertise du Royaume-Uni est très appréciée par nos partenaires. Il a contribué à l'accroissement de la capacité et de la volonté internationales d'affronter les cybermalveillances. Contrairement aux activités aveugles de certains de nos adversaires, elle a été renforcée par l'utilisation responsable de cybercapacités offensives conformes au droit britannique, au droit international et à nos positions déclarées publiquement.

26. Au cours de sa présidence du Commonwealth, le Royaume-Uni a conçu et dirigé la mise en œuvre de la Commonwealth Cyber Declaration. Cette déclaration relative à la cybersécurité illustre un engagement commun envers notre sécurité, notre prospérité et nos valeurs dans le cyberespace. Le réseau international de la National Crime Agency (NCA) a renforcé nos partenariats dans le domaine de l'application du cyberdroit à l'étranger, renforçant les relations entretenues au fil d'un long passé de réponse opérationnelle concertée. Par ailleurs, le Royaume-Uni a élargi son réseau international d'agents de cybersécurité et de sécurité technologique sur cinq continents et entrepris des travaux de renforcement des capacités dans 100 pays, renforçant la résilience, accroissant l'influence du Royaume-Uni et promulguant ses valeurs.

27. Le programme d'ambassadeurs de la cybersécurité Cyber Security Ambassador a développé les relations à long terme et aidé les entreprises britanniques à remporter des contrats internationaux importants. Les interventions du Royaume-Uni en matière de développement international, comme le Digital Access Programme, ont collaboré avec succès avec des pays partenaires en Afrique, en Asie et en Amérique latine, fournissant des conseils techniques pour améliorer la capacité de cybersécurité de leurs gouvernements, de leurs secteurs d'activité et de leurs utilisateurs, notamment en augmentant les compétences de cyberhygiène dans les communautés mal desservies pour permettre aux personnes les plus vulnérables de se protéger contre les risques et défis associés à la navigation sur Internet.

28. Cependant nous sommes confrontés à des approches concurrentielles à l'échelle internationale, dans un contexte où des concurrents systémiques comme la Chine et la Russie continuent de préconiser une plus grande souveraineté nationale sur le cyberespace pour résoudre les défis en matière de sécurité. La liberté de l'Internet s'estompe à l'échelle mondiale. L'ombre de la menace pèse sur la notion selon laquelle l'Internet est un espace partagé, propice à l'échange de connaissances et de biens entre les sociétés ouvertes.

[9] Définis comme des infractions à la loi relative au mauvais usage des ordinateurs Computer Misuse Act.
[10] ONS, Crime in England and Wales: year ending June 2021 (2021) (Criminalité en Angleterre et au Pays de Galles : année se terminant en juin 2021)
[11] DCMS, Cyber Security Breaches Survey 2021 (2021) (Enquête sur les atteintes à la cybersécurité)

Contrer les cybermenaces à l'encontre du Royaume-Uni et dissuader nos adversaires

29. Les menaces auxquelles nous sommes confrontés dans et à travers le cyberespace s'intensifient, se compliquent et s'aggravent depuis quelques années. Les cyberattaques contre le Royaume-Uni sont menées par un éventail d'acteurs étatiques, de groupes criminels (agissant parfois sous la direction d'États ou avec leur approbation implicite) et de militants de plus en plus divers à des fins d'espionnage, de gain commercial, de sabotage et de désinformation. De telles attaques entraînent des pertes financières considérables, le vol de propriété intellectuelle, la détresse psychologique, la perturbation des services et des biens et des risques pour notre infrastructure critique nationale, nos institutions démocratiques et nos médias. Elles risquent aussi de porter atteinte à la confiance des investisseurs, des consommateurs et d'amplifier les inégalités et préjudices existants. Pendant la pandémie de COVID-19, les attaques en ligne ont aggravé la pandémie parallèle de violence sexospécifique. Les attaques par rançongiciels sont de plus en plus sophistiquées et nuisibles. Même si globalement le niveau de cybermenace provenant d'acteurs hostiles est resté stable pendant la pandémie de COVID-19, ils l'ont exploitée comme une opportunité, modifiant leurs cyberopérations pour voler les vaccins, la recherche médicale et saper d'autres nations déjà grevées par la crise. La dépendance croissante à l'égard des technologies numériques du télétravail et des transactions en ligne a également accru l'exposition aux risques. Parallèlement, pour des raisons de littératie numérique limitée et de manque de sensibilisation aux mesures de cybersécurité pouvant être prises pour sécuriser la navigation sur Internet, les fossés numériques ont désuniformisé l'accès aux services en ligne, exposant les internautes aux abus et préjudices sur le Web.[12]

30. Le gouvernement a pris des mesures pour contrer ces menaces croissantes. Un investissement important dans nos capacités de renseignement nous a permis de mieux comprendre la menace et de mener des contre-campagnes secrètes plus efficaces. Nous avons développé une réponse répressive à la cybercriminalité intégrée, sous la direction de la National Crime Agency (NCA) et des cyberéquipes dédiées au sein de cellules régionales de la criminalité organisée et des forces de police locales d'Angleterre, du pays de Galles, d'Irlande du Nord et d'Écosse. Ces mesures ont consolidé notre avantage opérationnel et nos capacités d'enquête sur les cybercriminels et autres adversaires. D'autre part le gouvernement renforce la sécurité du nombre croissant de solutions d'identité numérique, en développant le cadre de confiance pour les identités et les attributs numériques du Royaume-Uni.[13] Il contribuera aussi à la lutte contre la criminalité impliquant une utilisation abusive des données d'identité. Le programme Cyber Choices de la NCA aide les personnes à faire des choix plus éclairés, les détournant de la criminalité pour utiliser leurs cybercompétences de manière utile et légale.

31. Nous avons beaucoup investi dans nos cybercapacités offensives, à travers le cyberprogramme d'offensive nationale National Offensive Cyber Programme d'une part et de l'autre, plus récemment, dans la création de la cyberforce nationale National Cyber Force (NCF). Cette cyberforce nationale rassemble pour la première fois le personnel du Government Communications Headquarters (GCHQ) (Quartier général des communications gouvernementales), du ministère de la Défense (MoD), du Secret Intelligence Service (SIS, service de renseignements aussi connu sous le nom de MI6) et de l'agence exécutive du ministère de la Défense Defence Science and Technology Laboratory (Laboratoire des sciences et technologies de la défense), sous un seul commandement. Elle opère dans et à travers le cyberespace pour assurer la sécurité du pays, protéger et promouvoir les intérêts du Royaume-Uni à l'échelle nationale et à l'étranger.

[12] NCSC, CyberAware

[13] DCMS, UK digital identity and attributes trust framework (2021) (Cadre de confiance pour les identités et les attributs numériques du Royaume-Uni)

32. Conjointement avec nos alliés, nous avons également cherché à augmenter le coût des activités hostiles parrainées par un État dans le cyberespace, en attribuant les attaques comme nous l'avons fait à l'occasion des récentes violations de SolarWinds et de Microsoft Exchange et en imposant des conséquences aux responsables. Le développement du régime autonome de cyber-sanctions du Royaume-Uni a ajouté un autre outil perturbateur, déjà utilisé pour répondre à des incidents comme les attaques WannaCry et NotPetya. Cependant et malgré tous ces efforts, nos méthodes de cyberdissuasion ne semblent pas encore avoir fondamentalement modifié le calcul du risque pour les attaquants, comme le montrent les pages suivantes consacrées à de récentes cyberattaques importantes.

Récentes études de cas de cyberattaques

En 2021, le Royaume-Uni a poursuivi avec ses partenaires mondiaux son travail visant à détecter et perturber les menaces communes, dont les plus constantes émanent de la Russie et de la Chine. En plus des menaces directes à la cybersécurité posées par l'État russe, ils ont pu constater qu'un grand nombre de gangs de crime organisé responsables des attaques par rançongiciel contre des cibles occidentales étaient basés en Russie. Plus que jamais déterminée à projeter son influence au-delà de ses frontières et portant un intérêt avéré aux secrets commerciaux du Royaume-Uni, la Chine continue de faire partie des acteurs hautement sophistiqués du cyberespace. Il est probable que la tournure de l'évolution de la Chine au cours de la prochaine décennie devienne le principal catalyseur des activités de cybersécurité du Royaume-Uni. Bien que moins sophistiqués que la Russie et la Chine, l'Iran et la Corée du Nord ont poursuivi leurs tentatives d'intrusion numérique pour atteindre leurs objectifs, notamment par le vol et le sabotage.

Cybercriminels utilisant les rançongiciels pour attaquer les services publics

En 2021, les rançongiciels ont pris la première place du classement des cybermenaces les plus importantes pour le Royaume-Uni. Tenant compte de l'impact probable d'une attaque réussie contre les services essentiels ou l'infrastructure critique nationale, le NCSC a évalué les rançongiciels comme étant potentiellement aussi nuisibles que l'espionnage parrainé par un État.[14]

En octobre 2020, une cyberattaque par rançongiciel lancée contre Hackney Council causait de nombreux mois de perturbations et l'obligeait à consacrer plusieurs millions GBP à sa rectification. À un moment critique de la pandémie de COVID-19, cette attaque a privé le Conseil de données importantes et perturbé de nombreux services, dont les impôts locaux et le versement des allocations. D'autres autorités locales ont subi des attaques similaires, au même titre que diverses organisations du secteur de l'enseignement.

[14] NCSC, Mitigating malware and ransomware attacks (2021) (Atténuer les attaques par logiciels malveillants et rançongiciels)

En mai 2021, une attaque par rançongiciel contre l'Irish Health Service Executive (HSE) perturbait les réseaux informatiques de santé et les hôpitaux irlandais pendant plus de 10 jours, faisant subir des conséquences réelles aux patients et à leurs familles. Certaines données volées de patients ont également été publiées en ligne. Le HSE, prestataire des services de santé et sociaux en Irlande, a dû fermer les réseaux nationaux et régionaux le même jour pour contenir l'incident. Une cybermalveillance a également été détectée sur le réseau du ministère irlandais de la Santé (DoH). Le déploiement d'outils au cours du processus d'enquête a néanmoins permis de détecter et stopper une tentative d'exécution de rançongiciel. L'attaque a également été ressentie en Irlande du Nord, empêchant certains services transfrontaliers aux patients d'accéder aux données détenues par le HSE.

Point crucial, aucune rançon n'a été versée dans un cas ou dans l'autre. **Le paiement des demandes de rançon n'est ni encouragé ni approuvé ni toléré par les services répressifs. Imaginons qu'une rançon soit versée :**

- **rien ne vous garantit que vous pourrez accéder à vos données ou à votre ordinateur ;**
- **votre ordinateur n'en serait pas pour le moins infecté ;**
- **l'argent versé servirait à financer des groupes criminels ;**
- **vous seriez plus susceptible d'être ciblé ultérieurement.**

Le NCSC publie des directives sur les moyens de défendre les organisations contre les attaques de logiciels malveillants ou de rançongiciels et notamment, sur la façon de se préparer à un incident et les mesures à prendre si votre organisation est déjà infectée.

Exploitation par les États des vulnérabilités stratégiques et des chaînes d'approvisionnement

L'atteinte à la société de logiciels SolarWinds et l'exploitation des serveurs Microsoft Exchange a mis en évidence la menace que représentent les attaques contre les chaînes d'approvisionnement. Ces deux attaques sophistiquées, par lesquelles les acteurs s'en sont pris à des éléments moins sécurisés comme les fournisseurs de services gérés ou les plates-formes logicielles commerciales des chaînes d'approvisionnement d'institutions économiques, gouvernementales et de sécurité nationale, comptent parmi les cyberintrusions les plus graves jamais observées par le NCSC.

Début décembre 2020, la société américaine de cybersécurité FireEye découvrait qu'un attaquant était parvenu à introduire une modification malveillante dans un produit qu'elle utilise et dont se sert également un grand nombre d'organisations du monde entier. Cette modification a permis à l'attaquant d'envoyer des commandes de niveau administrateur aux installations compromises de ce produit, pour pouvoir l'utiliser dans le cadre d'autres attaques ciblant les systèmes connectés.
L'attaque initiale lancée contre la chaîne d'approvisionnement a été menée à travers le logiciel Orion, outil de surveillance de réseau informatique développé par la société **SolarWinds**. L'implantation d'un code malveillant dans un fichier de mise à jour du logiciel remontait à mars 2020. En avril 2021, le NCSC et ses homologues de la sécurité aux États-Unis révélaient pour la première fois que le Service des renseignements extérieurs (SVR) russe était à l'origine de cette attaque, qui reste l'une des cyberintrusions les plus graves de l'ère moderne.[15]
SolarWinds confirmait qu'à l'échelle mondiale, 18 000 organisations dont des ministères américains avaient été touchées. Cet incident faisait partie d'une plus vaste série de cyberintrusions par le SVR, déjà à l'origine de

[15] FCDO, Russie : le Royaume-Uni et les États unis exposent une campagne mondiale d'activité malveillante lancée par les services de renseignement russes (2021)

tentatives d'accès aux réseaux informatiques des membres de l'OTAN et de plusieurs gouvernements européens.

Le 2 mars 2021, Microsoft annonçait publiquement que des acteurs sophistiqués avaient attaqué plusieurs serveurs **Microsoft Exchange**, avec lesquels des organisations du monde gèrent leurs e-mails, leur planification et leur collaboration. Selon l'évaluation de Microsoft, les premières intrusions remontaient à janvier 2021 et auraient été parrainées par l'État chinois. Microsoft a réagi en publiant plusieurs mises à jour de sécurité destinées aux serveurs concernés. En juillet 2021, le Royaume-Uni rejoignait un groupe de partenaires de même sensibilité pour confirmer que des acteurs soutenus par l'État chinois étaient responsables d'attaques touchant plus d'un quart de million de serveurs dans le monde.[16] L'attaque aurait très vraisemblablement été lancée à des fins d'espionnage à grande échelle et en particulier, pour l'acquisition d'informations personnellement identifiables (IPI) et de propriété intellectuelle.

Compromettre Microsoft Exchange a donné à l'auteur un point d'appui pour s'ancrer plus profondément dans les réseaux informatiques des victimes. Au moment de l'attaque, le gouvernement a rapidement conseillé les utilisateurs concernés, leur recommandant des mesures à prendre. Microsoft quant à elle a déclaré qu'à la fin du mois de mars les systèmes de 92 % de ses clients avaient été corrigés pour remédier à cette vulnérabilité.

[16] FCDO, le Royaume-Uni et ses alliés tiennent l'État chinois pour responsable d'un schéma de piratage généralisé (2021)

Moteurs du changement

33. Au cours de la prochaine décennie, **les données et la connectivité numérique continueront leur expansion rapide, confirmant leur rôle dans quasiment tous les aspects de notre vie**. Étayée par les données et l'infrastructure sur laquelle elles reposent, l'énorme croissance mondiale de l'accès et de l'utilisation de l'Internet crée de nouveaux marchés et augmente sa commodité, les choix et son efficacité. Mais elle augmente aussi considérablement la dépendance des pays à l'égard des systèmes numériques interconnectés, multipliant les opportunités d'activités malveillantes et le risque d'impacts significatifs dans le « monde réel ». À mesure que les technologies critiques et non critiques continuent de converger entre les secteurs, ces risques s'étendent vers de nouveaux domaines de notre économie. Le transfert de données et de services dans le Cloud, qui souvent sortent des limites territoriales du Royaume-Uni, nous rend encore plus vulnérables.

34. Nous constatons de plus en plus l'interaction entre les entreprises établies des secteurs réglementés comme les télécommunications et l'énergie et les entreprises nouvelles et largement non réglementées, comme celles qui fournissent des capacités de micro-génération, de recharge de véhicules électriques ou de « ville connectée ». Les infrastructures essentielles deviendront beaucoup plus distribuées et diffuses, aspects qui changeront fondamentalement l'impact de la réglementation sur la sécurité des fonctions et des services critiques sur lesquels nous nous appuyons. D'autre part cette diversification aura une incidence sur notre sécurité nationale au sens le plus large du terme, compliquant l'accès à l'information à des fins de répression ou de cybersécurité. Cette évolution de l'environnement se répercutera aussi plus largement sur les produits et services en dehors de notre infrastructure critique nationale traditionnelle.

35. Dans ce **paysage de plus en plus complexe**, les États, les entreprises et la société auront de plus en plus de mal à comprendre les risques auxquels ils sont confrontés et comment ils peuvent et doivent se protéger. La dépendance accrue à l'égard des fournisseurs tiers de services gérés, qui bénéficient souvent d'un accès privilégié aux systèmes informatiques de milliers de clients, crée de nouveaux risques qui doivent être pris en compte. Les appareils et les réseaux seront de plus en plus naturellement connectés à l'Internet, étendant le cyberespace à nos foyers, à nos véhicules, à l'environnement bâti et aux infrastructures industrielles. Les capteurs, wearables, dispositifs médicaux et la biométrie brouilleront encore plus la frontière entre les activités hors ligne et en ligne. Les cyberrisques se teinteront d'omniprésence, augmentant le volume généré de données personnelles et sensibles et l'impact potentiel d'une éventuelle violation des systèmes.

36. Dans ce contexte, les **menaces du cyberespace continueront d'évoluer et de se diversifier**, à mesure que les cybercapacités de haut niveau se banalisent et prolifèrent vers un éventail élargi d'États et de groupes criminels. Le nombre d'acteurs disposant de la capacité de cibler le Royaume-Uni dans le cyberespace et prêts à le faire augmentera. Les États multiplieront les types de leviers pour mener des activités perturbatrices, notamment par le biais d'acteurs « par procuration ». La transition accélérée vers le travail hybride et les restrictions imposées aux voyages internationaux consécutives à la pandémie ont accentué notre dépendance à l'égard des services numériques et incité les groupes criminels organisés à se tourner vers la cybercriminalité. Les signes de cette tendance se manifestent déjà. La dernière enquête sur la criminalité estime que les cybercrimes ont considérablement augmenté entre 2019 et 2021.[17] Créant une vulnérabilité réciproque pour tous ceux qui dépendent du cyberespace, ce défi ne touchera pas seulement le Royaume-Uni.

[17] ONS, Crime in England and Wales: year ending June 2021 (2021) (Criminalité en Angleterre et au Pays de Galles : année se terminant en juin 2021)

37. Le **cyberespace sera de plus en plus convoité**, les acteurs étatiques et non-étatiques luttant pour s'octroyer l'avantage stratégique dans et à travers ce nouvel incontournable. Les cyberopérations joueront un rôle de plus en plus important pour projeter la puissance sous le seuil des conflits armés et dans les situations de pré-conflit. Par ailleurs, les conflits futurs feront plus systématiquement appel aux cybercapacités. L'efficacité de l'action du Royaume-Uni dépendra de capacités de défense associées à de plus hauts niveaux de cyberrésilience. Les cyberopérations devront être intégrées à d'autres éléments de la force pour neutraliser les menaces et favoriser la mise en place d'activités de défense plus générales. L'espace fera de plus en plus partie des domaines d'activité, tels que définis dans la National Space Strategy (Stratégie spatiale nationale), ouvrant de nouveaux domaines de risque, mais créant également des opportunités pour le Royaume-Uni d'exploiter ses cybercapacités et d'y trouver d'autres moyens d'en tirer parti.[18]

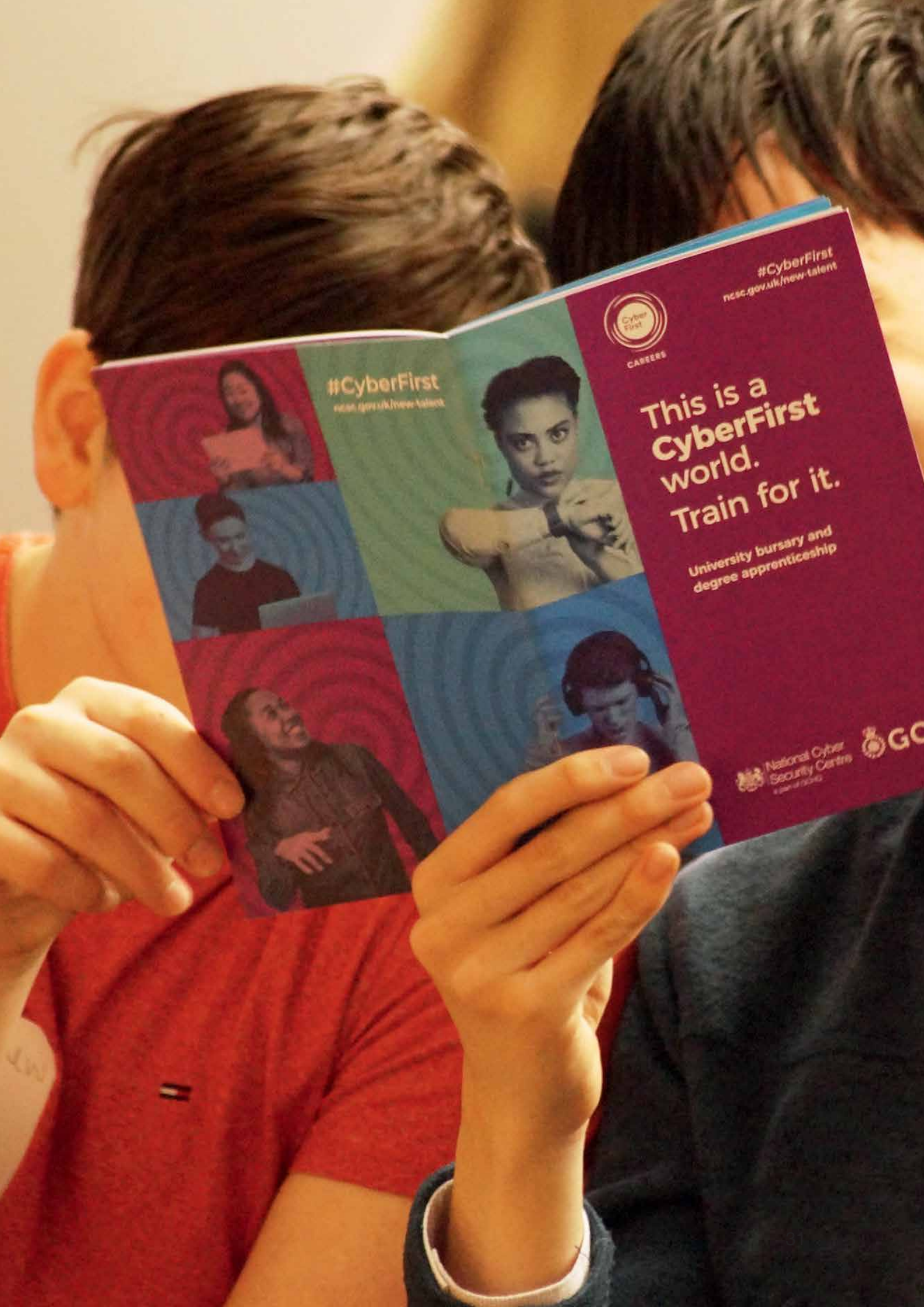
38. Les débats sur les règles gouvernant le cyberespace feront de plus en plus l'objet d'une **concurrence systémique entre les grandes puissances,** associée à l'incompatibilité des valeurs de pays qui veulent préserver un système basé sur des sociétés ouvertes et celles de concurrents systémiques comme la Chine et la Russie, défenseurs d'un système basé sur un contrôle de l'État renforcé comme seul moyen de sécuriser le cyberespace. L'Internet libre et ouvert subira la pression d'une telle situation, les États-nations, les grandes entreprises technologiques et d'autres acteurs favorisant des approches concurrentes en matière de normes techniques et de gouvernance de l'Internet.

39. Les **rivalités pour le contrôle d'un paysage technologique en évolution rapide** ne peuvent que l'exacerber. L'intégration de la technologie numérique dans notre vie quotidienne, nos entreprises et nos infrastructures fait de certaines technologies des éléments véritablement essentiels au fonctionnement de la société. Le pouvoir sera de plus en plus entre les mains des pays bénéficiant d'un avantage stratégique sur les plans scientifique, technologique et d'un accès aux données qui stimulent l'innovation, leur permettant d'exercer une influence sur les autres et de façonner les normes mondiales de la manière la plus avantageuse pour leurs propres intérêts économiques et politiques.

40. Les **technologies émergentes**, comme les jumeaux numériques, l'informatique quantique et les systèmes autonomes à grande échelle, au même titre que les informations qui en découlent, créeront de nouvelles opportunités, de nouveaux risques et ouvriront de nouvelles cybercapacités aux attaquants et défenseurs, à l'image des cryptomonnaies exploitées actuellement par les gangs de rançongiciels. Le leadership technologique est de plus en plus distribué et le Royaume-Uni ne parviendra pas à développer une capacité souveraine dans toutes les technologies qui comptent. Les États et les entreprises utilisent les normes techniques pour promouvoir leurs propres intérêts et les technologies clés risquent d'être façonnées par des acteurs qui ne partagent pas nos valeurs.

41. Depuis plus d'une décennie, le Royaume-Uni poursuit une stratégie nationale de cybersécurité ambitieuse, maintenant un niveau d'investissement considérable, établissant le pays parmi les leaders mondiaux du domaine de la cybernétique. Comme tente de l'illustrer l'analyse ci-dessus, des défis et des opportunités importants demeurent. Les sections suivantes de ce document décrivent notre réponse nationale.

[18] HMG, National Space Strategy (2021)


#CyberFirst
ncsc.gov.uk/new-talent
CAREERS
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

Notre réponse nationale

42. Un choix s'offre au Royaume-Uni dans cet environnement stratégique. Nous pourrions tout simplement nous contenter de suivre le rythme des menaces et des défis auxquels nous sommes confrontés dans un cyberespace de plus en plus complexe, consolidant les progrès des cinq dernières années et traitant les problèmes les plus urgents dans la mesure du possible. Toutefois cette approche nous exposerait à un double risque. Dans un premier temps, nous risquerions de ne pas réaliser pleinement le potentiel des atouts du Royaume-Uni dans le domaine du cyberespace pour soutenir les priorités nationales et d'en manquer les opportunités. Le deuxième risque est plus grave. Nous pourrions atteindre un point de basculement technologique et constater que les fondements de notre économie et de notre société futures sont façonnés par nos concurrents, nos adversaires et que nous devons redoubler d'efforts pour assurer notre propre sécurité.

43. À notre avis, plus l'importance fondamentale du cyberespace pour nos intérêts, ceux de nos alliés et de nos adversaires augmente, plus **la promotion de notre avantage concurrentiel pour négocier les méandres de ce paysage s'impose comme un impératif stratégique**. Non seulement il nous permettra de garantir notre sécurité actuelle, mais il nous aidera aussi à façonner le monde de demain et d'en tirer parti.

Notre vision, nos objectifs, nos principes

44. Notre vision du Royaume-Uni en 2030 est celle d'un pays qui **continue à faire partie des cyberpuissances mondiales de premier plan, responsable et démocratique, capable de protéger et de promouvoir ses intérêts dans et à travers le cyberespace, en adéquation avec ses objectifs nationaux**.

45. Nous poursuivrons cinq objectifs stratégiques pour la réaliser. Individuellement, chaque objectif vise à renforcer notre force nationale dans l'une des cinq dimensions du cyberpouvoir. Collectivement, leur but est d'améliorer notre capacité d'assurer le maintien d'un cyberespace reflétant nos valeurs et nos intérêts. Ces cinq objectifs ou « axes » constituent le cadre stratégique sur laquelle pivote notre activité. La deuxième partie définit les mesures que nous prendrons d'ici à 2025 par rapport à chacun d'entre eux.

- **Axe 1 : renforcer l'écosystème cyber du Royaume-Uni**, en investissant dans notre capital humain, dans les compétences et en approfondissant le partenariat entre le gouvernement, le monde universitaire et l'industrie.
- **Axe 2 : construire un Royaume-Uni numérique résilient et prospère**, en réduisant les cyberrisques pour permettre aux entreprises de maximiser les avantages économiques de la technologie numérique, que les citoyens se sentent moins menacés en ligne et qu'ils ne doutent plus que leurs données sont protégées.
- **Axe 3 : prendre l'initiative par rapport aux technologies essentielles au cyberpouvoir,** en renforçant notre capacité industrielle et en développant les structures nécessaires pour sécuriser les technologies futures.
- **Axe 4 : promouvoir le leadership et l'influence du Royaume-Uni sur la scène internationale, pour un ordre international plus sûr, prospère et ouvert**, en collaborant avec les partenaires du gouvernement et de l'industrie et en partageant l'expertise étayant le cyberpouvoir du Royaume-Uni.
- **Axe 5 : détecter, perturber et dissuader nos adversaires afin d'améliorer la sécurité du Royaume-Uni dans et à travers le cyberespace**, en recourant de manière plus intégrée, plus créative et plus régulière à l'ensemble des leviers du Royaume-Uni.

46. Ces objectifs sont censés se renforcer mutuellement. Par exemple, atteindre des niveaux plus élevés de cybersécurité et de résilience à l'échelle nationale fait partie des bases nécessaires d'une attitude internationale plus active. En revanche, compte tenu de nos chaînes d'approvisionnement mondiales et des menaces d'origine étrangère auxquelles nous faisons face, nous serons incapables d'assurer notre propre sécurité sans façonner plus activement le comportement des acteurs internationaux. Notre capacité d'influencer les débats mondiaux sur le cyberespace, l'internet et la technologie en général dépendra de notre capacité à préserver notre avantage technique et de la construction d'un écosystème d'innovation générateur d'un véritable avantage dans les technologies qui comptent le plus.

47. La **promotion d'un cyberespace libre, ouvert, pacifique et sûr** compte parmi les éléments fondamentaux de notre vision. La finalité stratégique de notre cyberpouvoir n'est pas d'alimenter les conflits ou d'apprêter le Royaume-Uni pour gagner un jeu à somme nulle. Comme l'indique la Revue intégrée, un monde dans lequel les sociétés et les économies ouvertes peuvent s'épanouir est le garant le plus fiable de notre prospérité, de notre souveraineté et de notre sécurité futures. Le Royaume-Uni collaborera avec des pays de même sensibilité pour promouvoir nos valeurs communes d'ouverture et de démocratie, en adoptant une **approche responsable et démocratique en matière de cyberpouvoir**. Il va donc de soi que nous appliquerons les **principes** suivants pour atteindre ces cinq objectifs stratégiques :

- Nous accorderons la priorité à la capacité des citoyens et des entreprises d'évoluer dans le cyberespace sans risque, en toute sécurité, afin de pouvoir maximiser les avantages économiques et sociétaux de la technologie numérique tout en exerçant leurs droits légaux et démocratiques.

- Nous œuvrerons pour que l'Internet reste ouvert et interopérable, qualités par lesquelles se définit le modèle le plus propice au soutien de la prospérité et du bien-être mondiaux, en résistant à la pression des États autoritaires qui prônent sa fragmentation et leur interprétation de la souveraineté numérique.

- Nous ferons un usage légitime, proportionné et responsable de nos cybercapacités, appuyé par une surveillance claire et notre engagement vis-à-vis du public et de nos alliés. Nous demanderons des comptes à tous ceux qui se conduisent de manière imprudente ou aveuglément dans le cyberespace.

- Nous prendrons des mesures contre l'utilisation criminelle du cyberespace, par tous les moyens dont nous disposons, dénonçant ceux qui utilisent des substituts criminels ou hébergent des groupes criminels sur leur territoire, en nous efforçant d'empêcher la prolifération de cybercapacités de haut niveau parmi les criminels.

- Nous défendrons une approche inclusive et multi-parties prenantes dans les débats sur l'avenir du cyberespace et de la technologie numérique, le respect des droits de la personne dans le cyberespace et la lutte contre les tendances à l'autoritarisme numérique et au contrôle de l'État.

Principaux changements dans notre approche

48. Dans de nombreux domaines, notre stratégie s'appuiera sur notre approche actuelle et cherchera à améliorer, à élargir ou à adapter nos efforts au besoin. Les principales différences avec la Stratégie nationale de cybersécurité 2016-2021 sont énoncées ci-dessous. Elles reflètent notre ambition plus générale de consolider la position du Royaume-Uni parmi les cyberpuissances mondiales de premier plan.

49. Volonté de maintenir le Royaume-Uni à la fine pointe de la cybernétique. Au cours des trois prochaines années, le gouvernement investira 2,6 milliards GBP dans la cybernétique et l'informatique héritée. Cette somme s'ajoute à un investissement important dans la National Cyber Force annoncé dans la Spending Review 2020 (Revue des dépenses) (SR20). Elle inclut une augmentation de 114 millions GBP du budget affecté au National Cyber Security Programme (Programme national de cybersécurité), ainsi qu'une augmentation des investissements également annoncés dans les domaines de la recherche et du développement (R&D), du renseignement, de la défense, de l'innovation, de l'infrastructure et des compétences, dont tous joueront un rôle dans la constitution du cyberpouvoir du Royaume-Uni. L'investissement dans la cybernétique annoncé dans les revues des dépenses SR20 et SR2021 dépasse largement les 1,9 milliard GBP sur cinq ans engagés dans la stratégie précédente.[19]

50. Une cyberstratégie nationale plus complète. La cybersécurité demeure au cœur de cette stratégie, mais rassemble désormais l'ensemble des capacités du Royaume-Uni à l'intérieur et à l'extérieur du gouvernement. Elle donne davantage de poids aux technologies et infrastructures critiques qui sous-tendent le cyberespace, aide les cyberentreprises britanniques à évoluer positivement sur les marchés domestiques et à faire concurrence sur les marchés étrangers, intensifie l'action internationale pour façonner et influencer l'avenir du cyberespace tout en intégrant la cyberoffensive aux leviers du pouvoir. Elle exige une approche stratégique réellement cohérente, nationale. La stratégie répartit les responsabilités en matière de leadership et de coordination entre les secrétaires d'État et implique beaucoup plus étroitement les administrations décentralisées. Elle s'appuie sur notre capacité éprouvée de coordonner les efforts sur l'ensemble du gouvernement, un des principaux atouts du Royaume-Uni.

[19] HM Treasury, Autumn Budget and Spending Review 2021 (2021) (Trésor public, budget automnal et revue des dépenses)

51. Un effort pansociétal. Nous visons une approche stratégique nationale, façonnée par la prise de décisions dans les organisations à travers le pays et capable de l'orienter, servant de base à une collaboration plus poussée avec nos partenaires du Royaume-Uni et du monde entier. Nous devrons multiplier nos efforts pour la concrétiser. Il s'agira notamment, à court terme : (i) d'établir un nouveau National Cyber Advisory Board (Comité consultatif national sur la cybernétique), en invitant les cadres supérieurs des secteurs privé et tertiaire à remettre en question, appuyer et éclairer notre approche ; (ii) de détourner nos programmes d'innovation dans le secteur de la cybernétique des grandes initiatives souvent basées à Londres en adoptant un modèle régional, établi en partenariat avec l'industrie locale, les innovateurs, les services répressifs et le monde universitaire; (iii) de prendre des mesures pour accroître la diversité de l'effectif cybernétique, reconnaissant que la capacité de tirer parti des compétences, des talents de l'ensemble de la population et de les entretenir est essentielle à notre sécurité nationale. Dans sa substance, la stratégie elle-même a bénéficié des échanges avec les gouvernements décentralisés d'Irlande du Nord, d'Écosse, du Pays de Galles et des partenaires de l'industrie, des services répressifs, régulateurs, du monde universitaire, de la société civile et internationaux. Notre intention est de veiller à ce que ces dialogues restent ouverts pendant sa période de mise en œuvre.

52. Une approche plus proactive pour favoriser et protéger notre avantage concurrentiel dans les technologies essentielles au cyberespace. La Revue intégrée et les stratégies consécutives ont déjà commencé à appliquer cette approche dans des domaines comme l'intelligence artificielle, les technologies quantiques et les données. Cette stratégie confirme les engagements relatifs à la conception de microprocesseurs sécurisés, à la sécurité des technologies opérationnelles et à la cryptographie. Elle annonce la création d'un laboratoire national pour la sécurité des technologies opérationnelles. Ce nouveau centre d'excellence se concentrera sur l'établissement du plus haut niveau de cyberrésilience possible en partenariat avec l'industrie et le monde universitaire. Elle annonce également l'expansion des capacités de recherche du National Cyber Security Centre (NCSC), avec notamment le nouveau centre de recherche appliquée de Manchester, l'accent étant mis sur les technologies émergentes dans des domaines tels que les villes connectées et les transports. La stratégie s'appuie également sur notre travail fructueux visant à promouvoir les approches qui intègrent la sécurité dans les nouvelles technologies, pour les rendre « secure by design » (sécurisé de façon native). Il s'agira par conséquent d'investir et de mobiliser davantage les leviers réglementaires et législatifs en cas de besoin, pour promouvoir des chaînes d'approvisionnement technologiques plus diversifiées, plus sûres et plus résilientes comme nous l'avons déjà fait pour le secteur des télécommunications.

53. Renforcer considérablement nos efforts de base pour promouvoir la cybersécurité, en suivant l'exemple du gouvernement. Nous investirons plus que jamais dans une refonte rapide et radicale de la cybersécurité du gouvernement, en établissant des normes claires pour les ministères et en traitant l'infrastructure informatique héritée. À l'horizon 2025, les fonctions essentielles du gouvernement auront été considérablement renforcées pour faire face aux cyberattaques et nous veillerons à ce que toutes les organisations gouvernementales, sur l'ensemble du secteur public, soient résilientes face aux vulnérabilités connues et aux méthodes d'attaque d'ici à 2030. Nous multiplierons nos efforts pour protéger les citoyens et les mobiliser tout en les délestant le plus possible du fardeau de responsabilité en la matière. Nous renforcerons l'environnement numérique, protégeant les citoyens contre la cybercriminalité et la fraude et rendrons davantage responsables les fabricants, détaillants, prestataires de services et le secteur public du renforcement des normes de cybersécurité. Nous augmenterons le niveau d'engagement et d'investissement du secteur privé dans la cyberrésilience, en harmonisant la réglementation et les incitatifs sur l'ensemble de l'économie et en proposant davantage de soutien. D'autre part, nous mettrons davantage l'accent sur les

risques liés à la chaîne d'approvisionnement, en testant diverses interventions pour aider les organisations à gérer les risques liés à la cybersécurité posés par leurs fournisseurs et en veillant à ce que les meilleures pratiques se transmettent tout au long de la chaîne d'approvisionnement.

54. Des campagnes plus intégrées et soutenues pour perturber et dissuader nos adversaires, protéger et promouvoir les intérêts du Royaume-Uni dans le cyberespace. Ces campagnes s'appuieront sur un plus large éventail de leviers diplomatiques, stratégiques et opérationnels à l'échelle du gouvernement. Elles seront fortement soutenues par la création et l'expansion de la National Cyber Force (NCF), basée à Samlesbury dans le Lancashire. Nous utiliserons plus régulièrement les capacités de cette cyberforce nationale pour perturber les menaces d'acteurs étatiques et non étatiques, mais aussi pour soutenir les intérêts plus généraux du Royaume-Uni en matière de sécurité nationale.
Nos campagnes bénéficieront également de nouveaux investissements majeurs dans des capacités de haut niveau de répression aux niveaux national, régional et local. Elles nous aideront à traiter la menace substantielle que constituent les rançongiciels et des cybercriminels de plus en plus créatifs. Nous continuerons également à utiliser le régime autonome de cybersanctions et le processus d'attribution du Royaume-Uni pour imposer des coûts à nos adversaires, tout en dénonçant les attaques malveillantes et irresponsables.

55. Placer le cyberpouvoir au cœur du programme de politique étrangère du Royaume-Uni et reconnaître que chaque élément de la stratégie demande un engagement international. Nous renforcerons nos principales alliances et échangerons avec un plus large éventail de pays pour contrer la propagation de l'autoritarisme numérique. Au cours des prochaines années, nous augmenterons la part d'investissements consacrée aux programmes internationaux visant à soutenir les pays partenaires, en les aidant à renforcer leur résilience et leurs capacités de lutter contre les cybermenaces. Nous ferons meilleur usage de l'ensemble de nos atouts nationaux et en particulier, de notre expertise opérationnelle et stratégique en communications, de notre leadership intellectuel, de nos relations commerciales et de nos partenariats industriels pour appuyer nos objectifs internationaux.

Rôles et responsabilités à l'échelle du Royaume-Uni

56. Notre stratégie reposera fondamentalement sur une cyber-perspective pansociétale. Nous devons établir un partenariat durable et équilibré avec l'ensemble des secteurs public, privé et tertiaire, chacun jouant un rôle important dans notre effort national.

Citoyens

57. Cette stratégie entend soulager le plus possible les citoyens du fardeau de la cybersécurité. Nous n'en continuerons pas moins, tous, de jouer un rôle important dans ce domaine. Le gouvernement fera tout son possible pour empêcher les cyberattaques avant qu'elles ne nuisent à la population. Le contournement par certains auteurs de menaces des dispositifs de protection mis en place est toutefois inévitable. Nous pouvons tous prendre des mesures pour améliorer la sécurité des biens auxquels nous tenons, autant dans le monde physique que dans l'univers virtuel.[20] Il nous appartient d'assumer personnellement la responsabilité de prendre toutes les mesures raisonnables pour protéger non seulement notre matériel, nos smartphones et autres appareils, mais aussi les données, logiciels et systèmes synonymes de liberté, de flexibilité et de commodité dans nos vies privée et professionnelle. À cette fin, le gouvernement fournit des conseils techniquement exacts, opportuns et réalisables. Les organisations de la société civile et les groupes communautaires jouent également un rôle important pour aider les gens à comprendre et à se protéger contre les cyberrisques.

[20] Source de conseils publiés en ligne par le gouvernement, Cyber Aware contribue à la sécurité numérique des internautes.

De nombreuses associations caritatives, par exemple, offrent aux groupes vulnérables un soutien ciblé, des conseils et des activités de sensibilisation.

Entreprises et organisations

58. Il incombe aux entreprises et organisations de faire le nécessaire pour gérer efficacement leurs cyberrisques, devenir cyber-résilientes, soutenir leurs clients et les utilisateurs de leurs services. Les entreprises et les organisations dépendent de plus en plus des technologies numériques et des services en ligne pour fonctionner, innover et se développer. Cette dépendance améliore les services, mais crée également de nouveaux risques et défis, notamment compte tenu du volume exponentiel de données à caractère personnel et d'actifs numériques dont elles sont responsables. Elles héritent par conséquent de la responsabilité de protéger ces données et ces biens, tout en assurant le maintien des services. Tout manquement dans ce domaine peut avoir de graves conséquences pour la réputation et l'économie des organisations, mais aussi porter préjudice à leurs clients. Les exploitants de services essentiels et fournisseurs de services numériques clés (comme les services infonuagiques), ont des responsabilités particulières liées à la gestion des cyberrisques auxquels ils font face et à leur obligation de respecter les termes de la règlementation sur les réseaux et systèmes d'information Network & Information Systems Regulations (« NIS regulations »). Les conseils et directives du NCSC contribuent au soutien des entreprises et organisations, en les aidant à protéger leurs informations, actifs et systèmes. Le Information Commissioner's Office (ICO - Office du commissaire à l'information) fournit également des conseils aux organisations quant à leurs obligations en matière de cybersécurité, au titre du Règlement général sur la protection des données du Royaume-Uni.

Le secteur de la cybersécurité et les grandes sociétés technologiques

59. Le secteur de la cybersécurité en pleine croissance du Royaume-Uni joue un rôle essentiel dans la réponse aux cybermenaces émergentes et aux défis auxquels est confronté notre pays. La prolifération rapide des produits connectables et la transformation numérique accélérée des entreprises et organisations offrent au secteur des opportunités de croissance et d'innovation, liées à la fourniture de nouveaux services et produits. Cette stratégie décrit la manière dont le gouvernement continuera de soutenir la croissance du secteur de la cybersécurité du Royaume-Uni, de tirer parti de ses capacités et de son expertise en maintenant et en renforçant nos partenariats. Nous souhaitons également renforcer les partenariats plus généraux entre le monde universitaire, l'ensemble de la communauté technique et le secteur privé, afin d'être sûrs de tirer pleinement parti de l'expertise et du savoir-faire techniques du Royaume-Uni.

60. Les grandes sociétés technologiques fournisseuses de services numériques ont un rôle crucial à jouer pour garantir la sécurité de l'environnement dans lequel doivent évoluer les entreprises et organisations britanniques. Cette vérité s'applique tout particulièrement aux fournisseurs de services gérés et de plateformes intégrant plusieurs activités. Ils doivent veiller à ce que leurs services soient « sécurisés par défaut » et ne dépendent pas excessivement de mesures de protection prises par leurs clients. Les grandes sociétés technologiques ont également la responsabilité particulière de prioriser leur propre cyberrésilience. La dépendance croissante des entreprises, du gouvernement et de la société en général à l'égard des services infonuagiques et en ligne crée des vulnérabilités et interdépendances à la fois nouvelles et uniques.

Gouvernement

61. Le **gouvernement du Royaume-Uni** est particulièrement bien placé pour rassembler les renseignements nécessaires pour comprendre les menaces les plus sophistiquées, élaborer et faire appliquer la loi, établir des normes nationales et contrer les menaces d'acteurs hostiles, notamment par la conduite d'opérations cyberoffensives. À travers cette stratégie, nous investirons dans le renforcement de nos cybercapacités nationales. Les ministères du gouvernement et les organismes du secteur public sont également responsables de la protection de leurs propres réseaux et systèmes. En tant que détenteur de données importantes et que prestataire de services, le gouvernement prend des mesures rigoureuses pour assurer la protection de ses actifs informationnels. Et enfin, le gouvernement a également l'importante responsabilité de conseiller et d'informer les citoyens, les entreprises et les organisations quant à ce qu'ils doivent faire pour se protéger en ligne. Il s'agit au besoin d'établir les normes que nous demandons aux principales entreprises et organisations de respecter, afin d'assurer la protection de tous les citoyens.

62. La plupart des domaines de la cyberpolitique et la majorité des mesures décrites dans cette stratégie concernent des questions réservées comme la sécurité nationale, les affaires étrangères et la défense, les télécommunications, les normes et la sécurité des produits, la protection des consommateurs. L'élaboration et la mise en œuvre de cette stratégie n'en dépendent pas moins des contributions, de l'action et des investissements des **gouvernements décentralisés d'Irlande du Nord, d'Écosse et du Pays de Galles**. C'est tout particulièrement le cas quand ils concernent des domaines de politique décentralisée relevant principalement des axes « écosystème » et « résilience » de cette stratégie, comme l'éducation, les services de police et la cyberrésilience de certains secteurs critiques dont leurs propres secteurs publics. La coordination et la coopération entre les quatre nations du Royaume-Uni sont essentielles pour maximiser l'impact de la stratégie sur l'ensemble du pays. Elles exigent un échange régulier et précoce du Cabinet Office et d'autres ministères du gouvernement britannique avec leurs homologues gallois, écossais et d'Irlande du Nord, dans un but d'échange d'informations sur les priorités et les plans à mettre en œuvre. Elles permettent également d'éviter les doublons et de maximiser le rapport qualité-prix du financement public. Les gouvernements décentralisés continueront d'élaborer leurs propres stratégies et plans en matière de cybernétique, en les alignant sur cette stratégie du gouvernement britannique.

National Cyber Security Centre

« Acteur de l'effort visant à faire du Royaume-Uni l'endroit le plus sûr pour vivre et travailler en ligne »

Faisant partie du GCHQ, le National Cyber Security Centre (NCSC) a été lancé officiellement en 2017 pour jouer le rôle d'autorité nationale du Royaume-Uni spécialiste de l'environnement de la cybersécurité, partager les connaissances, traiter les vulnérabilités systémiques et assurer le leadership dans le traitement des principales questions liées à la cybersécurité nationale.[21] L'établissement du NCSC a simplifié les structures opérationnelles du gouvernement, transformé la capacité du Royaume-Uni de répondre aux cyberincidents à l'échelle nationale et lancé le déploiement des services numériques innovants qui ont contribué à faire de la navigation en ligne un procédé automatiquement plus sûr pour les organisations et les particuliers.

Nous veillons à ce que le NCSC soit en mesure de relever les défis de la prochaine décennie, en clarifiant les capacités et attributs durables qui sous-tendent son travail, en les finançant de façon durable et en concentrant leur utilisation dans les domaines où l'état actuel de l'expérience opérationnelle nous indique qu'ils auront le plus d'impact possible à l'échelle nationale.

Les capacités et attributs durables qui sous-tendent le travail du NCSC sont :

- une expertise technique de classe mondiale dans les disciplines de la cybersécurité et les spécialisations dont le Royaume-Uni a besoin ;
- des connaissances inégalées des cybermenaces actuelles et potentielles (intention et capacité) menaçant le Royaume-Uni ;
- l'accès à la gamme complète de capacités et d'autorités de sécurité nationale du Royaume-Uni pour les objectifs de cybersécurité ;
- l'accès direct aux communautés de cybersécurité en collaboration avec des partenaires du monde universitaire, de l'industrie et internationaux ;
- les capacités et services cryptographiques, essentiels à la sûreté et à la sécurité des intérêts du Royaume-Uni à l'échelle mondiale.

Dans le cadre de la nouvelle stratégie, le NCSC sera surtout responsable :

- **de la prise de mesures directes pour réduire les cyberpréjudices subis par le Royaume-Uni** en assurant une protection à l'échelle nécessaire au moyen de services numériques (ex. cyberdéfense active), en favorisant l'évolution de la technologie, en gérant la réponse en cas de cyberincidents d'importance nationale et, avec la National Cyber Force (NCF), en contrant directement les cyberopérations de nos adversaires ;

[21] HMG, National Cyber Security Strategy 2016 to 2021 (2016): paragraphe1.9

- **d'aider l'ensemble de la société britannique à se protéger** en fournissant une expertise sur mesure et des connaissances uniques dont les citoyens, entreprises et organisations du Royaume-Uni peuvent se servir pour se protéger et contribuer à l'effort visant à faire du Royaume-Uni un pays plus sûr pour tous les internautes ;
- **de contribuer au contenu technique de la politique et de la règlementation du gouvernement britannique régissant les aspects les plus importants de la cybersécurité**, en fournissant aux responsables des politiques de Whitehall des données techniques faisant autorité et une évaluation des menaces découlant des capacités de base du NCSC, en appuyant l'élaboration et la mise en œuvre de politiques et de règlements pour assurer la sécurité numérique des citoyens, organisations et intérêts du Royaume-Uni ;
- **de contribuer aux capacités souveraines du Royaume-Uni** à travers le National Crypt-Key Centre du NCSC, mis en place pour protéger l'information et les services critiques sur lesquels comptent l'armée et la communauté de sécurité nationale du Royaume-Uni, notamment pour lutter contre les attaques de nos adversaires les plus compétents ;
- **de soutenir la croissance des compétences et des investissements en cybersécurité**, en fournissant les bases techniques à tous les niveaux de cyberéducation, en mobilisant et en soutenant l'industrie, en catalysant l'investissement dans le cybersecteur.

Le NCSC contribuera également à **l'évaluation des progrès** par rapport aux objectifs de cette cyberstratégie nationale à travers NCSC Assessments, fonction britannique de cyberévaluation indépendante sur le plan éditorial.

National Cyber Force

Créée en 2020, la National Cyber Force (NCF) assure la surveillance rapprochée dans et à travers le cyberespace pour contrer, perturber, discréditer et contester les auteurs d'activités susceptibles de nuire au Royaume-Uni ou à ses alliés, assurer la sécurité du pays, protéger et promouvoir les intérêts du Royaume-Uni sur les territoires nationaux comme à l'étranger. À parts quasiment égales, la NCF se compose de personnel de la défense et des services de renseignement, dont il réunit l'expertise, les ressources et les pouvoirs sous une structure de commandement unique. Il sera basé à Samlesbury, dans le Lancashire.

La NCF s'acquitte d'un large éventail de résultats dans l'intérêt de la sécurité nationale, notamment dans les domaines du soutien à la défense, du bien-être économique du Royaume-Uni et de la prévention des crimes graves. Ses activités vont du tactique au stratégique et ciblent aussi bien les acteurs étatiques que non étatiques. Ses travaux visent trois catégories principales :

- lutter contre les menaces des terroristes, des criminels et des États qui se servent de l'Internet pour agir au-delà des frontières territoriales et nuire au Royaume-Uni et à d'autres sociétés démocratiques ;
- lutter contre les menaces qui perturbent la confidentialité, l'intégrité et la disponibilité des données et services dans le cyberespace (c.-à-d. soutenir la cybersécurité) ;
- contribuer aux opérations de défense du Royaume-Uni et à la réalisation de son programme de politique étrangère (en intervenant dans le cadre d'une crise humanitaire pour protéger les civils, par exemple).

Les opérations de la NCF peuvent servir à influencer les particuliers et les groupes, perturber les systèmes en ligne et de communication, altérer le bon fonctionnement des systèmes physiques. Ce type d'activité s'apparente à l'offensive informatique dans le cyberespace dite « cyberoffensive ».

Les opérations de la NCF sont menées conformément à un cadre juridique bien établi, qui comprend la Intelligence Services Act 1994 (Loi relative aux services de renseignement) et la Investigatory Powers Act 2016 (Loi relative aux pouvoirs d'enquête). Comme il l'a déjà clairement déclaré, le Royaume-Uni développe et déploie ses capacités conformément au droit international et notamment, au droit des conflits armés s'il y a lieu. L'approbation ministérielle, la surveillance judiciaire et l'examen parlementaire auxquels sont soumises ses activités font du régime de gouvernance des cyberopérations du Royaume-Uni l'un des plus robustes au monde.

Le Royaume-Uni n'a pas pour habitude de publier la substance de cyberopérations individuelles, mais les types d'activités opérationnelles suivant font partie des missions que pourraient envisager la NCF :

- empêcher les groupes terroristes d'exécuter leurs plans en désactivant leurs communications de commandement et de contrôle et en limitant la diffusion des médias extrémistes ;
- réduire le risque de préjudice subi par les forces armées britanniques en dégradant les systèmes d'armes adverses ;
- défendre la démocratie et les élections libres, justes et ouvertes en s'opposant aux campagnes de désinformation organisées d'un État ayant pour but de les saper ;
- empêcher les groupes criminels de tirer profit de leurs activités en perturbant leur utilisation des plateformes et services en ligne ;
- contribuer aux mesures visant à faire appliquer les sanctions internationales en perturbant les efforts faits pour les éviter ;
- protéger le Royaume-Uni et d'autres pays contre les cyberattaques en perturbant l'infrastructure qu'exploitent les adversaires pour les exécuter ;
- protéger les populations civiles en cas de crise humanitaire en préservant leur capacité d'accéder aux informations critiques.

En tant que centre d'excellence national pour les opérations fondées sur les effets dans et à travers le cyberespace, la NCF transformera l'aptitude du Royaume-Uni à développer, intégrer et utiliser ces capacités en tandem avec d'autres intervenants et à en optimiser l'efficacité.

Réseau national de lutte contre la cybercriminalité des services répressifs

Établi dans le cadre de la Stratégie nationale de cybersécurité 2016-2021, prêt à fournir une réponse axée sur le renseignement à toutes les formes de cyberattaques contre des particuliers, des organisations ou visant des secteurs entiers, le réseau national de lutte contre la cybercriminalité des services répressifs a élaboré une réponse entièrement intégrée à la cybercriminalité. Ce système à l'échelle du pays opère aux niveaux national, régional et local. Il fournit des soins aux victimes, aide les entreprises et les particuliers à se protéger, à récupérer rapidement et veille à ce que les auteurs n'échappent pas au couperet de la justice pénale.

La cellule nationale de lutte contre la cybercriminalité National Cyber Crime Unit (NCCU) de l'agence nationale de lutte contre la criminalité **National Crime Agency (NCA)** assure le leadership et la coordination à l'échelle nationale de la réponse, avec l'appui d'un réseau de cellules régionales de lutte contre la cybercriminalité **Regional Cyber Crime Units (RCCU)** établies dans chacune des neuf régions policières d'Angleterre et du Pays de Galles, en partenariat avec leurs homologues de Police Scotland et de Police Service of Northern Ireland, ainsi qu'avec la cellule de lutte contre la cybercriminalité Cyber Crime Unit (CCU) des services de police de la capitale anglaise, Metropolitan Police Service.

Ces moyens sont également complétés par des cellules locales de lutte contre la cybercriminalité **Local Cyber Crime Units (LCCU)** dédiées, incorporées aux 43 services de police nationaux et synchronisées par un coordinateur régional. Ces CCU régionales et locales peuvent enquêter et poursuivre les contrevenants, aider les entreprises et les victimes à se protéger contre les attaques et collaborer avec des partenaires pour éviter que des personnes vulnérables ne se laissent entraîner dans la cybercriminalité.

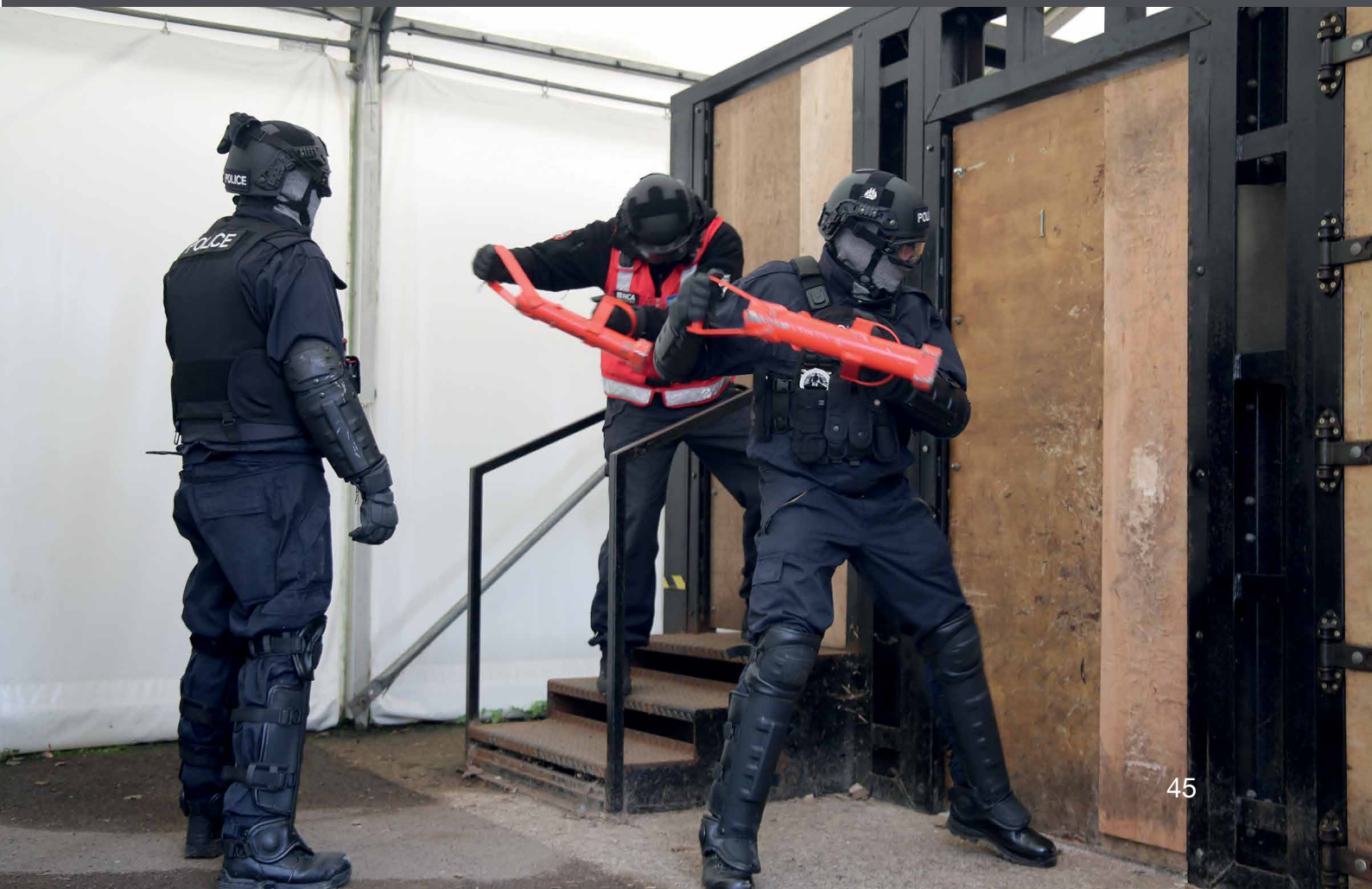
Le signalement, le triage et l'analyse centralisés de la criminalité sont assurés par le centre de signalement des manœuvres frauduleuses et de la cybercriminalité **Action Fraud**, hébergé par la **City of London Police**. Les cas les plus graves et/ou les plus complexes sont ensuite renvoyés à la NCA et au réseau régional. Les autres sont confiés aux diverses forces locales. La City of London Police coordonne également le soutien aux victimes, notamment par l'intermédiaire de la cellule de soutien aux victimes de la criminalité économique **Economic Crime Victim Care Unit**.

Les systèmes sont en cours d'intégration dans les capacités transformées de criminalistique, de renseignement et de partage de données. Le but de cette intégration est de construire une plateforme unique, par laquelle les cellules nationales et régionales pourront accéder à l'intégralité de l'éventail de capacités et d'outils de haut niveau spécialisés en cours d'élaboration. Elle inclut notamment la capacité de collaborer efficacement avec les partenaires de la communauté de la sécurité et du renseignement, particulièrement pour répondre aux menaces mixtes associant des éléments criminels et étatiques. Toujours

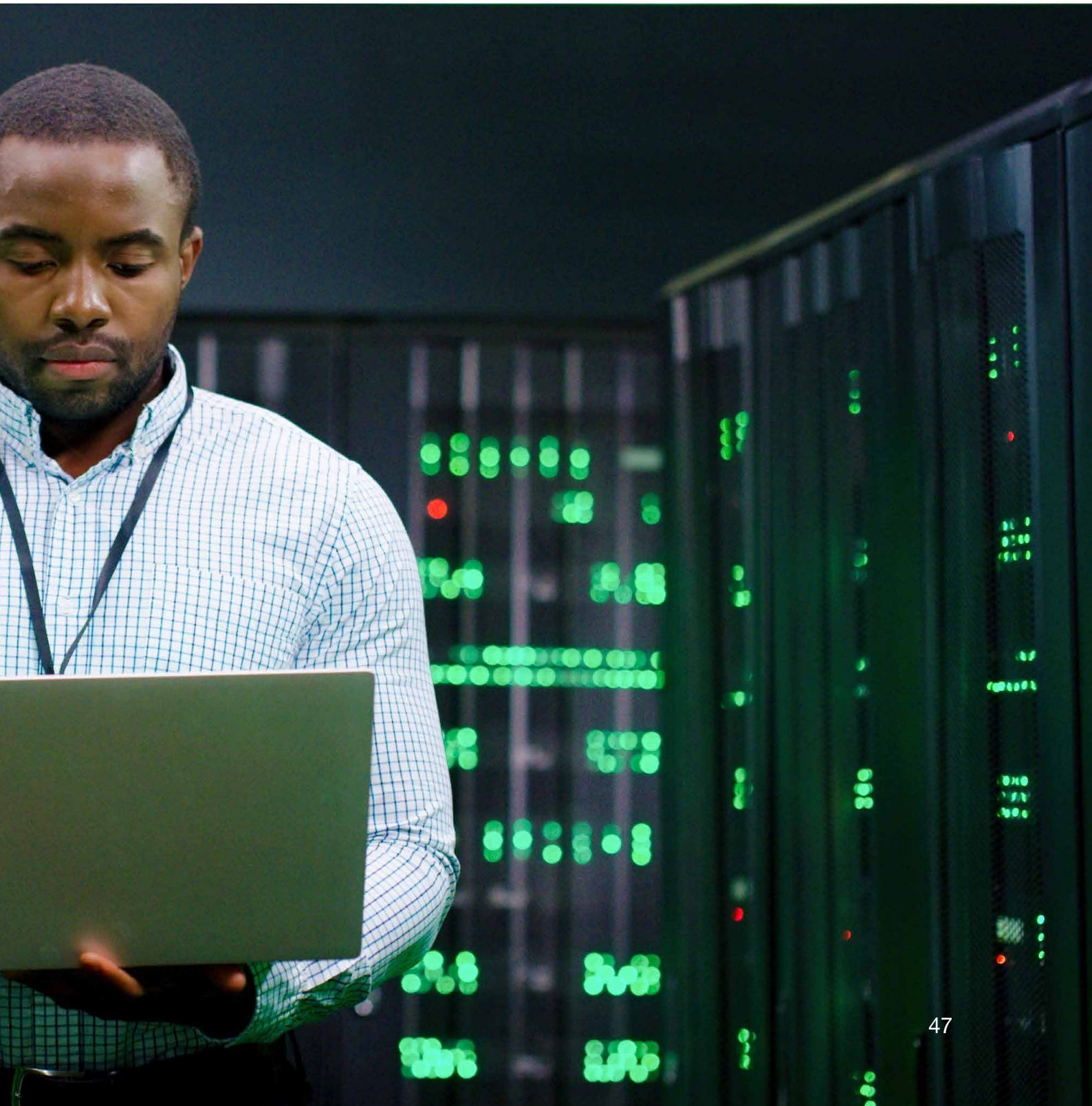
en vertu du principe « construire une fois, construire à l'échelle nationale pour l'ensemble du réseau de lutte contre la cybercriminalité », ces capacités sont accessibles aux cellules locales de lutte contre la cybercriminalité par le biais de coordonnateurs régionaux. Cette approche systémique se traduit déjà par une réponse largement plus efficace à la menace cybercriminelle.

Le Réseau de lutte contre la cybercriminalité des services répressifs continuera de motiver la réponse de notre justice pénale aux activités malveillantes dans le cyberespace, tous auteurs confondus de la menace aux échelles internationale, nationale, régionale et locale. Une gamme d'autres méthodes perturbatrices complèteront nos actions dans ce domaine en :

- développant des cybercapacités spécialisées d'enquête et perturbatrices de haut niveau ;
- recourant au vaste réseau international de la NCA pour appuyer les interventions des pays partenaires au moyen de renseignements et de données probantes ;
- empêchant les groupes criminels de profiter de leurs activités en perturbant leur utilisation des marchés criminels et des services habilitants ;
- protégeant le Royaume-Uni et les autres pays contre les cybercrimes, en dégradant et en perturbant l'infrastructure exploitée pour les commettre ;
- contribuant à l'activité de sanction et d'attribution publique contre les délinquants de haut rang ;
- en saisissant les cryptomonnaies et autres biens issus de la cybercriminalité.



2e partie :
Mise en œuvre



Axe 1 : l'écosystème cyber du Royaume-Uni

Renforcer l'écosystème cyber du Royaume-Uni

63. La réussite de cette stratégie dépend de la capacité du Royaume-Uni de rassembler les personnes, les connaissances et partenariats aptes à l'assurer. Nous devons pouvoir compter sur une main-d'œuvre diversifiée et techniquement qualifiée, sur une communauté de recherche dynamique, sur un cybersecteur concurrentiel à l'échelle internationale et un écosystème d'innovation régional prospère capable de nous placer au premier plan des technologies critiques, le tout reposant sur des partenariats plus solides entre le gouvernement, l'industrie et le monde universitaire.

64. La croissance de l'écosystème cyber doit être auto-entretenue et ne pas dépendre d'interventions gouvernementales. Au cours de cette stratégie, nous passerons du financement d'une gamme de programmes de compétences et d'innovation largement élaborés sur mesure et gérés de façon centralisée à une approche plus durable, systémique et régionale. Nous nous appuierons sur des réformes plus générales, engagées par le gouvernement dans le domaine des compétences et des systèmes d'éducation pour soutenir et donner envie à un plus grand nombre de personnes d'acquérir les compétences dont elles ont besoin pour poursuivre une carrière dans le domaine de la cybernétique. Par ailleurs, nous prioriserons diverses actions concrètes pour accroître la diversité des cybereffectifs. Il ne s'agit pas seulement de veiller à ce que tout le monde puisse accéder à ces emplois et carrières, mais aussi d'en comprendre le caractère critique pour notre sécurité nationale et de faire le nécessaire pour tirer parti du talent et des compétences de l'ensemble de la population. Nous veillerons également à ce que la croissance du cybersecteur profite à l'ensemble du Royaume-Uni et pas seulement à Londres et au Sud-Est qui, selon les estimations fournissent 45 % des emplois du secteur et bénéficient de 85 % des investissements extérieurs.[22]

65. Globalement, nous jouerons un rôle plus stratégique en facilitant le regroupement des chefs de file de l'industrie, des universitaires, des innovateurs, des services répressifs, de la communauté de la sécurité nationale et de tout intervenant souhaitant collaborer pour donner au Royaume-Uni les moyens d'être plus résilient face aux cybermenaces. Nous alignerons les leviers du gouvernement pour soutenir l'écosystème cyber, de la façon d'enseigner la cybernétique dans les écoles au recours à la réglementation économique contribuant à l'évolution positive des normes, pour veiller à ce que le Royaume-Uni développe les capacités vitales nécessaires pour se protéger contre de futures menaces.

[22] DCMS, Cyber Security Sectoral Analysis 2021 (2021) (Analyse sectorielle du secteur de la cybersécurité)

Objectif 1 : renforcer les structures, partenariats et réseaux nécessaires pour soutenir une approche basée sur la dimension pansociétale de la cybernétique.

66. Le cyberpouvoir exige une approche pansociétale. Notre avantage concurrentiel viendra de notre capacité de cultiver et tirer parti des talents des quatre coins du Royaume-Uni, de recruter des personnes compétentes aptes à appliquer les bonnes méthodes sur l'ensemble du secteur public, de l'industrie et du monde universitaire, dans un effort visant à rassembler toute la communauté cybernétique. Nous devrons former un véritable partenariat d'exécution intégré avec l'industrie et garantir une approche géographique généralisée, couvrant les nations et régions du Royaume-Uni, travaillant en étroite collaboration avec les gouvernements décentralisés d'Irlande du Nord, d'Écosse et du Pays de Galles, saisissant l'opportunité de nivellement par le haut que présente pour nous le cyberpouvoir. À l'horizon 2025, nous serons parvenus aux résultats suivants :

67. Un cyberdialogue national à la fois plus inclusif et stratégique avec l'industrie, le monde universitaire et les citoyens, en établissant un nouveau National Cyber Advisory Board (Conseil consultatif supérieur et national sur la cybernétique) et en consolidant les réseaux déjà puissants de partenariats pour la cybercroissance et la cyberrésilience, ainsi que les centres d'excellence universitaires dédiés à la recherche et à l'éducation liées à la cybersécurité.

68. Cyber-réseaux régionaux plus intégrés et plus efficaces sur l'ensemble du Royaume-Uni, propices à des partenariats plus solides entre le gouvernement, les entités commerciales et le monde universitaire pour favoriser la croissance sectorielle et la résilience des entreprises. Nous travaillerons avec les grappes industrielles régionales du domaine cyber et la Cyber Cluster Collaboration (UKC3) récemment établie au Royaume-Uni, le nombre croissant de centres régionaux de cyberinnovation et de centres de cyberrésilience afin de renforcer les liens entre les entreprises locales, centres d'excellence universitaires et services répressifs.

69. Ces mesures s'appuieront sur l'éventail de relations existantes entre le National Cyber Security Centre (NCSC - Centre national de la cybersécurité) et ses parties prenantes, entre les ministères, les organismes indépendants et les secteurs de l'économie qu'ils représentent, dont l'infrastructure critique nationale et les régulateurs, ainsi que sur le dialogue plus général du gouvernement avec l'industrie, les secteurs du numérique et des technologies.

Ciara Mitchell, Responsable Cyber de l'organe de gestion au service du secteur des technologies numériques ScotlandIS

Ciara est également manager du Cyber Cluster écossais et membre du conseil d'UKC3.

« Le Cyber Cluster écossais a joué un rôle déterminant dans le soutien à la communauté de la cybersécurité écossaise. L'expertise de l'Écosse en matière de gestion des grappes industrielles et l'opportunité d'y tirer parti d'un cybersecteur florissant sont de plus en plus comprises. Dans un contexte où la valeur des grappes industrielles est de plus en plus reconnue, je suis ravie d'avoir assumé un rôle clé dans la nouvelle collaboration des grappes industrielles du domaine cyber britanniques UKC3 en tant que Responsable du développement de l'écosystème. UKC3 mettra davantage l'accent sur la collaboration, l'innovation et le développement des compétences qui constituent une plateforme propice à la croissance du secteur britannique de la cybersécurité. »

Cyberorganisations (emplacements représentatifs)

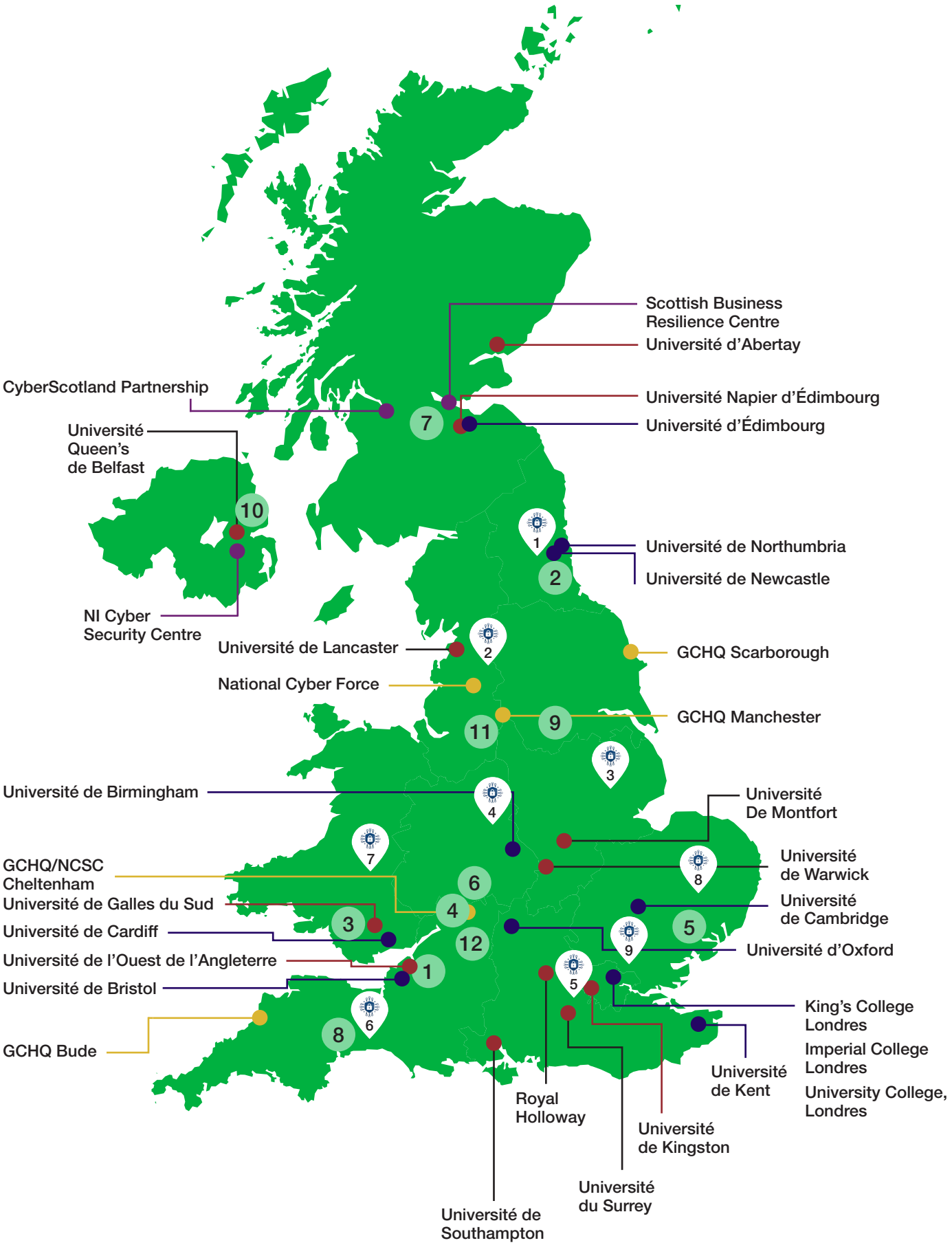
UK Cyber Clusters (Grappes industrielles)

1. Bristol and Bath Cyber
2. Cyber North
3. Cyber Wales
4. CyNam (Cyber Cheltenham)
5. East of England Cyber Security Cluster
6. Midlands Cyber
7. ScotlandIS Cyber
8. South West Cyber Security Cluster
9. Yorkshire Cyber Security Cluster
10. NI Cyber (Irlande du Nord)
11. North West Cyber Security Cluster
12. West of England Cyber Cluster

- Academic Centre of Excellence in Cyber Security Education
- Change Academic Centre of Excellence in Cyber Security Research*
- Site GCHQ/NCSC
- Organisations d'autorité décentralisée

*Le point rouge et la ligne noire correspondent aux statuts CSE (Éducation) et CSR (Recherche)

1. Business Resilience Centre de la région Nord-Est
2. Cyber Resilience Centre de la région Nord-Est
3. Cyber Resilience Centre de la région East Midlands
4. Cyber Resilience Centre de la région West Midlands
5. Cyber Resilience Centre de la région Sud-Est
6. Cyber Resilience Centre de la région Sud-Ouest
7. Cyber Resilience Centre du Pays de Galles
8. Cyber Resilience Centre de la région Est
9. Cyber Resilience Centre, Londres


Scottish Business Resilience Centre
Université d'Abertay
CyberScotland Partnership
Université Napier d'Édimbourg
Université d'Édimbourg
Université Queen's de Belfast
Université de Northumbria
Université de Newcastle
NI Cyber Security Centre
Université de Lancaster
GCHQ Scarborough
National Cyber Force
GCHQ Manchester
Université de Birmingham
Université De Montfort
GCHQ/NCSC Cheltenham
Université de Warwick
Université de Galles du Sud
Université de Cambridge
Université de Cardiff
Université d'Oxford
Université de l'Ouest de l'Angleterre
Université de Bristol
King's College Londres
Imperial College Londres
GCHQ Bude
Université de Kent
University College, Londres
Royal Holloway
Université de Kingston
Université du Surrey
Université de Southampton

Objectif 2 : améliorer et élargir les cybercompétences nationales à tous les niveaux, notamment par le biais d'une cyberprofession de calibre mondial et diversifiée, capable d'inspirer et d'équiper les futurs talents.

70. Pour réaliser ses ambitions, le Royaume-Uni aura à cœur de développer une offre soutenue et diversifiée de personnes hautement qualifiées pour alimenter la demande en cybereffectifs capables de concrétiser les éléments essentiels de l'économie numérique, tout en innovant et développant de nouvelles approches. Elle nous aidera à prêcher par l'exemple en reconnaissant et en retenant l'expertise de l'ensemble du secteur public, à augmenter nos capacités de répression, de défense et de sécurité, National Cyber Force (NCF) incluse. Comme pour d'autres éléments de cette stratégie, nous travaillerons avec les gouvernements décentralisés d'Écosse, du Pays de Galles et d'Irlande du Nord pour veiller à ce qu'une approche cohérente soit adoptée dans tout le pays relativement aux initiatives du gouvernement britannique se rapportant aux questions décentralisées, telles que l'éducation et les compétences. À l'horizon 2025, nous serons parvenus aux résultats suivants :

71. augmentation importante du nombre de personnes disposant des compétences dont elles ont besoin pour s'intégrer aux cybereffectifs nationaux, s'appuyant sur le travail accompli par les quatre nations du Royaume-Uni pour veiller à ce que la politique d'éducation et de compétences réponde aux exigences des personnes et des employeurs. Nous y parviendrons en mettant en œuvre un certain nombre de mesures, dont l'expansion des programmes de formation pour les plus de 16 ans en adéquation avec les besoins des cybereffectifs, le financement d'une gamme de formations « boot camp » sur les compétences en cybersécurité, le déploiement national du programme des instituts de technologie et la poursuite du programme de bourses CyberFirst destiné aux étudiants de premier cycle. Ces mesures s'appuient sur le travail du gouvernement visant à aligner la majeure partie des programmes d'éducation et de formation destinés aux plus de 16 ans sur les normes consolidées jugées nécessaires par les employeurs, à l'horizon 2030. Elles seront développées conjointement avec le Cyber Security Council (Conseil de la cybersécurité) du Royaume-Uni pour la communauté cybernétique au sens large et soutiendront l'apprentissage, les T-Levels et les nouvelles qualifications techniques supérieures. Elles permettront de veiller à que les employeurs jouent un rôle déterminant dans la conception et le développement des qualifications et formations.

72. Une profession de la cybersécurité de meilleure qualité, mieux établie, reconnue et structurée. Le Cyber Security Council du Royaume-Uni établira des normes professionnelles et des voies d'accès à et de poursuite d'une carrière dans le domaine de la cybersécurité étayées par une Charte royale, fondées sur le Cyber Security Body of Knowledge (CyBOK), corpus de connaissances de calibre mondial en matière de cybersécurité. D'autre part, nous examinerons les différents leviers du gouvernement, législation incluse, pour intégrer ces normes à l'ensemble de la profession, en veillant à ce que l'excellence et l'expertise puissent être reconnues clairement et uniformément sur l'ensemble des cybereffectifs.

73. Des cybereffectifs plus diversifiés, au sein desquels les groupes sous-représentés et membres des communautés défavorisées du Royaume-Uni sont mieux soutenus pour se lancer et s'épanouir en faisant carrière dans la cybernétique. Notre gamme de mesures comprendra notamment des mécanismes de soutien pour permettre à un plus grand nombre de femmes de rejoindre les cybereffectifs, ainsi que des interventions ciblées pour aider les groupes sous-représentés à progresser vers les échelons supérieurs. Nous nous appuierons également sur les réussites des activités parascolaires proposées dans le cadre de notre programme phare CyberFirst et notamment du concours CyberFirst Girls. Nous faciliterons également l'accès à l'éducation et aux opportunités de carrière pour les jeunes à risque, grâce au programme Cyber Choices de la National Crime Agency. Le but de ce programme est de les détourner des cyberactivités illégales et de les réorienter vers des opportunités plus positives de tirer parti de leur talent et de leur enthousiasme.

74. Un flot constant et diversifié de personnes hautement qualifiées émanant de notre système éducatif. Nous inciterons et soutiendrons davantage de jeunes à suivre une éducation passant par la filière d'enseignement technologique, notamment en augmentant l'intégration et la diversité des candidats optant pour les GCSE en science informatique et des qualifications équivalentes en Écosse, décidant de poursuivre leurs études jusqu'aux T Levels en Angleterre et de saisir une opportunité d'apprentissage ou d'études supérieures. Nous perfectionnerons un plus grand nombre d'enseignants en Angleterre grâce au National Centre for Computing Education (NCCE - Centre national de formation aux métiers de l'informatique), en veillant à ce qu'ils aient accès aux ressources et opportunités de développement qui les aideront à susciter l'intérêt d'un plus grand nombre d'élèves.

75. Le gouvernement est mieux placé pour repérer, recruter, former et retenir les professionnels de la cybernétique dont il a besoin. Faisant partie des grands employeurs de cyberprofessionnels, le gouvernement et le secteur public devront montrer l'exemple en s'appuyant sur les mesures décrites précédemment et en les renforçant. Nous adopterons une approche plus cohérente et plus efficace sur l'ensemble du secteur public, tout en adaptant des mesures spécifiques pour perfectionner les fonctionnaires, les cadres supérieurs et renforcer nos capacités dans les domaines de la défense et de la sécurité, notamment à travers la NCF, le NCSC et les services répressifs. Il s'agira notamment d'investir dans les jeunes talents en élargissant la filière d'accès rapide aux métiers de la cybernétique Cyber Fast Stream et en multipliant les apprentissages dans le domaine de la cybersécurité, en soutenant les programmes de compétences spécialisées au sein de la NCA, dont les stages pour diplômés et placements de stagiaires, programmes sur mesure liés à la neurodiversité et de diversité estivaux. Elle s'appuiera sur les réussites de la Defence Cyber School en l'intégrant à la Defence Cyber Academy dans le cadre d'un offre élargie de formations à la cybersécurité défensive et offensive, tout en collaborant avec des partenaires universitaires, industriels et internationaux.

UK Cyber Security Council (Conseil de cybersécurité du Royaume-Uni)

Lancé en mars 2021, UK Cyber Security Council est une première mondiale pour les métiers de la cybersécurité. Il a pour mission de servir de porte-parole à la profession, apportant clarté et structure aux cybereffectifs en pleine croissance et à la gamme de qualifications, de certifications et de diplômes proposés dans ce domaine. Il s'agit d'une étape essentielle, sachant que la cyberprofession intègre un large éventail d'expertises et de spécialisations techniques et non techniques sur l'ensemble de l'économie, dont l'envergure rappelle celle de professions plus ancrées comme la médecine et le droit.

Le Conseil vise quatre objectifs :

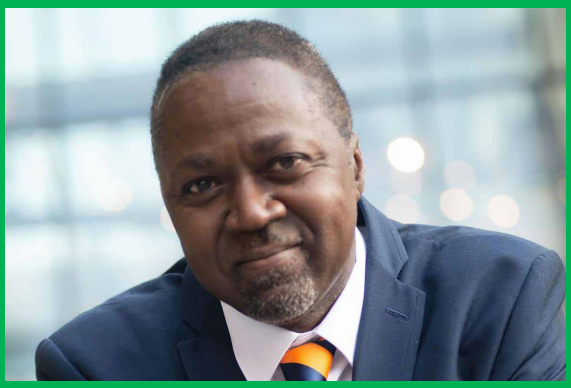
- leadership intellectuel et normes professionnelles : diriger le travail d'élaboration et d'adoption des normes définissant la cybersécurité ;
- carrières et apprentissage : aider les employeurs et les personnes à faire leurs choix de carrière en les conseillant sur les compétences, le perfectionnement professionnel et la reconnaissance liés au secteur de la cybersécurité ;
- éthique professionnelle : fournir les principes directeurs sur la base desquels les professionnels en exercice et les organisations elles-mêmes peuvent montrer leur respect de bonnes pratiques éthiques en matière de cybersécurité ;
- diversité et inclusivité : promouvoir la cybersécurité comme une source d'opportunités de carrière pour les personnes de tous âges et de tous horizons, en s'efforçant d'éliminer les obstacles à l'entrée et à la progression dans ce domaine.

Le Conseil cherchera à augmenter et établir sa crédibilité et sa durabilité en tant qu'autorité professionnelle tout au long du cycle de vie de cette stratégie. Il réunira un éventail d'organismes professionnels et de certification existants, en identifiant et en habilitant les organisations expertes aptes à fournir des précisions sur les conditions de progression et les compétences aux nouveaux entrants, praticiens existants et employeurs.

La Reine a approuvé l'attribution d'une Charte royale au Cyber Security Council du Royaume-Uni en novembre 2021. Première reconnaissance dédiée, agréée spécifiquement pour la cybersécurité, elle couvre l'éventail de spécialités dont se compose ce domaine.

Nous sommes conscients que des efforts restent à faire pour intégrer les normes et parcours professionnels dans l'écosystème cyber en général et plus particulièrement, au sein du gouvernement, des secteurs de la défense et de la répression. Le Conseil jouera un rôle déterminant à cet égard, en aidant les jeunes et les personnes qui changent de métier à négocier leurs carrières liées à la cybernétique.

Simon Hepburn, PDG, UK Cyber Security Council



Je suis chargé de promouvoir le Cyber Security Council, « porte-parole des métiers de la cybersécurité » au Royaume-Uni. Organe d'autoréglementation des métiers de la cybersécurité au Royaume-Uni, le Council entend unir l'industrie pour développer, promouvoir, gérer des normes cybernétiques nationales reconnues et faire du Royaume-Uni l'endroit le plus sûr pour vivre et travailler en ligne. Officiellement lancé en mars 2021 consécutivement à un projet de formation réussi, le Council est désormais prêt à recevoir des demandes d'adhésion. La Cyberstratégie nationale est cruciale pour veiller à ce que le travail des personnes et des organisations fasse progresser la profession, en association avec les principaux acteurs coordinateurs dont le Council fait partie.

Objectif 3 : favoriser la croissance d'un secteur de la cybersécurité et de la sécurité de l'information durable, novateur et concurrentiel à l'échelle internationale, source de produits et de services de qualité répondant aux besoins du gouvernement et de l'ensemble de l'économie.

76. Pour renforcer le cyberpouvoir national tout en stimulant la croissance et les exportations numériques, le Royaume-Uni a besoin d'un cybersecteur dynamique composé d'entreprises de grande qualité, dignes de confiance. Les entreprises du Royaume-Uni fournissent des technologies, formations et conseils de référence mondiale, aux industries et aux gouvernements du Royaume-Uni et du monde entier. Toutefois pour mettre au point des technologies de pointe, certaines entreprises ont besoin de soutien et d'être orientées vers les sources d'investissements nécessaires pour parvenir à l'étape à laquelle elles pourront proposer un produit viable.

77. Les entreprises doivent également être suffisamment sûres d'innover en respectant les limites de paramètres approuvés par le gouvernement et que respectent également leurs concurrents. D'autre part nous pouvons faire davantage pour aider les acheteurs à négocier les méandres d'un paysage complexe, occupé par une vaste gamme de produits et services de qualité variable. Ces actions stimuleront la demande au sein de l'écosystème et favoriseront la poursuite de la croissance. À l'horizon 2025, nous serons parvenus aux résultats suivants :

78. Un cybersecteur ayant enregistré une croissance mondiale en glissement annuel supérieure à la moyenne, notamment grâce au commerce et aux cyberexportations. Nous aiderons les cyberentreprises à accéder à de nouveaux marchés domestiques et à l'étranger en appuyant des cyberévénements phares et de calibre mondial au Royaume-Uni et en invitant nos cyberentreprises les plus novatrices à participer à des missions commerciales et cyberfoires internationales. En outre, nous utiliserons plus efficacement les marchés publics et établirons un répertoire complet de fournisseurs accrédités par le NCSC, pour encourager la demande de produits et de services de cybersécurité de grande qualité.

79. Un cybersecteur encore plus novateur, témoin d'une augmentation considérable des investissements d'amorçage et du nombre de cyberentreprises qui ont pu se lancer, se développer et s'élargir. Notre nouveau programme Cyber Runway donne aux entreprises un point focal de soutien unique tirant parti des enseignements de programmes précédents comme Tech Nation Cyber Programme, Cyber101 et Hut Zero. Nous transformerons le Cheltenham Innovation Centre, qui comprend l'accélérateur cybernétique « NCSC for Startups », en un véritable centre international de l'innovation baptisé National Cyber Innovation Centre. Nous mettrons à profit l'expertise des organisations existantes pour promouvoir et favoriser la co-création, à l'image du partenariat de technologie et d'innovation National Security Technology and Innovation Exchange. Nous encouragerons également les investissements à plus haut risque dans les jeunes start-up spécialisées dans le domaine cyber, notamment par le biais du fonds d'investissement stratégique pour la sécurité nationale National Security Strategic Investment Fund, en partenariat avec la banque de développement économique British Business Bank.

80. Une cyberéconomie britannique considérablement nivelée par le haut, caractérisée par une augmentation de la croissance en dehors de la région Sud-Est, contribuant à la reprise post-pandémie de coronavirus (COVID-19) et favorable à l'activité économique régionale plus générale. Nous établirons le quartier général permanent de la NCF à Samlesbury, dans le Nord-Ouest de l'Angleterre, pour stimuler la croissance dans les secteurs de la technologie, du numérique et de la défense en dehors de Londres et contribuer à la création de nouveaux partenariats dans la région. Nous intensifierons notre soutien aux innovateurs et aux entrepreneurs en dehors de Londres et du Sud-Est pour développer leurs produits et services, favoriser la croissance de leurs entreprises et recruter du personnel qualifié. Dirigé par le conseil d'arrondissement de Cheltenham pour favoriser la croissance des entreprises de technologie en rapport la cybernétique, le campus de Golden Valley aura notamment son rôle à jouer en la matière. Nous augmenterons les capacités d'exportation des cyberentreprises d'un plus grand nombre de régions du Royaume-Uni, en collaborant avec les grappes industrielles cybernétiques régionales et en organisant des événements pour mettre en valeur auprès d'acheteurs internationaux un plus grand nombre de nos talents de la cyberindustrie.

81. Un plus grand nombre d'entreprises sont en mesure de proposer des technologies, produits et services de cybersécurité répondant à des normes de qualité vérifiées de façon indépendante, d'où une augmentation de la confiance des utilisateurs. Nous y parviendrons conformément au livre blanc The Future of NCSC Technology Assurance publié par le NCSC en septembre 2021, en utilisant la marque et l'expertise du NCSC pour créer un marché digne de confiance, dans lequel les consommateurs du Royaume-Uni n'hésiteront pas à acheter des services dans des conditions de sécurité améliorées et de critères de cybersécurité nationale revus à la hausse.[23]

[23] NCSC, White paper: The future of NCSC Technology Assurance (2021) (Livre blanc : l'avenir de l'assurance technologique du NCSC)

Berta Pappenheim, PDG et fondatrice de la société Cyberfish

CyberFish a participé à un programme gouvernemental de cyber-accélérateur. Notre mission consiste à aider les entreprises et les équipes gouvernementales à se préparer pour mieux gérer les interruptions d'activité, en cas de cyberincident par exemple. Dans ce but, nous organisons avec elles des exercices de simulation d'incident, observons la dynamique de leurs équipes en situation de stress et leur expliquons les améliorations possibles. Les conseillers sont souvent très compétents pour traiter l'aspect technique des mécanismes de réponse aux incidents ou le côté comportemental du leadership et de la prise de décisions. Nous les maîtrisons l'un comme l'autre, ensemble, à parts égales de connaissances spécialisées. Nos exercices ont déjà aidé près de 500 chefs de file de l'industrie travaillant au sein d'équipes essentielles à la mission aux quatre coins du monde, à changer leurs perspectives, améliorer leur travail d'équipe et leurs mécanismes de réponse en cas de crise et de prise de décisions.

Vous avez envie de rejoindre les cybereffectifs ou de créer votre propre entreprise ?

82. Notre stratégie précédente accordait une grande importance à la croissance de la base de cybercompétences et du secteur des services de cybersécurité au Royaume-Uni. Comme l'indique le contexte stratégique, nous avons fait d'importants progrès en termes de **développement du secteur et des exportations** :

Aider les cyberentreprises à trouver des marchés internationaux. Le Royaume-Uni a exporté l'équivalent de 4,2 milliards GBP de cyberservices en 2020.

Cyber Exchange, notre cyberportail en ligne, rassemble les cyberentreprises des différentes régions du Royaume-Uni.

Le partenariat pour la cybercroissance Cyber Growth Partnership rassemble le gouvernement et l'industrie pour démanteler les obstacles à la croissance.

83. Nous avons **soutenu des innovateurs pour favoriser le développement et l'élargissement de leurs entreprises**, tout en assurant l'épanouissement de l'écosystème cyber du Royaume-Uni au cours des cinq dernières années :

NCSC for Startups oriente les innovateurs vers les défis stratégiques les plus importants. Ses start-up ont déjà participé à plus de 160 nouveaux essais d'entreprise.

LORCA a aidé 72 cyberinnovateurs à lever plus de 200 millions GBP d'investissements et engranger plus de 37 millions GBP de revenus.

Cyber Runway aide les innovateurs à lancer, développer et élargir leur entreprise, sur la base du succès des programmes Hutzero et Cyber101.

84. Nous nous sommes efforcés de remédier au déficit annuel de 10 000 professionnels **rejoignant les cybereffectifs** :[24]

Le programme de bourses CyberFirst soutient les étudiants du premier cycle et permet chaque année à des centaines de personnes initiées au monde du travail de rejoindre les cybereffectifs.

Il existe désormais quatre standards de cyberapprentissage élaborés par l'industrie. Ils s'ajoutent aux trois offres d'extrants de formation professionnelle initiale dans le même domaine, de l'initiative « Courses for Jobs » mise en place par le ministère de l'Éducation britannique.

Neuf cyber-bootcamps soutenus par le récent National Skills Fund ont déjà été organisés pour faire découvrir aux participants des cybercarrières prometteuses. D'autres sont programmés pour chaque année de la prochaine période de dépenses.

85. Nous avons **professionnalisé les cybereffectifs**, pour permettre aux organisations de déterminer plus facilement les compétences dont elles ont besoin et aux personnes de définir plus aisément ce qu'elles doivent savoir :

UK Cyber Security Council est la première autorité professionnelle mondiale en matière de cybersécurité. Elle a commencé à définir des normes professionnelles claires et cohérentes, sur la base des travaux déjà réalisés par des organes professionnels existants. Le Council cherchera à identifier clairement les qualifications efficaces, parmi la multitude d'options proposées à l'heure actuelle.

Le Cyber Security Body of Knowledge (CyBOK) façonne et étaye l'enseignement et la formation professionnelle au service du cybersecteur.

[24] DCMS, Understanding the cyber security recruitment pool (2021) (Comprendre le vivier de recrutement des métiers de la cybersécurité)

86. Nous travaillons pour **veiller à ce que tout le monde puisse rejoindre les cybereffectifs**, luttant contre les inégalités dans ce secteur où seulement 16 % des postes sont occupés par des femmes et où ces dernières et les minorités ethniques ne se partagent que 3 % des postes de direction.[25]

Les formations CyberFirst et le programme Discovery ont intéressé près de 300 000 jeunes âgés de 11 à 17 ans au cours des cinq dernières années.

La UK Cyber Cluster Collaboration construit des partenariats entre l'industrie, les écoles et les universités pour faire en sorte que les opportunités et l'expertise soient disponibles dans l'ensemble des régions.

Le programme Cyber Choices de la NCA aide les jeunes à faire des choix éclairés et à exploiter leurs cybercompétences de manière légale, les sensibilisant et leur fournissant de meilleures solutions de remplacement sous forme d'apprentissages et de stages professionnels.

[25] HMG, Cyber security skills in the UK labour market (2021) (Compétences de cybersécurité dans le marché du travail du Royaume-Uni)

Axe 2 : Cyber-résilience

Construire un Royaume-Uni numérique résilient et prospère

87. La cybersécurité et la cyberrésilience sont essentielles à la réalisation des objectifs stratégiques plus généraux d'une cyberpuissance comme la nôtre : sans elles, nous ne pouvons pas espérer tirer pleinement parti du potentiel transformationnel des technologies numériques pour rebâtir une société plus performante, plus juste, plus forte et protéger l'avantage stratégique du Royaume-Uni dans et à travers le cyberespace. Nous devons continuer à construire des cyberdéfenses robustes, en prenant les mesures qui s'imposent pour sécuriser les réseaux, informations et actifs numériques du Royaume-Uni à l'échelle nationale, locale et individuelle, tout en les rendant le plus résilient possible pour parer aux incidents.

88. Ce chapitre concerne surtout la cyberrésilience qui, pour être pleinement efficace, devra faire partie d'un effort holistique et pansociétal visant à améliorer la résilience du Royaume-Uni. La prochaine National Resilience Strategy (Stratégie de résilience nationale), engagement clé de la Revue intégrée, définira la substance de l'approche fondamentale en matière de résilience nationale.

89. Des progrès importants ont été réalisés au cours de la dernière décennie pour améliorer notre cyberrésilience, comme l'illustre la création du National Cyber Security Centre (NCSC), la multiplication des sources de conseils, d'orientation et d'autres outils ou encore, la mise en œuvre de législations dont le règlement sur les réseaux et systèmes d'information Network & Information Systems Regulations (NIS Regulations), le Règlement général sur la protection des données (RGPD) et la loi relative à la protection des données Data Protection Act 2018. D'importantes lacunes n'en subsistent pas moins. Les atteintes à la cybersécurité nuisent au gouvernement, aux entreprises, aux organisations et aux particuliers. Un grand nombre d'organisations signalent encore de nombreuses atteintes à la cybersécurité et cyberattaques.

90. Nous nous appuyons sur les fondements de la stratégie précédente, développons notre approche et réorientons notre attention vers la cyberrésilience du Royaume-Uni en mettant l'accent sur les aspects suivants :

- intensifier nos efforts pour que l'Internet soit automatiquement plus sûr, prévenir les attaques, intégrer des protections de base au profit des entreprises, organisations et citoyens britanniques et augmenter le soutien mis à la disposition des personnes les moins bien placées pour se protéger en ligne ;
- définir l'ambition du gouvernement de servir de modèle de bonnes pratiques en matière de cybersécurité ;
- imbriquer la cybersécurité parmi les éléments essentiels des bonnes pratiques commerciales en faisant meilleur usage de la réglementation ainsi que d'autres incitatifs et exploiter la force de nos connaissances des menaces pour bâtir des communautés capables de se défendre ;
- sous-tendre ces différents éléments au moyen de normes, de preuves et de données objectivement mesurables et passer de la collecte de données à l'action consécutive.

91. Le concept de cyberrésilience de cette stratégie se caractérise par trois aspects déterminants. Premièrement, la nature du **risque** doit être comprise. Deuxièmement, une action s'impose pour **sécuriser** les systèmes afin de prévenir et de résister aux cyberattaques. Troisièmement, reconnaissant l'impossibilité d'empêcher toutes les attaques nous devons nous apprêter à devoir les gérer, tout en étant suffisamment **résilients** pour en limiter l'impact au maximum et pouvoir nous en remettre.

92. Notre approche sera adaptée à chaque public et appuyée par des capacités nationales qui nous permettront de traiter les risques systémiques. Les publics que nous cherchons à protéger et à influencer sont les citoyens, les entreprises et les organisations du Royaume-Uni, le gouvernement et le secteur public et ceux dont dépend le fonctionnement de notre infrastructure critique nationale (prestataires de services essentiels de distribution d'eau potable, d'électricité, financiers, de transports et de télécommunications dont nous ne pourrions pas nous passer).

93. Nous nous concentrerons dans un premier temps sur les mesures à prendre pour sécuriser l'environnement numérique pour tous les internautes du Royaume-Uni, prévenir les attaques, intégrer la sécurité de base dans les produits et services et aider les particuliers, les petites entreprises et les organisations à prendre des mesures de base pour améliorer leur cybersécurité. À mesure de notre progression vers les acteurs qui assument une plus grande part de responsabilité et disposent de plus grands moyens pour mettre en place des couches de sécurité et de résilience supplémentaires proportionnelles au risque, nous aboutirons au niveau attendu de protection le plus élevé des principaux services publics et essentiels sur lesquels comptent notre population et notre économie.

94. Il doit s'agir d'un projet partagé entre le gouvernement et tous les secteurs de l'économie et de la société. Il incombe aux conseils d'administration des entreprises et des organisations de gérer leurs propres cyberrisques. Notre but est de définir des attentes claires étayées par un cadre d'incitatifs, de soutien et de réglementation adapté pour favoriser l'amélioration et transférer le fardeau du risque de cybersécurité des utilisateurs finaux vers des acteurs mieux placés pour le gérer.

95. Nous demandons aux ministères, à l'ensemble du secteur public et aux exploitants réglementés des infrastructures critiques nationales qu'ils revoient à la hausse leurs critères et adoptent un comportement plus proactif en matière de gestion des risques. Nous attendons de la part des grandes entreprises et organisations, prestataires de services et de plateformes numériques inclus, qu'elles soient davantage responsables de la protection de leurs systèmes, de leurs services et de leurs clients et qu'elles intègrent cette responsabilité au cœur même des principes d'exploitation de leurs activités. En contrepartie, le gouvernement redoublera d'efforts pour sécuriser l'environnement numérique, traiter les risques systémiques et soutenir au moyen de conseils, d'outils, d'accréditations sur le marché et en développant les compétences propices à l'amélioration.

96. Nos efforts pour promouvoir la cyberrésilience au Royaume-Uni doivent également faire partie de notre engagement international. Compte tenu de l'intensification de la mondialisation des chaînes d'approvisionnement, plateformes informatiques, entreprises multinationales et de l'Internet lui-même, nous ne pouvons pas, isolément, améliorer la cybersécurité du Royaume-Uni. Pour relever ce défi nous devrons continuer à mieux comprendre les rapports entre la cyberrésilience du Royaume-Uni et mondiale, traiter les domaines à haut risque et collaborer avec des partenaires internationaux pour renforcer la résilience favorable à la transformation numérique, à la sécurité et au commerce dans l'intérêt mutuel des parties concernées, conformément au chapitre consacré à l'axe 4 : leadership mondial.


Alléger le fardeau pour tout le monde
Travailler avec les fournisseurs pour mieux protéger les
internautes du Royaume-Uni et intégrer des mécanismes de protection de base aux services en ligne destinés aux citoyens.
Étendre la cyberdéfense active, prévenir et perturber la cybercriminalité et la fraude.
Sensibilisation des citoyens et cyberhygiène.
Des entreprises et organisations plus résilientes
Adoption de normes comme Cyber Essentialset plus grande transparence.
Incitations économiques et surcroît de soutien local.
Meilleure réglementation des domaines ciblés, services numériques et données personnelles inclus.
Des services publics plus résilients
Toutes les organisations gouvernementales résilientes face aux méthodes d'attaque connues d'ici à 2030.
Responsabilisation, normes et assurance indépendante accrues.
Investissement pour traiter l'informatique héritée.
Infrastructure critique nationale plus résiliente.
Résilience face aux méthodes d'attaque communes et protection plus sophistiquée proportionnelle à la posture de risque.
Comprendre et gérer les risques liés à la numérisation et aux nouvelles technologies.

Objectif 1 : améliorer la compréhension des cyberrisques pour favoriser une action plus efficace en matière de cybersécurité et de cyberrésilience.

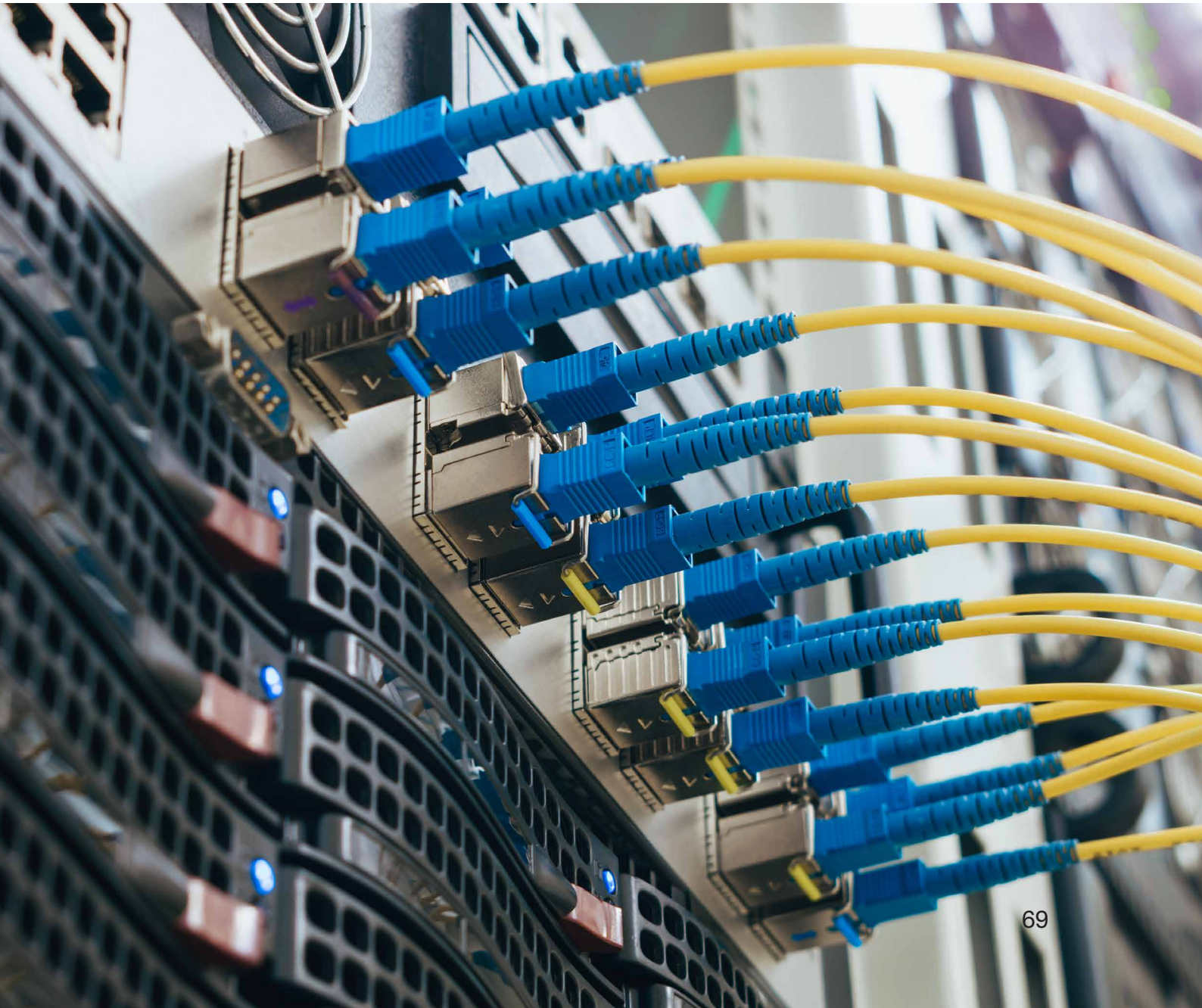
97. Nous mettrons en place un partenariat beaucoup plus rapproché entre le gouvernement, les entreprises et les organisations afin d'améliorer la compréhension collective du risque, d'orienter la priorisation et d'établir les arguments fédérateurs de l'action. Nous appuierons les citoyens en collaborant avec les entreprises et les organisations qui fournissent des services aux consommateurs et continuerons de renforcer la capacité du gouvernement à identifier les risques transversaux. À l'horizon 2025, nous serons parvenus aux résultats suivants :

98. Le gouvernement a acquis une compréhension stratégique actualisée des cyberrisques du pays, dont il se sert pour identifier les risques systémiques, communiquer les priorités, stimuler la stratégie et son exécution. Nous maintiendrons les investissements significatifs décidés dans le cadre de l'ancienne Stratégie nationale de cybersécurité pour « comprendre la menace » et en augmenterons la valeur, tout en consolidant les efforts existants pour comprendre les risques dans un monde de plus en plus interconnecté. Il s'agira notamment de déterminer les points de concentration excessive des chaînes d'approvisionnement numériques et de collaborer avec des partenaires internationaux pour gérer les risques collectifs. Nous améliorerons également nos mécanismes d'enregistrement des infractions à la loi sur l'utilisation abusive des ordinateurs Computer Misuse Act (CMA), en comprenant les liens entre les atteintes à la protection des données et la criminalité en aval et en améliorant notre compréhension de la manière dont les infractions à la CMA facilitent l'exécution d'autres types d'activités criminelles.

99. Le gouvernement prêche par l'exemple dans sa compréhension du cyberrisque. Nous ferons du cadre de cyberévaluation Cyber Assessment Framework (CAF) du NCSC le cadre d'assurance des ministères du gouvernement ; les systèmes critiques et fournisseurs communs seront cartographiés. Nous mettrons sur pied un nouveau centre de coordination de la cybersécurité du gouvernement Government Cyber Coordination Centre (GCCC) et un service pangouvernemental de signalement des vulnérabilités Vulnerability Reporting Service (VRS) pour permettre au gouvernement de « se défendre à l'unisson » dans les scénarios de gestion des incidents, vulnérabilités et menaces. Le VRS s'efforcera d'établir des relations de confiance précieuses avec la communauté des chercheurs en sécurité, pour aboutir à une réduction des vulnérabilités sur l'ensemble du patrimoine du gouvernement. Nous continuerons également de soutenir et coordonner des initiatives similaires au sein des gouvernements décentralisés, comme en témoigne la création proposée d'une fonction de coordination centralisée de la cyberrésilience en Écosse.

100. À l'échelle des infrastructures critiques nationales (CNI) du Royaume-Uni, nous nous efforcerons d'acquérir une compréhension plus sophistiquée des cyberrisques.. Nous intensifierons l'adoption du cadre de cyberévaluation Cyber Assessment Framework (CAF) ou des mécanismes équivalents, tous secteurs des infrastructures critiques nationales confondus et améliorerons la comparabilité avec d'autres cadres d'évaluation et de reporting de cybersécurité utilisés à l'heure actuelle. Nous nous livrerons à des examens de criticité et cartographierons les dépendances des CNI et de leurs chaînes d'approvisionnement. Nous établirons des partenariats plus solides avec les propriétaires et exploitants de CNI afin d'améliorer l'accès aux informations sur les menaces, les risques et de convenir de la posture de risque. Et nous œuvrerons pour comprendre les nouveaux risques ou où de nouveaux CNI apparaissent sous l'effet de la numérisation et de l'émergence de nouvelles technologies, notamment dans le cadre de priorités plus générales comme celle de la transition vers le net zéro.

101. Les entreprises et les organisations du Royaume-Uni comprennent mieux les cyberrisques et leurs responsabilités quant à leur gestion. Nous aiderons les organisations à mieux comprendre le risque pour leurs clients et en particulier, comment les données stockées dans leurs systèmes pourraient servir à faciliter des infractions comme la fraude, le vol d'identité ou l'extorsion. En outre nous partagerons d'autres renseignements tirés de la recherche et des données sur la prévalence, l'incidence des cyberattaques et les progrès relatifs réalisés par les secteurs dans l'amélioration de la cybersécurité.



Objectif 2 : prévenir et résister plus efficacement aux cyberattaques en améliorant la gestion des cyberrisques au sein des organisations britanniques et en protégeant mieux les citoyens.

102. Notre approche vis-à-vis de la prévention et de la résistance aux cyberattaques suppose : (i) que les organisations ont la responsabilité de prendre des mesures pour gérer leurs propres cyberrisques, mais que des cadres de responsabilisation et de bonne gouvernance plus solides sont nécessaires au niveau du conseil d'administration pour en faire une priorité ; (ii) que le gouvernement a un rôle à jouer en collaborant avec l'industrie, pour prendre des mesures visant à réduire directement les risques à l'échelle nécessaire pour traiter les scénarios où il est particulièrement bien placé pour le faire ; (iii) que nous devons veiller à ce qu'un soutien et des conseils soient disponibles pour aider les particuliers, commerçants indépendants, petites entreprises et organisations à gérer leurs cyberrisques. À l'horizon 2025, nous serons parvenus aux résultats suivants :

103. Le gouvernement a réduit le préjudice causé au Royaume-Uni à l'échelle nécessaire et allégé le fardeau porté par les citoyens britanniques. Nous agirons de plus en plus en amont au nom de tous les internautes du Royaume-Uni, en élargissant nos mesures de cyberdéfense active pour soutenir un plus large éventail de secteurs dont les associations caritatives, le monde universitaire, les PME et les citoyens. Nous renforcerons les mesures de protection des services en ligne en augmentant la participation et l'échange d'informations avec l'industrie.

104. Ces travaux s'ajoutent à d'autres priorités gouvernementales visant à protéger les citoyens britanniques en ligne, telles que le projet de loi sur la sécurité en ligne Online Safety Bill et la politique de lutte contre les crimes économiques tels que la fraude.

105. Ils nous obligeront à collaborer plus étroitement avec les secteurs concernés, dont les fournisseurs de services en ligne, les télécommunications, la technologie, les services bancaires et détaillants pour mieux protéger les internautes du Royaume-Uni en : entravant l'enregistrement de sites Web à des fins illégales, augmentant le retrait et le blocage de contenus malveillants en ligne, améliorant la récupération et le retour des informations d'identification volées et la sécurité de l'infrastructure de télécommunications du Royaume-Uni. D'autre part, nous élaborerons des options pour donner un statut juridique à la protection des citoyens dans les cas où les dispositions volontaires s'avèrent insuffisantes.

106. Nos efforts pour réduire les préjudices à l'échelle nécessaire incluront également la lutte contre les risques systémiques de la chaîne d'approvisionnement numérique. Au besoin, nous interviendrons pour promouvoir la diversification de la chaîne d'approvisionnement comme nous le faisons dans le domaine des télécommunications, renforcerons notre sécurité économique collective en améliorant le partage de l'information et en adoptant des approches robustes, prévisibles et proportionnées en matière de filtrage préalable des investissements directs étrangers (IDE) dans les secteurs critiques et en établissant des conditions claires pour les fournisseurs critiques et communs du gouvernement.

107. Les fonctions critiques du gouvernement sont beaucoup plus résistantes aux cyberattaques et toutes les organisations gouvernementales, de l'ensemble du secteur public, seront résilientes face aux vulnérabilités connues et aux méthodes d'attaque d'ici à 2030. Notre but est de faire du secteur public du Royaume-Uni un modèle de meilleures pratiques. Nous publierons la première Government Cyber Security Stragegy (Stratégie de cybersécurité du gouvernement) dédiée dans le cadre de l'effort pour y parvenir. Elle se concentrera sur des processus, une gouvernance et une

responsabilisation plus efficaces en matière de gestion des risques, des capacités développées et employées de manière centralisée (Active Cyber Defence incluse), une surveillance plus complète des systèmes, réseaux et services, l'intervention rapide et proportionnée en cas d'incident, l'investissement dans les compétences, les connaissances et une culture favorisant le changement durable.

108. Les cyberrisques menaçant l'infrastructure critique nationale du Royaume-Uni sont mieux gérés. Par définition, il s'agit des services sur lesquels le pays compte le plus. Nous continuerons de travailler en étroite collaboration avec les exploitants afin de garantir, le plus tôt possible, la résilience des opérations contre les méthodes d'attaque communes et de mettre en place des mesures de protection plus avancées s'il y a lieu. Les opérateurs de services essentiels désignés au titre de la réglementation NIS devront par conséquent, au minimum, satisfaire à la norme de référence établie par les autorités compétentes pertinentes pour chaque secteur.

109. Dans le cadre de l'effort pour y parvenir, nous ferons le point sur la capacité du gouvernement d'obliger les exploitants de CNI à rendre des comptes, pour vérifier qu'ils investissent dans la cybersécurité des systèmes critiques et qu'ils gèrent efficacement leurs risques, notamment au niveau de leurs chaînes d'approvisionnement. Nous renforcerons le cadre réglementaire afin d'en améliorer la portée, les pouvoirs et la capacité d'adaptation, dans le contexte d'un risque plus vaste pour la sécurité nationale, de l'évolution rapide de la menace et de la technologie. Nous commencerons par une consultation sur les réformes du règlement NIS relatif aux réseaux et systèmes d'information, la mise en œuvre du nouveau cadre de sécurité pour les fournisseurs de services de télécommunications du Royaume-Uni et l'élaboration d'un cadre de réglementation proportionnel, pour veiller à ce que le futur système énergétique intelligent et souple dont le Royaume-Uni a besoin pour atteindre le net zéro soit sûr et résilient face aux cybermenaces.

110. Nous améliorerons parallèlement la capacité des régulateurs, investirons dans les compétences pour améliorer la capacité des exploitants de CNI d'attirer, de perfectionner et de retenir les cyberprofessionnels (voir le chapitre consacré à l'écosystème cyber du Royaume-Uni) et aiderons les exploitants à gérer les risques liés à la chaîne d'approvisionnement en intensifiant l'engagement avec les fournisseurs critiques et en étudiant la gamme de leviers possibles, de l'orientation aux propositions législatives et liées à l'approvisionnement.

111. L'infrastructure sur laquelle repose notre utilisation des données est à la fois sécurisée et résiliente. Cette infrastructure est un bien national essentiel. Elle soutient notre économie, sert à l'exécution des services publics et stimule la croissance. Nous jouerons un plus grand rôle pour veiller à ce que les volumes importants de données traités, acheminés ou stockés dans des centres de données externes par exemple, soient suffisamment protégés. Nous établirons un cadre de gestion des risques plus solide pour garantir des normes de sécurité et de résilience plus élevées sur l'ensemble du secteur. Nous mettrons en œuvre les dispositions de la loi relative à la sécurité nationale et aux investissements National Security and Investment 2021, afin de renforcer le filtrage des investissements. Nous renforcerons notre travail avec les partenaires internationaux, pour veiller à ce que la mondialisation croissante de l'accès aux flux de données et leur multiplication n'augmentent pas les risques pour la sécurité auxquels fait face le Royaume-Uni et relever les défis que pose la collecte de données de masse.

112. Nous examinerons également le caractère de plus en plus critique des services d'infrastructure de données du Royaume-Uni comme pilier de l'économie et son rôle dans l'infrastructure critique nationale. Ces mesures sont en phase avec les engagements de la stratégie nationale sur les données National Data Strategy et de la Revue intégrée.

113. Un plus grand nombre d'entreprises et d'organisations britanniques gèrent leurs cyberrisques de manière proactive et prennent des mesures pour améliorer leur résilience. Nous soutiendrons et favoriserons le changement de comportement en élaborant des incitatifs économiques encourageant le recours à une cybersécurité efficace. Au besoin, ces mesures seront complétées par des mesures législatives ciblées. Elles veilleront à ce que les cyberrisques soient gérés efficacement par les instances auxquelles revient la plus grande part de responsabilité dans ce domaine, mais aussi à ce que l'efficacité de la législation du Royaume-Uni en matière de cybersécurité soit préservée compte tenu de l'évolution des risques et des technologies.

114. Dans le cadre de l'effort pour y parvenir, nous intensifierons notre collaboration avec les influenceurs du marché (acheteurs, institutions financières, investisseurs, vérificateurs et assureurs) pour encourager le recours aux bonnes pratiques de cybersécurité sur l'ensemble de l'économie. Nous proposerons des moyens d'améliorer le reporting d'entreprise sur la résilience aux risques, cyberrisques inclus. Ils permettront aux investisseurs et aux actionnaires de mieux comprendre comment les entreprises gèrent et atténuent les risques importants pour leur entreprise. Nous continuerons également de promouvoir l'adoption des accréditations et des normes comme le programme de certification Cyber Essentials, ainsi que l'engagement des conseils d'administration à l'égard de la gestion des cyberrisques.

115. La législation ciblée sera principalement axée sur les secteurs les plus vulnérables à l'impact potentiel d'une cyberattaque, dont les fournisseurs de certains services essentiels et numériques, la protection des données de l'ensemble de l'économie et les plus grandes entreprises. Dans un premier temps, cette mesure s'ajoutera au Plan for Digital Regulation (Plan de réglementation numérique) et mettra l'accent sur la réglementation régissant la sécurité des réseaux et des systèmes d'information (NIS) décrite précédemment et dans le chapitre Technologie, puis sur les prochaines étapes de la réforme du régime britannique de protection des données à caractère personnel.

116. De plus amples détails sur les mesures envisagées pour améliorer la résilience des activités et la cybersécurité pour l'ensemble des entreprises et des organisations du Royaume-Uni, seront présentés dans l'examen de la réglementation et des mesures incitatives en matière de cybersécurité, Cyber Security Regulation and Incentives Review.

117. Les conseils techniques, outils d'auto-assistance, produits et services assurés pour améliorer la cyberrésilience sont faciles à trouver et s'améliorent continuellement, l'accent étant particulièrement mis sur l'aide aux citoyens, aux commerçants indépendants et aux petites organisations. Nous continuerons d'élaborer des directives et des outils d'auto-assistance techniquement précis, opportuns et actionnables par le biais du NCSC. Nous veillerons à ce que les messages soient cohérents, clairs et transmis par les canaux les plus efficaces, que ce soit par l'intermédiaire de la campagne Cyber Aware, du site Web du NCSC, du gouvernement, des réseaux de répression ou des partenariats avec l'industrie et multiplierons nos offres de soutien à l'échelle locale. Dans le cadre du programme « Digital Entitlement » (Droit au numérique), nous continuerons de financer entièrement les compétences numériques essentielles au profit des adultes qui en ont besoin, en veillant à ce que les apprenants acquièrent les compétences numériques de base nécessaires pour surfer de manière sûre et responsable. Nous aiderons les entreprises et les organisations à négocier les méandres du marché complexe de la cybersécurité en élargissant nos cadres de produits et de services assurés et en développant des offres commerciales autour de Cyber Essentials, afin de faciliter l'accès des petites entreprises aux conseils de base.

Elis Power, Responsable cyberprotection et prévention, Tarian Regional Cyber Crime Unit

Tarian Regional Cyber Crime Unit (Cellule régionale Tarian de lutte contre la cybercriminalité) est une équipe pluridisciplinaire composée de policiers et de personnel détachés des forces de police galloises. Ils ont pour mission de contribuer à l'établissement d'un cyberenvironnement plus sûr et plus sécurisé dans le sud du Pays de Galles.

Le responsable cyberprotection et prévention Elis Power fait partie de l'équipe d'engagement :

« C'est un cliché, mais il n'y a pas vraiment de journée type pour notre cellule. De jour en jour, je peux aussi bien être chargé de présenter un exposé contenant des conseils destinés aux services de police internes ou des organisations externes, pour veiller à ce qu'ils comprennent parfaitement comment se protéger eux et leur lieu de travail contre les cybermenaces. Je peux aussi devoir présenter à de jeunes écoliers des sujets allant de la sécurité sur Internet à la loi Computer Misuse Act de 1990, par exemple. J'assiste fréquemment à des réunions avec des organismes et des forces partenaires, pour discuter des nouvelles menaces et des conseils connexes destinés à nos publics. Je collabore également avec les organisations qui nous envoient des alertes de vulnérabilité et participe à des opérations nationales. Il m'arrive de faire partie des invités spéciaux d'événements et de conférences sur mon domaine d'activité et je m'efforce de trouver le temps d'améliorer continuellement mes capacités et ma base de connaissances. »

Objectif 3 : renforcer la résilience aux niveaux national et organisationnel afin de se préparer aux cyberattaques, d'y répondre et de s'en remettre.

118. Les efforts déployés pour comprendre le risque et prendre des mesures préventives n'empêcheront jamais l'occurrence de tous les incidents. Nous devons renforcer les capacités de gestion des incidents et de réponse de toutes les organisations, afin de limiter au maximum les préjudices causés et de mieux soutenir les victimes. À l'horizon 2025, nous serons parvenus aux résultats suivants :

119. La gestion stratégique et la coordination de la réponse du Royaume-Uni en cas de cyberincident d'importance nationale sont encore plus efficaces. Nous nous appuierons sur l'expérience du gouvernement en matière de réponse aux cyberincidents importants, en veillant à ce que les enseignements en découlant servent à améliorer nos politiques et processus. Nous partagerons notre expérience de la gestion de crise avec des partenaires internationaux et l'industrie et, à charge de revanche, déterminerons les pratiques exemplaires d'autres pays pour améliorer nos mécanismes de préparation et processus. Nous veillerons à ce que le NCSC et les équipes répressives de gestion des incidents disposent de l'expertise et des outils nécessaires, pour réagir à la gamme complète de types d'incidents évolutifs et coordonner une réponse nationale aux menaces prioritaires.

120. Les cyberincidents sont plus faciles à signaler et les victimes de cybercriminalité sont mieux soutenues. Les informations de signalement seront également utilisées pour faciliter la prévention de futurs incidents et aider les services répressifs à enquêter sur, perturber et poursuivre les cybercriminels. À cette fin, nous substituerons à Action Fraud un nouveau service national de signalement et d'analyse de la fraude et de la cybercriminalité d'ici à 2025. Nous encouragerons le recours plus systématique au signalement des cyberincidents par d'autres moyens, notamment grâce à un nouveau service de signalement pour les entreprises au sein du service de police métropolitaine City of London Police. Dans les secteurs réglementés, nous permettrons aux régulateurs d'exiger la déclaration d'un plus large éventail d'incidents dont les « quasi-accidents ». Le déploiement de la cellule nationale de soutien aux victimes de la criminalité économique améliorera le soutien et l'orientation proposés aux victimes d'une expérience potentiellement stressante et préjudiciable.

121. Le gouvernement et les CNI sont mieux placés pour répondre aux incidents et s'en remettre, notamment grâce à une meilleure planification des incidents et à des exercices réguliers. Nous aiderons le gouvernement du Royaume-Uni et les exploitants de CNI à trouver sur le marché les services de cyberexercices et de gestion des incidents dont ils ont besoin, en élargissant le programme accrédité de réponse aux cyberincidents du NCSC et en introduisant un nouveau système d'exercices.

122. Au sein du gouvernement, les capacités de surveillance et de détection seront améliorées au niveau des ministères et sur l'ensemble du patrimoine numérique du gouvernement. Nous veillerons à ce que les enseignements soient identifiés et servent à améliorer nos politiques et processus, partagerons notre expérience de la gestion de crise avec nos partenaires internationaux et l'industrie et mettrons tout en œuvre pour que nos équipes de gestion des incidents possèdent l'expertise, l'aptitude et les capacités nécessaires pour répondre aux divers types d'incidents évolutifs.

123. Au sein des CNI, nous établirons des conditions claires relativement aux exercices, aux essais ou aux simulations d'adversaires sur l'ensemble des exploitants de CNI, stimulerons l'innovation et la collaboration en matière de réponse et d'exercices en cas d'incident, tout en envisageant l'application de modèles tels que le centre de collaboration cybernétique du secteur financier Financial Sector Cyber Collaboration Centre. En outre, dans le cadre de nos ambitions en matière de technologie (décrites dans le chapitre suivant), nous établirons un laboratoire national de sécurité des technologies opérationnelles comme centre d'excellence des essais, des exercices et de la formation aux technologies industrielles critiques, afin de renforcer les capacités dans ce domaine en collaboration avec l'industrie, le monde universitaire et nos partenaires internationaux.

124. Les entreprises et organisations britanniques comprennent mieux la marche à suivre en cas d'incident, à qui elles doivent faire appel, qui peut les aider et comment s'en remettre. Nous améliorerons l'accès à la formation et aux exercices, avec l'appui des services assurés de l'industrie et notamment d'un nouveau programme de réponse aux cyberincidents Cyber Incident Response Scheme et d'un service d'exercices de cyberincident Cyber Incident Exercising. Nous veillerons à ce que les victimes de la cybercriminalité puissent accéder à un soutien de répression cohérent et national, tout en encourageant les petites entreprises et les organisations à profiter du soutien local d'organismes comme leur centre régional de cyberrésilience Cyber Resilience Centre.

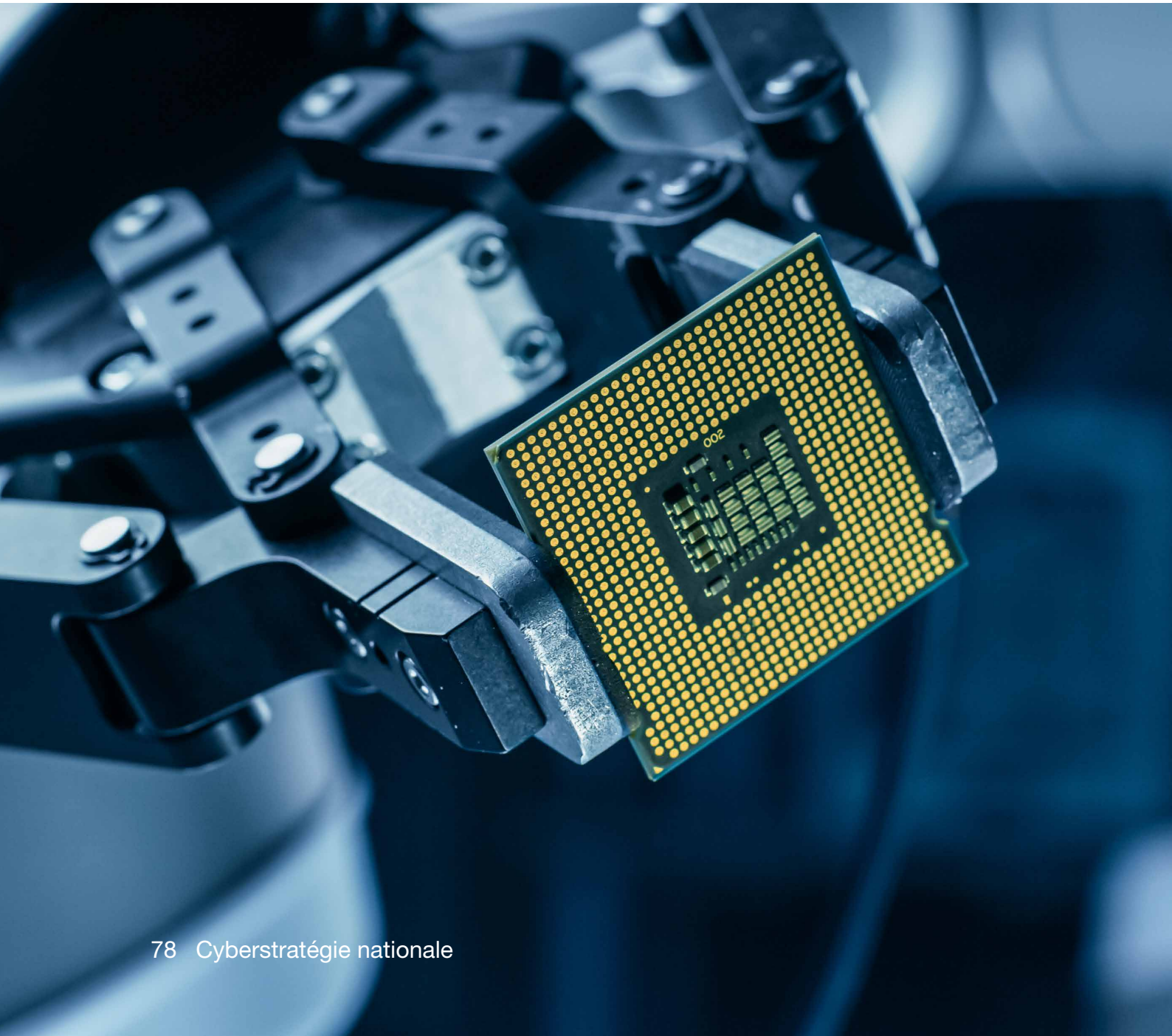
Daniel Ng, PDG de CyberOwl

CyberOwl a bénéficié du programme de cyberdéveloppement proposé par le gouvernement. Nous assurons la surveillance et l'analyse des conditions de cybersécurité des actifs opérationnels, dans les secteurs maritime et infrastructure critique nationale. Exigeant davantage de connectivité et la numérisation des actifs de terrain, l'effort de durabilité environnementale les expose aux cyberrisques. CyberOwl aide les exploitants à identifier et cartographier leurs actifs, à détecter rapidement les cyberrisques afin d'être sûrs de les avoir sécurisés et de montrer aux régulateurs qu'ils ont fait le nécessaire en la matière. Nous travaillons avec les plus grands exploitants d'actifs maritimes de la région EMEA et Asie-Pacifique, pour améliorer la résilience de la chaîne d'approvisionnement mondiale des transports maritimes. En 2021, nous avons multiplié par 14 les réservations et doublé nos opérations au Royaume-Uni et à Singapour.

Jen Ellis, vice-présidente, Affaires communautaires et publiques, Rapid7

Mon travail consiste à échanger avec des professionnels de la sécurité et dirigeants d'organisations, de toutes tailles et tous secteurs confondus, afin de comprendre les défis auxquels ils font face et d'essayer de trouver des solutions pour les aider à améliorer leur cybersécurité. J'entends constamment dire que les organisations sont dépassées, qu'elles ne savent pas où donner de la tête, par où commencer ou comment progresser. Le personnel technique peut aussi avoir beaucoup de mal à susciter l'adhésion des dirigeants. Une stratégie de cybersécurité claire, cohérente et transparente élaborée par le gouvernement peut contribuer à régler ce problème. Elle donne au personnel technique matière à débattre dans le cadre de ses discussions avec les dirigeants. D'autre part, elle identifie les principaux domaines d'intérêt et une voie possible vers la maturité. La cybersécurité est un domaine encore extrêmement complexe, sans fin, mais la vaste stratégie de cybersécurité permet de mieux en cerner l'importance et rappelle que nous sommes tous dans le même bateau.

Axe 3 :
Avantage technologique



Prendre l'initiative par rapport aux technologies essentielles au cyberpouvoir

125. Certaines technologies seront essentielles pour façonner l'avenir du cyberespace. Les pays qui parviennent à établir un rôle de premier plan dans ces technologies seront mieux placés pour influencer la façon dont elles sont conçues et déployées, plus en mesure de protéger leur sécurité et leur avantage économique et d'exploiter plus rapidement les possibilités de percées dans les cybercapacités. La concurrence dans ce domaine s'intensifiera à mesure que la technologie confirme son importance comme outil du pouvoir géopolitique.

126. En tant que cyberpuissance, la poursuite d'un avantage stratégique par la science, la technologie et l'accès aux données dont il dépend sera une condition préalable à la réalisation des objectifs plus généraux du Royaume-Uni. Le gouvernement a pris des mesures dans le cadre de stratégies antérieures pour stimuler la recherche et l'innovation dans les technologies de cybersécurité, notamment au moyen de programmes d'accélérateur de croissance pour les start-up, de centres d'excellence universitaires en recherche sur la cybersécurité et pour encourager l'élaboration d'appareils grand public issus d'une approche « secure by design » (sécurisé de façon native). Quoi qu'il en soit nous avons désormais besoin d'une approche plus ambitieuse et proactive, pour préserver notre intérêt dans les technologies critiques tout en évitant de trop dépendre de nos concurrents et d'être à la merci de nos adversaires.

127. La Revue intégrée a établi des plans pour faire du Royaume-Uni une superpuissance scientifique et technologique en recourant à la science et à la technologie pour construire et maintenir son avantage stratégique. Cette stratégie soutient les travaux du National Science and Technology Council et de l'Office of Science and Technology Strategy dans la poursuite de cet objectif. Elle complète les stratégies du Royaume-Uni dans des domaines comme l'intelligence artificielle ou les technologies et données quantiques.

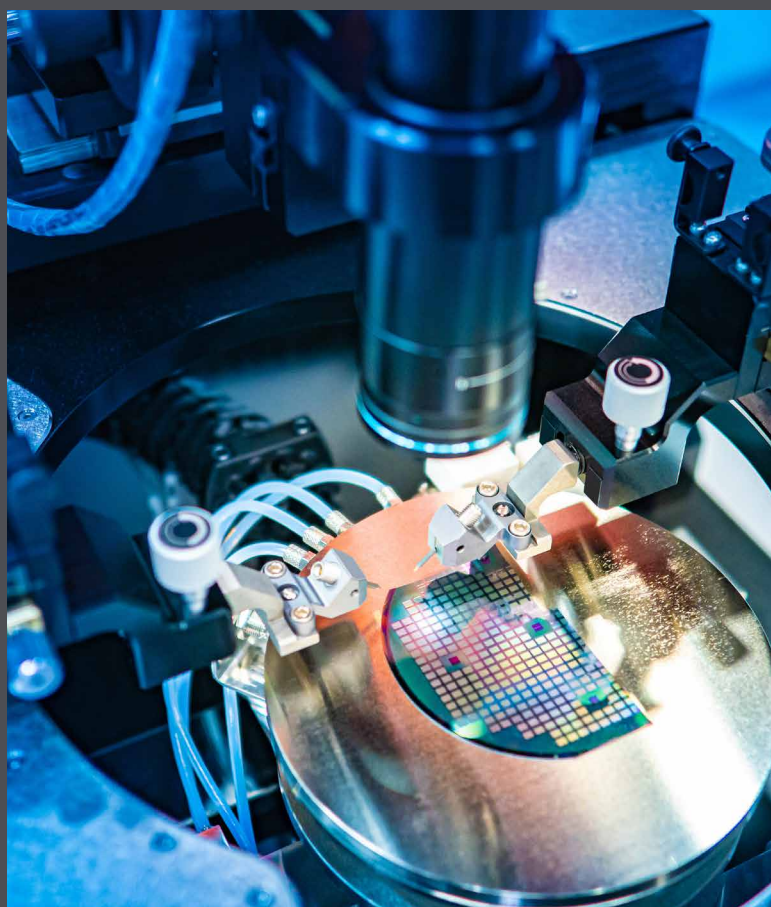
128. Sous l'impulsion de l'expertise technique du National Cyber Security Centre (NCSC) et d'autres organismes gouvernementaux, nous renforcerons notre capacité d'identifier les domaines technologiques les plus essentiels à notre cyberpouvoir. Nous prendrons des décisions stratégiques à l'échelle nationale au sujet des priorités, en nous inspirant du cadre Own-Collaborate-Access décrit dans la Revue intégrée. Dans certains domaines, nous investirons dans les activités de recherche-développement et les partenariats stratégiques nécessaires pour développer les capacités nationales du Royaume-Uni et, dans les cas où nous devons compter sur les marchés mondiaux, travaillerons avec l'industrie, les régulateurs et les partenaires internationaux pour encourager des chaînes d'approvisionnement dignes de confiance et diversifiées, tout en façonnant les normes pour veiller à ce que les technologies soient sûres et ouvertes. En outre, nous renforcerons la capacité du Royaume-Uni d'exploiter et de protéger les volumes croissants de données et d'informations générées par les technologies émergentes et stimulant l'innovation dans ce domaine, en nous appuyant sur le cadre établi dans la National Data Strategy (Stratégie nationale sur les données) pour en maximiser les avantages pour notre économie et notre société.

Technologies essentielles au cyberpouvoir

Diverses technologies existantes et émergentes seront essentielles au cyberpouvoir du Royaume-Uni ; nous devons être en mesure d'anticiper, d'évaluer et d'agir par rapport à ces développements. Nous nous attendons à accorder la priorité à un éventail de technologies et d'applications dont font partie les suivantes, dans le cadre de la mise en œuvre de la stratégie. Cette liste n'a pas pour prétention d'être exhaustive ou statique et nos priorités continueront d'évoluer en consultation avec l'industrie, le monde universitaire et les experts techniques :

- Technologies 5G et 6G, ainsi que d'autres formes émergentes de transmission de données.
- Intelligence artificielle (IA), dont la nécessité de sécuriser les systèmes d'IA et la possibilité d'utiliser l'IA pour améliorer la cybersécurité dans un large éventail d'applications, comme la surveillance des réseaux.
- Technologie blockchain et ses applications telles que les cryptomonnaies et la finance décentralisée.
- Semi-conducteurs, puces de microprocesseurs, architecture de microprocesseur et leur chaîne d'approvisionnement, leur conception et leur procédé de fabrication.
- Authentification cryptographique, notamment pour la gestion de l'identité, des accès et les produits cryptographiques à garantie élevée.
- Internet des objets et technologies utilisées dans les environnements de consommation, d'entreprise, industriels et physiques tels que les villes connectées.
- Technologies quantiques dont l'informatique quantique, la détection quantique et la cryptographie post-quantique.

Ce travail appuiera et s'alignera sur l'exécution d'un certain nombre de stratégies et de résultats à l'échelle du gouvernement, comme la National Data Strategy (Stratégie nationale sur les données), la National AI Strategy (Stratégie nationale sur l'intelligence artificielle) et la Revue intégrée, ainsi que sur les résultats axés sur la technologie se rapportant à cet axe.



Objectif 1 : améliorer notre capacité d'anticiper, d'évaluer et d'agir par rapport aux progrès scientifiques et technologiques les plus essentiels à notre cyberpouvoir.

129. Nous devons, pour construire et maintenir un avantage concurrentiel dans les cybertechnologies, adopter une approche coordonnée, rigoureuse et cohérente qui nous permettra d'identifier et d'analyser les domaines critiques de la science, de la technologie et de prioriser les efforts nationaux. Nous devrons par conséquent continuer à développer notre recherche et notre expertise techniques au sein du gouvernement et du monde universitaire. Nous les intégrerons aux nouvelles structures gouvernementales d'analyse prospective des sciences et de la technologie, tout en tirant parti des connaissances acquises par les experts de l'industrie et de notre réseau à l'étranger pour comprendre les priorités et systèmes des partenaires et concurrents internationaux. À l'horizon 2025, nous serons parvenus aux résultats suivants :

130. Le gouvernement est mieux placé pour analyser les sciences et technologies nouvelles et en développement, mais aussi pour en comprendre les répercussions sur la cyberpolitique et la cyberstratégie du Royaume-Uni. Nous étendrons nos capacités de recherche, notamment par le nouveau centre de recherche appliquée du NCSC à Manchester, en mettant l'accent sur les technologies émergentes dans des domaines comme les villes et transports connectés et en travaillant aux côtés d'experts du Government Office for Science (Bureau du gouvernement pour la science) entre autres. Nous puiserons dans l'expertise de sources externes au gouvernement, en appuyant les quatre Cyber Security Research Institutes (Instituts de recherche sur la cybersécurité) et les dix-neuf Academic Centres of Excellence in Cyber Security Research (Centres d'excellence universitaires en recherche sur la cybersécurité), en finançant les Pathfinder Awards pour les chercheurs dans des sujets prioritaires et en exploitant plus efficacement notre présence à l'étranger et nos partenariats internationaux.

131. Cette meilleure compréhension éclaire plus rapidement et plus efficacement l'analyse prospective élargie, la priorisation et la prise de décisions du gouvernement. Elle nous permet d'adopter une approche plus proactive pour exploiter les opportunités et atténuer les risques. Nous mettrons en place une nouvelle fonction interne d'analyse prospective pour anticiper les progrès scientifiques, technologiques et leurs répercussions sur le domaine cyber. Nous prendrons des décisions mieux éclairées pour prioriser les principales cybertechnologies, en orientant la R&D et l'élaboration de politiques susceptibles de profiter à la sécurité du Royaume-Uni. Elles façonneront s'il y a lieu la prise de décisions plus générales sur les priorités en matière de sciences et de technologie, par l'intermédiaire du Office for Science and Technology Strategy (Bureau de la stratégie scientifique et technologique) et du National Science and Technology Council (Conseil national scientifique et technologique).

Máire O'Neill, Enquêteur principal du Centre for Secure Information Technologies (CSIT)

Le CSIT compte parmi les plus grands centres universitaires de recherche en technologie du Royaume-Uni spécialisé dans la cybersécurité. Dirigé par le Professeur Máire O'Neill, enquêteur principal, il a été choisi en 2009 pour faire partie des premiers centres d'innovation et de connaissances du pays. La réussite du CSIT en termes de recherche, d'innovation et d'engagement de l'industrie contribue depuis dix ans à la croissance considérable de sa réputation, aussi bien sur la scène nationale qu'à l'international. En soutenant les activités d'essaimage, l'expansion des entreprises autochtones et les IDE dans la région, le CSIT a joué un rôle essentiel dans le succès de la grappe industrielle d'Irlande du Nord Northern Ireland Cyber Security Cluster spécialisée dans la cybersécurité. Parti de zéro en 2009, le cybersecteur d'Irlande du Nord emploie aujourd'hui 2 300 personnes dans 104 entreprises et génère une masse salariale annuelle de 110 millions GBP.

Objectif 2 : favoriser et maintenir l'avantage souverain et allié dans le domaine de la sécurité des technologies essentielles au cyberespace.

132. Dans les cas où le Royaume-Uni est susceptible d'établir une position de leader, d'obtenir un avantage concurrentiel dans des domaines clés de la cybertechnologie ou lorsque la dépendance vis-à-vis de sources d'approvisionnement non-alliées pose des risques inacceptables pour la sécurité, nous chercherons à développer notre base industrielle nationale. Nous devrons maintenir une capacité réellement souveraine dans certains domaines. D'autres seront traités en collaborant avec des partenaires internationaux ou en cherchant une position de leader dans un des aspects du marché. Une approche coordonnée s'impose par conséquent, pour stimuler l'innovation et la R&D conjointement avec l'industrie et le monde universitaire. À l'horizon 2025, nous serons parvenus aux résultats suivants :

133. Le Royaume-Uni réussit mieux à traduire la recherche en innovations et en nouvelles entreprises dans les domaines technologiques les plus vitaux pour son cyberpouvoir. Nous aiderons les universitaires du Royaume-Uni à commercialiser et opérationnaliser leurs recherches, en adoptant une approche plus axée sur les défis en collaboration avec des partenaires de l'industrie. Elle permettra d'identifier les idées les plus prometteuses et de stimuler les investissements des bailleurs de fonds. Par ailleurs, nous nous appuierons sur l'approche définie dans l'Innovation Strategy (Stratégie d'innovation), en soutenant le développement d'écosystèmes plus établis autour des technologies clés et en veillant à ce que l'avantage du Royaume-Uni soit plus robuste et difficile à copier.

134. Le Royaume-Uni a consolidé sa place de chef de file mondial de la conception de microprocesseurs sécurisés.[26] Nous nous appuierons sur le programme Digital Security by Design (Sécurité numérique native), lequel a mis au point une nouvelle technologie de puces informatiques plus sûres pour protéger les logiciels contre les vulnérabilités. Nous mettrons cette expérience à profit sur les processeurs d'intelligence artificielle, pour donner aux fournisseurs britanniques un avantage international. Nous travaillerons avec le programme national de technologies quantiques National Quantum Technologies Programme, pour concevoir un modèle de sécurité pour les ordinateurs quantiques et veiller à ce que les entreprises britanniques comptent parmi les chefs de file mondiaux de cette technologie.

135. Le Royaume-Uni est considéré comme un leader mondial dans la recherche sur la sécurité des technologies opérationnelles, des systèmes de contrôle-commande industriels critiques et dans sa capacité à les tester et à les exercer au Royaume-Uni. Nous établirons un laboratoire national pour la sécurité des technologies opérationnelles en partenariat avec l'industrie et le monde universitaire. Il accueillera des programmes de recherche de calibre mondial et fournira aux partenaires du gouvernement, militaires, de l'industrie et internationaux les installations nécessaires pour soumettre ces technologies aux tests et exercices ici-même, au Royaume-Uni. Et comme le confirme la 5G Telecoms Supply Chain Diversification Strategy (Stratégie de diversification de la chaîne d'approvisionnement des télécommunications au standard 5G), nous mettrons sur pied le UK Telecoms Lab réunissant le gouvernement, le régulateur et l'industrie pour appuyer le nouveau cadre de sécurité des télécommunications et contribuer à augmenter la diversité des fournisseurs d'équipement de télécommunications, au sein de la chaîne d'approvisionnement du Royaume-Uni.[27]

136. Le gouvernement est mieux placé pour protéger l'innovation et la propriété intellectuelle du Royaume-Uni dans les cybertechnologies critiques contre les activités hostiles, contribuant au maintien de notre avantage concurrentiel.[28] Nous investirons dans les ressources et l'expertise nécessaires pour concrétiser notre leadership technique lié à la sécurité de ces technologies au fil de leur développement, notamment en conseillant sur les risques liés à l'investissement étranger direct en adéquation avec les objectifs de la loi National Security and Investment Act 2021 relative à la sécurité nationale et à l'investissement. Et nous poursuivrons notre travail avec les entreprises et les universités, pour créer un environnement éprouvé dans les domaines clés de la recherche et du développement, tout en élaborant des mesures robustes pour prévenir le vol de données et de propriété intellectuelle.

[26] Les microprocesseurs sont les cerveaux de nombreux appareils utilisés à l'heure actuelle. Ils sont omniprésents, notamment dans des domaines cruciaux comme les télécommunications, la défense, les soins de santé et sur l'ensemble de nos grandes industries. Les progrès technologiques dans la conception des systèmes sont actuellement freinés par les préoccupations en matière de sécurité et de sûreté, amplifiées par la complexité croissante des systèmes.

[27] DCMS, 5G Supply Chain Diversification Strategy (2020) (Stratégie de diversification de la chaîne d'approvisionnement des télécommunications au standard 5G)

[28] En mettant tout particulièrement l'accent sur les secteurs inclus dans la loi National Security and Investment Act 2021 : robotique de pointe, intelligence artificielle, communications, matériel informatique, authentification cryptographique et technologies quantiques.

Digital Security by Design (Sécurité numérique native)

Soixante-dix pour cent des vulnérabilités actuelles de cybersécurité exploitent une faille connue depuis les années 1970 dans la conception des microprocesseurs. Tous les appareils numériques, des téléviseurs aux appareils de télécommunication, sont dotés de microprocesseurs. Le gouvernement collabore avec le secteur de la technologie pour régler ce problème et d'ici à 2025, un nouveau concept de microprocesseur sera disponible pour les smartphones et une liste croissante d'autres appareils.

Modifier la conception des microprocesseurs nécessite des partenariats et des investissements mondiaux. Sur l'impulsion directrice du Royaume-Uni et grâce à un investissement de 70 millions GBP du gouvernement, la sécurité en cours d'intégration à la phase de conception des futurs appareils réduira considérablement le risque de réussite des cyberattaques.

Cette technologie révolutionnaire a été recherchée et développée au Royaume-Uni. Des leaders technologiques comme Microsoft, Google et d'autres investissent pour doter leurs produits de ces nouveaux avantages de sécurité. Des chercheurs des universités du Royaume-Uni s'efforcent de trouver de nouvelles façons de mieux utiliser cette technologie sécurisée. Le gouvernement aide les PME britanniques à trouver de nouveaux marchés pour vendre les produits dotés de cette nouvelle sécurité.

Phil Wilson, Directeur R&D de The Hut Group

The Hut Group est une société de commerce électronique spécialisée dans la distribution de produits de grande consommation. Nous disposons de plus de 200 sites Web fonctionnant sur une plate-forme commune et chargés de traiter jusqu'à 3 000 commandes par minute. La sécurité de notre plate-forme et de nos clients est donc pour nous une priorité absolue. Comme nous déployons d'énormes efforts pour être sûrs de pouvoir maîtriser n'importe quelle cyberattaque, nous avons hâte de pouvoir utiliser la technologie Digital Security by Design (DSbD) sur nos systèmes. Exécuter nos systèmes sur ces nouveaux microprocesseurs issus d'un partenariat de 180 millions GBP entre le gouvernement et l'industrie rendrait nos systèmes plus résilients. La gestion de cette transition n'en est pas moins complexe, dans la mesure où nous ne pouvons pas adopter une nouvelle technologie qui ne répondrait pas à nos exigences de performance. Nous sommes fiers d'avoir eu le privilège d'être le premier projet de démonstration du programme DSbD et espérons bénéficier très prochainement de cette nouvelle sécurité sur tous nos systèmes.

Objectif 2a : préserver des capacités cryptographiques « Crypt- Key » nationales robustes et résilientes répondant aux besoins des clients du gouvernement britannique, de ses partenaires et de ses alliés et ayant adéquatement atténué nos risques les plus importants, dont la menace de nos adversaires les plus compétents.

137. Le terme « Crypt-Key » évoque l'utilisation par le Royaume-Uni de la cryptographie pour protéger l'information et les services critiques sur lesquels comptent le gouvernement, l'armée et la communauté de sécurité nationale du Royaume-Uni, notamment pour lutter contre les attaques de nos adversaires les plus compétents. Elle sous-tend notre capacité de choisir la façon dont nous déployons nos capacités de sécurité nationale et de défense. Pour faire partie des chefs de file mondiaux du chiffrement Crypt-Key, notre gouvernement et le secteur privé doivent disposer des compétences et technologies qui conviennent.

138. Nous continuerons d'investir dans nos capacités au sein du gouvernement et de travailler avec notre industrie nationale de la Crypt-Key, pour veiller à ce que le Royaume-Uni continue de faire partie des rares pays capables de développer la Crypt-Key souveraine de demain. Nous continuerons également d'exercer un leadership mondial en matière de Crypt-Key, notamment en soutenant l'OTAN en tant que fournisseur de matériel clé. Ce leadership apportera également des avantages de deuxième ordre, en entretenant une industrie hautement qualifiée au Royaume-Uni et en préservant nos atouts en matière d'ingénierie très résiliente, tout en présentant la possibilité de favoriser de nouvelles capacités robustes pour d'autres contextes à garantie élevée et notamment, pour l'infrastructure critique nationale. À l'horizon 2025, nous serons parvenus aux résultats suivants :

139. Un projet de chiffrement Crypt-Key britannique plus résilient et plus sécurisé, doté d'une base industrielle plus durable et de calibre mondial, fournissant la gamme complète de solutions dont le Royaume-Uni a besoin et les exportant vers des partenaires et alliés choisis. Nous combinerons plus efficacement les capacités et l'expertise du gouvernement et de l'industrie, tout en adoptant une approche nationale plus rigoureuse pour gérer l'entreprise. Elle nous permettra de développer les compétences distinctes et spécialisées dont nous avons besoin.

140. Le Royaume-Uni dispose de capacités et de services Crypt-Key plus solides au sein du gouvernement, capables de répondre à ses besoins évolutifs, à ceux de ses alliés et lui permettant de rester à l'avant-garde du développement du chiffrement Crypt-Key. Nous assurerons un leadership technique solide pour comprendre les besoins des utilisateurs et améliorer nos services de base, notamment en fournissant du matériel clé et la garantie des produits et systèmes. D'autre part, nous transformerons les services Crypt-Key en tirant parti des nouvelles technologies pour les rendre plus souples et invisibles.

141. Le Royaume-Uni a amélioré son leadership mondial par rapport à la technologie Crypt-Key et augmenté ses exportations vers ses partenaires et alliés. Nous maintiendrons notre rôle de leader au sein du Groupe des cinq « Five Eyes », de l'OTAN et d'autres partenariats internationaux et façonnerons l'élaboration de normes reconnues à l'échelle internationale pour assurer l'interopérabilité des solutions Crypt-Key du Royaume-Uni. Et nous travaillerons avec l'industrie pour maximiser les opportunités d'exportation.

Objectif 3 : sécuriser la prochaine génération de technologies connectées, en atténuant les risques de cybersécurité liés à la dépendance à l'égard des marchés mondiaux et en veillant à ce que les utilisateurs britanniques aient accès à un approvisionnement fiable et diversifié.

142. Au cours de la prochaine décennie, nous constaterons une intégration de plus en plus générale de la puissance de calcul, de la connectivité Internet et de l'automatisation dans notre environnement, dans les objets physiques et l'infrastructure certes, mais aussi à long terme, dans les humains eux-mêmes. Cette intégration élargira la portée du cyberespace et augmentera considérablement le volume de données générées. Le fonctionnement sécurisé de notre économie dépendra de plus en plus de la capacité de gérer les données sans risque.

143. Nous devons veiller à ce que, dans la mesure du possible, la prochaine génération de technologies connectées soit conçue, développée et déployée en tenant compte des impératifs de sécurité, de résilience et dans le cadre d'un effort concerté visant à adopter une approche « Secure by design » (Sécurisé de façon native). Le caractère mondial des chaînes d'approvisionnement technologiques nous oblige à recourir à tous les leviers disponibles pour gérer plus activement les risques liés à la dépendance technologique. Dans la mesure du possible, nous nous efforcerons de veiller à ce que la sécurité soit intégrée. Quand cette intégration n'est pas possible, nous mettrons en œuvre des mesures robustes comme la réglementation nationale et la collaboration internationale en matière de normes pour atténuer les risques. À l'horizon 2025, nous serons parvenus aux résultats suivants :

144. Les produits de consommation connectables vendus au Royaume-Uni répondent aux normes de cybersécurité essentielles. Nous introduirons et mettrons en œuvre le Product Security and Telecommunications Infrastructure Bill (Projet de loi sur la sécurité des produits et l'infrastructure de télécommunications), afin de pouvoir exiger l'application de normes de sécurité minimales relativement à tous les nouveaux produits de consommation connectables vendus au Royaume-Uni.
Nous appuierons une transition cybersécuritaire vers un système énergétique intelligent et souple, points de recharge pour véhicules électriques et appareils électroménagers intelligents inclus.
Nous collaborerons avec les organismes de normalisation, l'industrie et des partenaires internationaux pour influencer le consensus mondial sur les normes techniques.
Nous aiderons les organisations du Royaume-Uni à acquérir, déployer et gérer les appareils connectés de manière plus sécurisée, notamment au moyen de nouvelles directives de sécurité pour les appareils connectés d'entreprise.

145. Les principaux fournisseurs de services numériques, Cloud, logiciels, services gérés et magasins d'applications inclus, doivent appliquer de meilleures normes de cybersécurité pour contribuer à la protection des organisations et consommateurs contre les cybermenaces.
Nous consoliderons et élargirons les mécanismes de réglementation des fournisseurs de services numériques et renforcerons la capacité de l'Office du commissaire à l'information (ICO) de veiller à ce que les fournisseurs de services numériques gèrent de manière plus proactive les risques associés à leurs services.
Nous poursuivrons notre collaboration avec l'industrie, grandes sociétés technologiques incluses, pour tirer parti de leur expertise du marché et veiller à ce que tout le monde joue un rôle dans la sécurisation des chaînes d'approvisionnement numériques du Royaume-Uni. Et nous prendrons l'initiative de l'activité de développement de solutions de politique internationale axées sur les fournisseurs numériques.

146. Le Royaume-Uni est à l'avant-garde de l'adoption sûre et durable de la technologie des villes connectées au profit des citoyens et des entreprises. Parfois appelées « villes intelligentes » ou en anglais « smart cities », les villes connectées présentent un certain potentiel d'apport d'avantages tangibles à la société : gestion de la circulation, réduction de la pollution ou réalisation d'économie d'argent et de ressources. Toutefois l'interconnectivité qui permet aux villes de fonctionner plus efficacement est aussi à l'origine de cyber vulnérabilités et d'un risque de cyberattaques. Nous nous appuierons sur les principes de sécurité du NCSC applicables aux villes connectées, afin de réduire les risques pour les entreprises, l'infrastructure, le secteur public et les citoyens.[29] Nous renforcerons la capacité des autorités et organisations locales comme les ports, les universités et les hôpitaux, d'acheter et d'utiliser la technologie des villes connectées en toute sécurité. Et nous établirons un consensus international vis-à-vis d'une approche cohérente et efficace pour traiter la sécurité des villes connectées.

147. La cybersécurité est intégrée de façon native à d'autres technologies émergentes déployées au Royaume-Uni. Nous identifierons les applications technologiques nouvelles et émergentes susceptibles de compromettre la cybersécurité des systèmes et veillerons à ce que le Royaume-Uni soit à l'avant-garde du développement sûr et sécurisé de ces technologies. Dans le cadre de la réflexion du gouvernement quant aux moyens de donner au Royaume-Uni l'accès à la technologie du jumeau numérique et à l'« infrastructure cyberphysique » généralisée, nous veillerons à ce que la cybersécurité soit au cœur du processus décisionnel.[30] Et nous déploierons un système d'assurance pour faire en sorte que le Royaume-Uni occupe une position de choix par rapport à un large éventail de déploiements de véhicules connectés et automatisés.[31]

[29] NCSC, Connected Places Cyber Security Principles (2021) (Principes de cybersécurité des villes connectées)
[30] Annoncé dans la Stratégie de l'innovation (2021)
[31] Connected and Automated Vehicles Process for Assuring Safety and Security (CAVPASS - Processus automobile connecté et automatisé pour garantir la sûreté et la sécurité)

Shadi A. Razak, Directeur des techniques informatiques (CTO), co-fondateur d'Angoka

Les directives sur les villes connectées sécurisées publiées par le gouvernement et l'utilisation croissante de véhicules autonomes soulignent l'importance de la sécurité dans notre société. Angoka est fière de faire partie des anciens bénéficiaires du programme Cyber Accelerator du NCSC. Nous fournissons des solutions valables pour un large éventail d'applications liées à l'infrastructure critique nationale, à la mobilité terrestre et aérienne entre autres, garantissant leur résilience de bout en bout et leur sécurité.

La société s'est donnée pour mission d'assurer la sécurité et la résilience des villes intelligentes ainsi que la mobilité, aspects dont la complexité augmente et qui dépendent de plus en plus des réseaux d'appareils connectés et de la communication intermachines. Notre solution permet de créer des zones de confiance opérant une sécurité décentralisée, résistante aux attaques d'ordinateurs quantiques, mise à jour dynamiquement pour fournir une cible mobile aux attaquants. Les propriétaires d'appareils sont alors entièrement maîtres de leur sécurité.

L'équipe d'Angoka présente sa solution

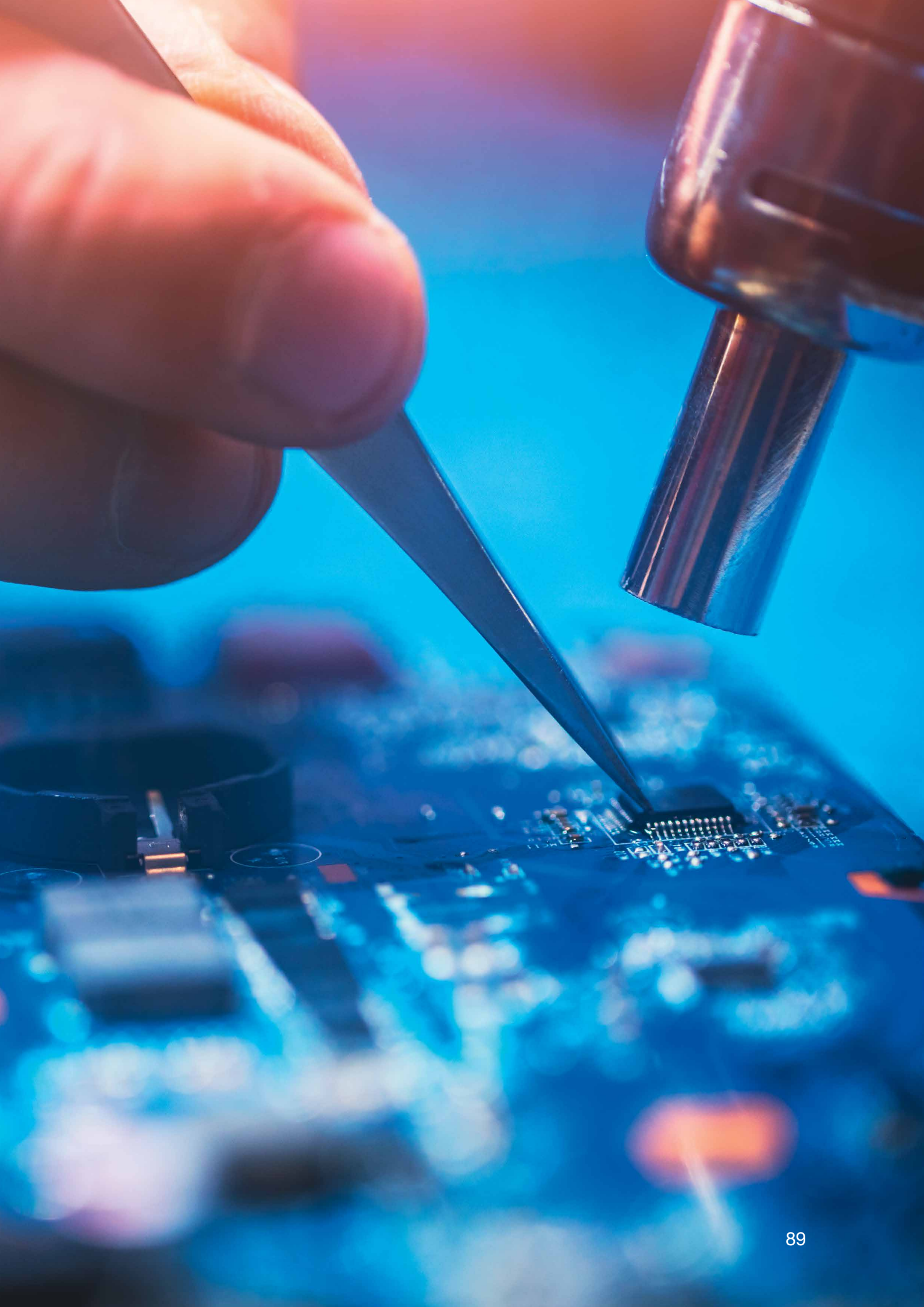
Objectif 4 : œuvrer avec la communauté multi-parties prenantes, pour façonner l'élaboration de normes techniques numériques mondiales dans les domaines prioritaires qui comptent le plus pour préserver nos valeurs démocratiques, garantir notre cybersécurité et favoriser l'évolution des intérêts stratégiques du Royaume-Uni à travers la science et la technologie.

148. Les normes techniques numériques mondiales jouent un rôle fondamental dans le fonctionnement de l'Internet, des réseaux de télécommunications et des technologies émergentes. La façon dont elles sont élaborées et déployées peut avoir une incidence sur nos objectifs de cybersécurité, notre prospérité économique, nos normes et nos valeurs. Historiquement, ces normes étaient façonnées par les acteurs les plus puissants du marché. Des barrières à l'entrée substantielles font entrave à la participation de certaines parties prenantes importantes, comme les PME, les universitaires et d'autres experts. À l'horizon 2025, nous serons parvenus aux résultats suivants :

149. Participation multi-parties prenantes plus engagée dans l'écosystème mondial des normes techniques numériques. Nous renforcerons la participation multi-parties prenantes aux principales organisations d'élaboration de normes et prêcherons par l'exemple avec nos délégations auprès de l'Union internationale des télécommunications (UIT). Nous favoriserons des discussions ouvertes sur les principales tendances et considérations des décideurs, par le biais du Forum sur la gouvernance de l'Internet des Nations Unies et d'autres forums. Nous renforcerons la coordination et le partage d'informations avec les partenaires internationaux, notamment par le biais du Digital Technical Standards Points of Contact Group (Groupe points de contact sur les normes techniques numériques), mis en place pendant la présidence britannique du G7.

150. Les normes techniques numériques mondiales dans les domaines prioritaires pour le Royaume-Uni sont façonnées plus efficacement par les valeurs démocratiques, les considérations de cybersécurité, la recherche et l'innovation britanniques dans les technologies émergentes. Nous collaborerons avec l'industrie, le monde universitaire, des experts techniques et la société civile dans des domaines comme les protocoles Internet, les futurs réseaux et l'intelligence artificielle (IA), dans une optique de sensibilisation aux questions de politique publique importantes pour le développement de normes techniques. Nous mettrons à l'essai un centre des normes d'intelligence artificielle pour appuyer l'engagement mondial du Royaume-Uni en la matière, conformément à la stratégie nationale relative à l'IA.

151. Ces aspects seront étayés par des mécanismes de coordination stratégique au Royaume-Uni, à l'exemple de l'initiative énoncée dans la stratégie nationale relative à l'IA entre le gouvernement, la British Standards Institution (BSI) et le National Physical Laboratory. Cet engagement favorisera également la prospérité du Royaume-Uni en promouvant des normes propices à l'innovation, facilitant la croissance et le nivellement par le haut.



Axe 4 : leadership mondial

Promouvoir le leadership et l'influence du Royaume-Uni sur la scène internationale pour un ordre international sûr et prospère.

152. Notre sécurité et notre prospérité collectives continuent de dépendre d'un cyberespace libre, ouvert, pacifique et sûr. L'engagement international continuera d'être essentiel à la réalisation des différents objectifs de la cyberstratégie du Royaume-Uni. Quoi qu'il en soit, pour répondre à une ère de concurrence systémique, le Royaume-Uni jouera un rôle de leadership international plus activiste afin de promouvoir nos intérêts et nos valeurs dans le cyberespace. L'activité du Royaume-Uni dans le cyberespace et notre expertise dans ce domaine se positionneront également au cœur de l'exécution du programme plus général de politique étrangère du gouvernement : nous les utiliserons de façon proactive pour favoriser la concrétisation d'un ordre international ouvert, sûr et prospère.

153. Nous renforcerons nos alliances de base, tout en travaillant avec un plus large éventail de partenaires et en particulier avec l'industrie, les organismes mondiaux de normalisation technique, la société civile et le monde universitaire en tant que pays orienté vers la résolution des problèmes et le partage des fardeaux. Nous investirons dans des relations plus étroites avec nos partenaires africains et de la région Indopacifique et saisirons les occasions de créer de nouvelles alliances plus agiles. Nous continuerons également d'améliorer notre boîte à outils diplomatiques, en joignant notre influence à l'étranger à nos forces nationales, en tirant parti de notre expertise des communications opérationnelle et stratégique, de nos programmes de compétences et de nos partenariats économiques en tant que force mondiale pour le bien. Nous adoptons cette approche dans l'intérêt de la sécurité et de la prospérité mondiales et non pas uniquement de celles de notre pays.

Objectif 1 : renforcer la cybersécurité et la cyberrésilience des partenaires internationaux et accroître l'action collective pour perturber et dissuader nos adversaires.

154. L'action collective et la résilience mutuelle sont essentielles pour contrer les menaces en amont, tout en réduisant les perspectives de gains susceptibles d'inciter les auteurs de cybermenaces à orienter leurs attaques vers le Royaume-Uni et ses partenaires. À l'horizon 2025, nous serons parvenus au résultat suivant :

155. Les partenaires internationaux du Royaume-Uni disposeront de capacités, d'une volonté politique, de mécanismes de gouvernance et de systèmes plus solides pour enquêter sur les cybermenaces, les perturber et pour consolider leur résilience. Il en découlera une réduction de la menace d'origine étrangère ciblant les citoyens du Royaume-Uni. Nous prioriserons notre aide au renforcement des cybercapacités en Europe de l'Est, en Afrique et dans la région Indopacifique et continuerons de travailler avec nos principaux alliés du Moyen-Orient et d'Amérique. Nous développerons une offre technique plus intégrée et pangouvernementale, en augmentant la part d'investissement dans la répression et l'expertise en matière de défense, en mettant à contribution plus systématiquement l'industrie et le monde universitaire du Royaume-Uni. Nous nous concentrerons sur la protection des chaînes d'approvisionnement et de l'infrastructure internationales critiques, la promotion de l'utilisation sécurisée des technologies numériques et la collaboration avec nos partenaires de l'industrie pour le faire à l'échelle nécessaire.

156. Nous redoublerons d'effort pour renforcer les capacités des organisations de la société civile, en favorisant le débat axé sur les valeurs autour de la technologie et de la société et en créant des mécanismes locaux de responsabilisation. Nous continuerons de travailler avec des organisations et partenariats multilatéraux efficaces, dont les Nations Unies, le Groupe des cinq « Five Eyes », l'OTAN, le G7, l'Union européenne, le Commonwealth, l'OCDE, le Forum mondial sur la cyber expertise (GFCE), le Forum de l'ASEAN, l'Union africaine et la Banque mondiale.

157. Afin de mieux protéger les intérêts et citoyens du Royaume-Uni à l'étranger, nous élaborerons et lancerons également une campagne internationale de cyberhygiène pour les missions du Royaume-Uni à l'étranger, sur mesure et mise en œuvre sur place dans les pays concernés. Elle aura pour but d'augmenter le coût d'activités malveillantes telles que le piratage, le vol de données et d'IP et les rançongiciels. La campagne sera menée par l'intermédiaire de nos diplomates, de notre personnel en mission sur place, de la communauté d'affaires britannique locale et des exécutants des programmes de développement du Royaume-Uni.

158. Une alliance internationale élargie, disposée à imposer des conséquences plus significatives aux adversaires du Royaume-Uni et capable de le faire. Nous améliorerons la détermination et les capacités internationales en intensifiant l'engagement diplomatique, la collaboration opérationnelle, l'échange d'informations et grâce à des exercices conjoints. Emprunter les voies politique, opérationnelle et de répression nous permettra d'augmenter l'impact de mesures comme les cybersanctions ciblées et d'identifier de nouveaux outils pour augmenter le coût des cybermalveillances pour les auteurs de cybermenaces. Nous renforcerons la compréhension mutuelle entre les cyberforces de nos principaux pays alliés et partenaires et intégrerons mieux les cyberopérations dans les opérations alliées tous domaines confondus : terre, mer, air, espace et cyberespace.

159. Nous continuerons de soutenir le développement des capacités de cybersécurité de l'OTAN pour en renforcer l'action collective, notamment en soutenant les processus d'intégration dans les opérations et les missions de l'OTAN des cybereffets souverains fournis volontairement par le Royaume-Uni et d'autres alliés.

Objectif 2 : façonner la gouvernance mondiale pour promouvoir un cyberespace libre, ouvert, pacifique et sécurisé.

160. Les États qui ne partagent pas les valeurs du Royaume-Uni exploitent les défis associés à un Internet libre et ouvert pour imposer leur interprétation autoritaire du cyberespace, en prétextant des raisons de sécurité. Le Royaume-Uni adoptera une approche plus proactive, collaborant avec ses alliés et partenaires pour veiller à ce que les règles et cadres internationaux se développent conformément à nos valeurs démocratiques communes. Nous entendons soutenir la croissance économique nationale et mondiale, améliorer la sécurité collective, encourager l'utilisation responsable de cyberoutils offensifs et veiller à ce que les cybermalveillances et autres activités irresponsables aient de vraies conséquences pour leurs auteurs. À l'horizon 2025, nous serons parvenus aux résultats suivants :

161. La gouvernance globale du cyberspace et de l'Internet protège les intérêts et les valeurs du Royaume-Uni, ce dernier et nos partenaires influençant davantage le développement et la mise en œuvre des cadres internationaux de gouvernance et normatifs. Nous emploierons des méthodes plus progressives et proactives pour façonner les cadres régissant le cyberespace, afin de promouvoir la croissance économique et la sécurité mondiales. Nous concevrons et proposerons des mesures pratiques qui débloqueront le débat international sur l'application des règles, des normes et des principes dans le cyberespace et l'orienterons vers un consensus sur les contraintes effectives visant à faire barrage aux activités destructrices et déstabilisatrices. Nous y parviendrons par le biais d'organisations régionales et spécialisées clés dont l'organisation OSCE, l'association ASEAN, le forum GFCE et participerons de façon constructive au processus des Nations Unies pour élaborer un nouveau traité international sur la cybercriminalité s'inscrivant dans le cadre de la Convention de Budapest, en veillant à ce qu'il renforce la coopération internationale et préserve les mécanismes de protection des droits humains.

162. Nous continuerons également de promouvoir la Convention de Budapest sur la cybercriminalité, collaborant avec des partenaires internationaux pour présenter des arguments susceptibles de convaincre du besoin de continuer à la considérer comme le principal accord international de coopération. Nous continuerons également de promouvoir et d'améliorer les processus multi-parties prenantes de gouvernance de l'Internet, dont la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) et le Forum sur la gouvernance de l'Internet (FGI). Ces efforts seront complétés par notre travail visant à façonner les normes techniques numériques mondiales (décrites dans le chapitre sur la technologie) et développer les exportations de cybersécurité du Royaume-Uni (voir ci-dessous), lesquelles contribueront également à l'intégration des normes du Royaume-Uni dans les écosystèmes cyber d'autres pays.

163. La plupart des pays « intermédiaires » soutiennent et promeuvent la vision du cyberespace et de l'avenir de l'Internet avancée par le Royaume-Uni, considérée comme un moyen plus efficace de contrer l'influence des États autoritaires sur le système multi-parties prenantes. Nous montrerons qu'il est possible de relever les défis dans le cyberespace sans adopter des approches autoritaires et tout en favorisant l'innovation, le développement et la croissance. Nous aiderons les pays aux prises avec la numérisation à développer toutes les facettes de l'expertise juridique et stratégique des communications dont ils ont besoin pour participer au débat international et mettre en œuvre les cadres convenus. Nous continuerons de dénoncer l'utilisation irresponsable des cybercapacités, renforçant la confiance à l'échelle internationale. Et nous continuerons de faire preuve d'ouverture et de transparence dans notre utilisation des cybercapacités offensives partout où nous le pouvons, pour renforcer la réputation du Royaume-Uni en tant que force pour le bien.

Objectif 3 : tirer parti des cybercapacités et de l'expertise du Royaume-Uni et les exporter pour accroître notre avantage stratégique, promouvoir notre politique étrangère plus générale et les intérêts propices à notre prospérité.

164. En réponse à la concurrence systémique et à l'évolution rapide des technologies, la cyberactivité et les cybercapacités du Royaume-Uni seront prises en compte parallèlement à d'autres sources de puissance nationale, pour renforcer notre avantage stratégique, promouvoir nos objectifs en matière de politique étrangère et de prospérité. Notre objectif est de parvenir à un ordre international dans lequel les sociétés et les économies ouvertes peuvent prospérer et où les droits de l'humain sont défendus, tout en favorisant la prospérité de notre pays. À l'horizon 2025, nous serons parvenus aux résultats suivants :

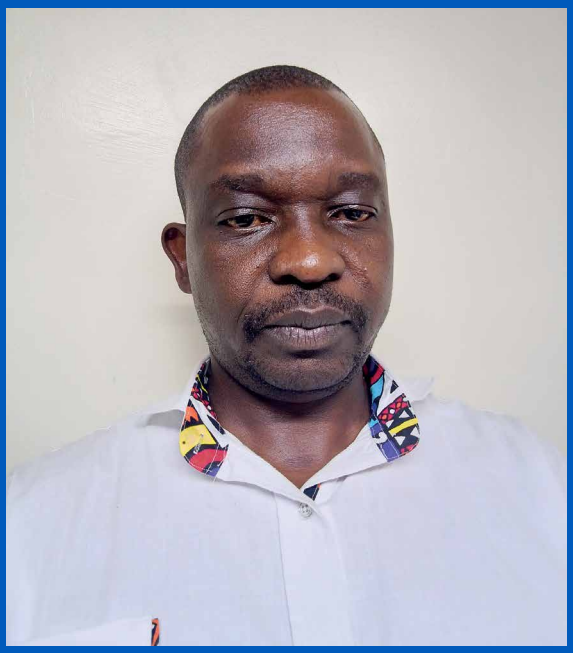
165. Nos activités dans et par rapport au cyberespace ont amélioré la stabilité mondiale et protégé le système international fondé sur des règles, les sociétés ouvertes et les systèmes démocratiques où ils sont compromis. Nous lancerons une campagne internationale axée sur les valeurs pour promouvoir les droits de l'humain, la diversité et l'égalité des sexes dans la conception, le développement et l'utilisation du cyberespace. Il s'agira notamment, mais pas exclusivement, de lutter contre les fermetures d'Internet, les biais algorithmiques en intelligence artificielle et d'améliorer la sécurité en ligne. Nous redoublerons nos efforts pour protéger les valeurs, systèmes et processus démocratiques tout en renforçant le système international fondé sur des règles (dont les Nations Unies, l'Organisation mondiale de la santé et le régime de commerce mondial sont des composantes) en investissant davantage dans notre réseau de Cyber Officers (Délégués à la cybersécurité) couvrant six continents. Nous améliorerons notre utilisation des communications stratégiques pour promouvoir la collaboration du Royaume-Uni dans le domaine de la recherche et les programmes d'échanges universitaires. Nous veillerons à ce que les idées du Royaume-Uni aboutissent à des applications pratiques.

166. Le Royaume-Uni compte parmi les trois principaux exportateurs mondiaux de cybersolutions et de cyberexpertise. Notre cyberindustrie est considérée comme le fournisseur incontournable de solutions de cybersécurité aux gouvernements étrangers et grands clients commerciaux. Nous mettrons en valeur le meilleur de la cybersécurité du Royaume-Uni grâce à un engagement international plus actif de gouvernement à gouvernement, sous les auspices du UK Cyber Security Ambassador Programme (Programme des ambassadeurs de la cybersécurité du Royaume-Uni) et de notre réseau international. Nous aiderons les entreprises du Royaume-Uni à chaque étape du parcours entre l'innovation et l'exportation, à devenir des exportateurs compétents, attirer des investissements entrants et soutiendrons davantage les PME, notamment par l'intermédiaire d'une nouvelle faculté d'exportation Export Faculty.[32] [33] Parallèlement à notre travail dans le cadre du partenariat pour la cybercroissance Cyber Growth Partnership et d'autres efforts décrits dans le chapitre sur l'écosystème cyber du Royaume-Uni, nous créerons également un nouveau bureau de campagne sur les cybercapacités ou Cyber Capability Campaign Office, chargé de fournir un soutien plus structuré et plus coordonné aux grandes campagnes d'exportation.

[32] Décrite dans UK Innovation Strategy (2021) (Stratégie d'innovation du Royaume-Uni)

[33] L'Export Faculty des services de conseil et d'assistance pratique UK Defence & Security Exports (UKDSE) est un centre d'apprentissage et de perfectionnement en ligne. S'adressant aux PME du secteur de la défense et de la sécurité, il propose des modules élaborés spécifiquement pour les entreprises de cybersécurité. L'inscription à cette faculté donne accès à une série de modules d'apprentissage organisés en programme, ainsi qu'à des informations précieuses sur les événements et activités programmés de UK Defence and Security Exports.

Charles Juma, UK Digital Access Programme (Programme d'accès numérique) à Nairobi



Je m'appelle Charles Wesonga Juma. Je suis chargé de diriger, façonner et réaliser les volets cybersécurité, développement numérique, inclusion et entrepreneuriat du programme mondial et pangouvernemental Digital Access Programme (DAP) entrepris au Kenya par le Royaume-Uni. Je participe également à des projets complémentaires dans le cadre du cyberportefeuille du Conflict, Stability and Security Fund (CSSF - Fonds pour la résolution des conflits, la stabilité et la sécurité). On ne saurait trop insister sur l'importance de la sécurité en ligne, de la protection des données et de l'utilisation responsable du cyberespace. Comme nous l'a appris la pandémie de COVID-19, la sécurité et l'hygiène en ligne peuvent être aussi importantes que la santé et l'hygiène publiques. J'ai à cœur de veiller à ce que tout le monde soit protégé contre les menaces et les préjudices en ligne dans le cadre du cyberpouvoir global du gouvernement du Royaume-Uni.

Sara Merchant, Cyber Officer à l'Ambassade britannique de Tbilisi

Je m'appelle Sara et j'occupe un poste de Cyber Officer à l'Ambassade britannique de Tbilisi dans le cadre d'une coopération rapprochée avec le gouvernement géorgien et NCSC UK. Mon travail quotidien varie de l'engagement politique au soutien à la mise en œuvre de la nouvelle cyberstratégie, en passant par le recours à des spécialistes du Royaume-Uni pour renforcer la capacité technique de la Géorgie. J'estime que j'ai beaucoup de chance d'être au premier plan de la projection de l'expertise du Royaume-Uni et d'aider la Géorgie à renforcer sa résilience face aux cybermenaces.
La Géorgie ayant malheureusement eu maintes occasions d'être aux premières lignes d'activités étatiques hostiles, elle a beaucoup à nous enseigner dans ce domaine. Grâce à notre travail, nous sommes à la fois plus forts, plus résilients et mieux informés.

Axe 5 : lutter contre les menaces

Détecter, perturber et dissuader nos adversaires afin d'améliorer la sécurité du Royaume-Uni dans et à travers le cyberespace.

167. La menace à laquelle nous sommes confrontés est intrinsèquement complexe. Nous sommes préoccupés par les menaces qui pèsent sur le cyberespace (sur nos activités en ligne, par exemple), sur le Royaume-Uni et ses partenaires à travers le cyberespace (notamment sur les infrastructures critiques nationales en réseau du Royaume-Uni) et sur le fonctionnement de la cyberinfrastructure internationale porteuse. Chacune de ces menaces peut avoir une incidence sur la disponibilité des services sur lesquels comptent les personnes, sur la confidentialité ou l'intégrité des données et informations acheminées par ces systèmes. Comme nous avons déjà pu le constater en lisant ce document, notre approche pour lutter contre la menace est fondamentalement basée sur la promotion de la cyberrésilience. Ce chapitre porte sur la façon dont nous augmenterons les coûts et les risques liés aux attaques contre le Royaume-Uni dans le cyberespace et maximiserons notre potentiel de cyberpuissance.

168. Depuis la Stratégie nationale de cybersécurité 2016-2021, nous avons transformé notre approche en matière d'atténuation de la menace. Nous avons établi des capacités de calibre mondial de détection et d'analyse des cybermenaces dans le cadre du centre national de la cybersécurité National Cyber Security Centre (NCSC). Le NCSC collabore avec des partenaires des secteurs public et privé, sur le territoire national et à l'étranger, pour détecter les menaces, les incidents et y répondre. En tant que membre de la communauté élargie du renseignement, le NCSC a également pu informer les décideurs relativement à l'attribution des attaques portées contre les intérêts du Royaume-Uni. Ce type de renseignement fait partie des éléments essentiels de nos mécanismes de dissuasion des cybermenaces. Nous avons beaucoup investi dans nos cybercapacités offensives, à travers le cyberprogramme d'offensive nationale National Offensive Cyber Programme d'une part et de l'autre, plus récemment, dans la création de la cyberforce nationale National Cyber Force (NCF). Par ailleurs, nous avons créé une réponse répressive intégrée dirigée par l'agence nationale de lutte contre la criminalité National Crime Agency (NCA) et cherché à perturber et augmenter le coût des activités criminelles et hostiles dans le cyberespace. Nous avons créé des capacités de détection et d'évaluation des menaces de calibre mondial, capables de traduire les connaissances résultantes en mesures d'atténuation efficaces sur l'ensemble des secteurs public et privé. Nous avons également développé un régime autonome de cybersanctions, qui s'ajoute aux leviers servant à imposer des coûts aux acteurs hostiles. Conjointement, notre engagement diplomatique, le NCSC, nos services de sécurité et de renseignement, la NCA, la répression plus générale et la NCF ont réduit l'impact réel des menaces, en prenant des mesures pour contrer directement les adversaires, contribuer à la prévention des attaques et réduire les préjudices.

169. Quoi qu'il en soit les niveaux de sophistication, de complexité et de gravité des menaces ont aussi augmenté et nos efforts ne sont pas encore parvenus à fondamentalement modifier le calcul du risque par les attaquants, qui continuent de cibler avec succès le Royaume-Uni et ses intérêts. Les cyberattaques contre le Royaume-Uni sont motivées par l'espionnage, les gains criminels, commerciaux, financiers et politiques, le sabotage et la désinformation. Les attaquants développent des capacités qui échappent aux mesures d'atténuation. Des cyberoutils de plus en plus sophistiqués et des activateurs connexes ont été banalisés dans une industrie en pleine croissance, réduisant les obstacles à l'entrée pour toutes sortes d'acteurs malveillants. Qui plus est, les gains consécutifs augmentent à mesure que la capacité des acteurs de voler et de chiffrer des données précieuses, d'extorquer des paiements par rançongiciel continue de croître, perturbant les entreprises et principaux services publics. Bilan : les attaqueurs en tirent des gains financiers de plus en plus conséquents, exploitent la vie privée et la liberté d'expression et tentent de manipuler les événements par la désinformation.

170. Le Royaume-Uni passera donc désormais à une base de campagne plus intégrée, plus soutenue, impliquant une utilisation systématique, intégrée et créative de l'ensemble des leviers et des capacités disponibles, pour imposer des coûts à nos adversaires, poursuivre et perturber les auteurs et empêcher de futures attaques. Les principaux éléments porteurs de cette approche sont les suivants :

- développement continu de la NCF comme prochaine étape de la capacité du Royaume-Uni à mener des cyberopérations offensives contre ses adversaires ;
- campagnes pangouvernementales sur mesure pour contrer les menaces pesant sur le Royaume-Uni, tirant parti de nos outils diplomatiques, militaires, de renseignement, de répression, économiques, juridiques et de communication stratégique ;
- nouveaux investissements pour permettre aux services répressifs de mener des enquêtes à l'échelle nécessaire, à un rythme soutenu et de conserver un avantage technique sur nos adversaires afin de prévenir et détecter les criminels dangereux, ainsi que les services habilitants sur lesquels ils comptent ;
- étape importante du partage des données entre le gouvernement et l'industrie, comme l'explique le chapitre sur la résilience.

171. Le cyberespace présente des opportunités pour le Royaume-Uni. Il crée de nouvelles façons pour nous de poursuivre activement nos intérêts nationaux. Par exemple, les cyberopérations offensives nous font bénéficier d'une gamme de mesures flexibles, évolutives et de désescalade susceptibles d'aider le Royaume-Uni à maintenir son avantage stratégique et à réaliser ses priorités nationales, par des moyens qui souvent évitent d'exposer les personnes au risque de préjudice physique.

172. Nous continuerons de développer et d'investir dans nos cybercapacités offensives, à travers la NCF. La NCF transformera la capacité du Royaume-Uni de lutter contre ses adversaires dans le cyberespace et dans le monde réel, afin de protéger le pays, ses habitants et notre mode de vie. Ces capacités seront utilisées de façon responsable, comme une force pour le bien, parallèlement aux leviers du pouvoir diplomatiques, économiques, de la justice pénale et militaires. Elles serviront à appuyer et à faire progresser un large éventail de priorités gouvernementales liées à la sécurité nationale, au bien-être économique, à la prévention et à la détection des crimes graves.

Objectif 1 : détecter, enquêter et partager des informations sur les cyberacteurs et cyberactivités malveillants étatiques, criminels et autres afin de protéger le Royaume-Uni, ses intérêts et ses citoyens.

173. À l'horizon 2025, nous serons parvenus aux résultats suivants :

174. Le gouvernement est tout à fait conscient des cybercapacités des acteurs malveillants étatiques, criminels et autres, ainsi que de leur intention stratégique à l'égard du Royaume-Uni. Nous maintiendrons et augmenterons les investissements considérables de la stratégie de 2016 dans les services de renseignement et répressifs pour comprendre la cybermenace. En particulier, nous augmenterons la capacité des services répressifs de comprendre et de lutter contre la menace de cybercrime et notamment, ses rapports avec les menaces étatiques, les autres menaces nationales et internationales ainsi qu'avec ses catalyseurs technologiques afin d'élaborer des réponses politiques plus efficaces. Nous améliorerons la façon dont nous coordonnons la détection des menaces à l'échelle du gouvernement, grâce à une stratégie conjointe d'accès aux et d'exploitation des données sur l'ensemble des services de renseignement et répressifs. Par ailleurs nous ferons encore plus d'efforts pour comprendre l'intention et les critères décisionnels de nos adversaires, mais aussi l'incidence de nos activités sur leurs actions pour déterminer, entre autres, comment une personne devient cybercriminelle et quelles mesures nous pourrions prendre pour que cela ne se produise pas.

175. Notre travail visant à accélérer et simplifier le processus de signalement des cyberincidents et cybercrimes décrit dans le chapitre sur la résilience, nous aidera également à atteindre ce résultat.

176. Les menaces étatiques, criminelles et autres les plus graves font l'objet d'enquêtes régulières et exhaustives, s'appuyant sur les différentes sources d'information et rassemblant l'expertise du gouvernement, des services répressifs et du secteur privé. Nous renforcerons les capacités de renseignement, opérationnelles et techniques du cyberréseau de répression du Royaume-Uni. Nous investirons dans la capacité de cyberrenseignement dont se sert la NCA pour cibler les groupes du crime organisé, dans l'initiative de renforcement du renseignement régional qui améliorera l'accès et la circulation du renseignement sur l'ensemble du Royaume-Uni, ainsi que dans les compétences et capacités dont ont besoin les services répressifs pour enquêter sur la cybercriminalité, la criminalité numérique et les perturber.

177. Les enquêtes seront appuyées par des renseignements provenant des différentes sources. Elles tireront parti des compétences et connaissances de l'ensemble du secteur privé, notamment en aidant les entreprises à partager plus facilement les données avec les services répressifs. Et nous continuerons de mettre en œuvre les recommandations du HMICFRS sur l'intervention policière en matière de cybercrime, pour veiller à ce que le réseau de cybercrime aux niveaux national, régional et local se maintienne sur des bases stables.[34]

[34] Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (Organe britannique d'inspection des services de police, d'incendie et de sauvetage)

178. L'information et les données sur la menace sont régulièrement partagées à l'échelle nécessaire, à un rythme soutenu et ceux qui les reçoivent sont mieux placés pour agir. Le NCSC a mis à l'essai diverses initiatives visant à créer des communautés plus efficaces de défenseurs des réseaux dans un large éventail de secteurs, qui non seulement reçoivent et sont en mesure de partager l'information sur les menaces, mais sont aussi de plus en plus capables de l'utiliser pour le bien commun. Nous élargirons ce travail, en mettant l'accent dans un premier temps sur le besoin d'aider le gouvernement à mieux se défendre, avec l'appui du centre de cybercoordination du gouvernement Government Cyber Coordination Centre (décrit dans le chapitre consacré à la résilience). Le Financial Sector Cyber Collaboration Centre montre déjà la voie dans le secteur privé.[35]

179. Le NCSC étudie également des moyens de suivre les menaces émergentes et continue de travailler avec l'Alan Turing Institute pour déterminer si l'apprentissage automatique pourrait servir à détecter certains types de cyberattaques. Cette recherche nous permettra de mieux comprendre comment nous pourrions exploiter l'intelligence artificielle pour détecter les activités malveillantes.

[35] NCSC, Financial sector cyber collaboration centre (FSCCC) (2021) (Centre de cybercollaboration du secteur financier)

Mettre fin aux cybercrimes signifie également s'attaquer à d'autres types d'activités criminelles.

Un cybercrime (défini comme une infraction à la loi Computer Misuse Act) se produit en cas d'accès non autorisé à des ordinateurs, réseaux, données et à d'autres appareils numériques, d'acte connexe causant des dommages, de fabrication ou de fourniture d'outils pour commettre ces infractions. Il peut permettre aux cybercriminels de commettre d'autres cybermalveillances, telles que des attaques par rançongiciel, l'accès non autorisé à un compte, le vol de propriété intellectuelle, les attaques par déni de service ou le vol de grands jeux de données à caractère personnel, infractions importantes et dont la fréquence est en hausse.

Pour les citoyens, les cybercrimes donnent souvent lieu à d'autres infractions qu'ils rendent possibles et facilitent. L'accès non autorisé à un ordinateur peut mener à un large éventail de fraudes, de vols, de sextorsion et, dans certains cas, faciliter le harcèlement, la violence familiale et la persécution. Quotidiennement, ces infractions causent des dommages importants aux citoyens britanniques, détruisant des entreprises et ruinant des vies. Les cybercrimes sont donc distincts et différents des problèmes de sécurité en ligne plus vastes, comme l'intimidation et le harcèlement, les discours haineux, la propagation de la désinformation, la promotion de la culture et de la violence des gangs ou l'accès des mineurs à la pornographie. Le gouvernement traite ces problèmes au moyen du livre blanc sur les préjudices en ligne et du projet de loi sur la sécurité en ligne.

Objectif 2 : dissuader et perturber les cyberacteurs et cyberactivités malveillants étatiques, criminels et autres menaçant le Royaume-Uni, ses intérêts et ses citoyens.

180. À l'horizon 2025, nous serons parvenus aux résultats suivants :

181. Il est plus onéreux et plus risqué pour les cyberacteurs malveillants étatiques, criminels et autres de cibler le Royaume-Uni. Nous mettrons en œuvre des campagnes de dissuasion soutenues et adaptées tirant parti de la gamme complète de capacités du Royaume-Uni (dont les leviers diplomatiques, économiques, secrets et manifestes) pour influencer le comportement des cyberacteurs malveillants et criminels. En particulier, nous améliorerons la manière dont nous signalons à nos adversaires notre capacité et notre volonté d'imposer des coûts significatifs, y compris par les sanctions, la répression et les opérations de la cyberforce nationale (NCF). Et grâce au programme Cyber Choices de la NCA, nous éloignerons de la cybercriminalité les personnes, en travaillant avec l'industrie et le monde universitaire pour proposer aux contrevenants potentiels des solutions de remplacement plus attractives comme les apprentissages et stages d'initiation en entreprise.

182. En outre, nous fournirons les outils et les pouvoirs dont les services répressifs et de renseignement ont besoin par le biais du projet de loi contre les menaces étatiques Counter State Threats Bill, en mettant à jour la législation existante et en introduisant de nouvelles infractions tenant compte de l'évolution des menaces provenant des États. Nous modifierons la loi sur les produits du crime Proceeds of Crime Act 2002, afin d'optimiser la capacité des services répressifs d'identifier, de saisir et de récupérer les produits de la cybercriminalité. En particulier, nous créerons un pouvoir de confiscation civile pour atténuer les risques posés par ceux qui ne peuvent être poursuivis.

183. Nos efforts perturbateurs et de dénigrement de leurs activités et capacités ont diminué la capacité des cyberacteurs malveillants étatiques, criminels et autres de cibler le Royaume-Uni. Nous placerons la révision de la politique et de l'approche opérationnelle du gouvernement en matière de lutte contre les rançongiciels parmi nos campagnes prioritaires, en collaborant avec l'industrie et nos partenaires internationaux. Nous maximiserons les partenariats entre la NCF, le NCSC, la NCA, l'ensemble des services répressifs et les communautés diplomatiques et du renseignement pour contrer les menaces qui perturbent la confidentialité, l'intégrité et la disponibilité du cyberespace ou des données et services dans le cyberespace. En particulier, nous investirons dans les capacités de cibler l'infrastructure cybercriminelle et de déployer nos capacités de répression et cybercapacités offensives pour perturber les cybermalveillances. Nos adversaires renforcent leurs cybercapacités et les utilisent de plus en plus à des fins pernicieuses. Nous utiliserons à fond la NCF lorsque nous le jugerons approprié, pour perturber ces efforts, défendre et protéger le Royaume-Uni.

184. Nous lutterons également contre la prolifération de cybercapacités de haut niveau dans les États et les groupes criminels organisés sur des marchés commerciaux et criminels, en nous attaquant aux forums qui favorisent, facilitent ou glorifient la cybercriminalité.

185. Amélioration des résultats de la justice pénale et d'autres résultats perturbateurs pour les cybercriminels, la capacité améliorée de la justice pénale servant à poursuivre les cybercriminels au Royaume-Uni. Nous réviserons la loi sur l'utilisation abusive des ordinateurs Computer Misuse Act (CMA) et les pouvoirs pertinents pour faire en sorte que les services répressifs aient la capacité d'enquêter sur les menaces nouvelles et émergentes des criminels et multiplierons le nombre de procureurs spécialistes pour traiter le nombre croissant de dossiers liés à la cybercriminalité. Par l'intermédiaire du conseil national des chefs de police National Police Chiefs' Council (NPCC), du prospectus des cybercompétences et du College of Policing Cyber Digital Career Pathways (Parcours professionnels des métiers du cybernumérique du College of Policing), nous améliorerons également les compétences de répression spécialisées, d'exercice et d'intégration afin d'assurer un flux continu d'agents possédant les connaissances de cyberspécialistes requises.

Susan Moody, Agent de prévention, Police Service of Northern Ireland (PSNI)

De gauche à droite Susan Moody (PSNI), Sarah Travers (Présentatrice de télévision) et Joe Dolan (Chef du Centre de la cybersécurité d'Irlande du Nord).

Les ordinateurs et les appareils mobiles font partie du quotidien des jeunes. Ils donnent accès à de grandes opportunités certes, mais aussi à des dangers en cas de mauvais usage. La fonction de prévention du PSNI est un outil indispensable d'intervention précoce auprès des jeunes. Elle les aide à comprendre la loi relative à l'utilisation et au mauvais usage des ordinateurs. Elle attire l'attention sur les signes de danger avant-coureurs d'une activité criminelle potentielle, mais aussi sur les grandes opportunités, à travers des initiatives telles que CyberFirst et Cyber as a career, conçues pour montrer à ceux qui manifestent un intérêt ou disposent d'un talent dans ce domaine que l'infraction n'est pas leur seule option et leur éviter que des éléments malveillants profitent d'eux à des fins criminelles. Susan a travaillé sans relâche pour élaborer un programme de cyberinformation destiné aux établissements d'enseignement secondaire, collaborant directement avec plus de 40 écoles primaires, de nombreuses écoles secondaires, des organisations de jeunes et groupes en uniforme. Ces jeunes pourraient très bien être nos cyberambassadeurs et cyberdéfenseurs de demain.

Objectif 3 : prendre des mesures dans et à travers le cyberespace pour étayer notre sécurité nationale, la prévention et la détection des crimes graves

186. À l'horizon 2025, nous serons parvenus aux résultats suivants :

187. Les cybercapacités du Royaume-Uni parviennent mieux à dissuader et perturber les menaces non-cyber. Nous étendrons et développerons la NCF en concrétisant notre vision à long terme quant à cette capacité clé, tout en veillant à ce qu'elle soit pleinement intégrée au GCHQ, au ministère de la Défense britannique, au SIS, au laboratoire des sciences et technologies de la défense (Dstl) et à ce qu'elle travaille en étroite collaboration avec les services répressifs et le gouvernement en général. Nous mènerons des cyberopérations offensives légales et proportionnées à travers la NCF, en agissant de façon responsable dans le cyberespace et en montrant l'exemple. Les cyberopérations offensives continueront d'appuyer la sécurité nationale du Royaume-Uni, politique de défense et politique étrangère incluses, ainsi que la prévention des crimes graves.

188. Nous intensifierons et développerons également nos capacités techniques de répression contre les infrastructures et cryptomonnaies, sachant qu'elles peuvent aussi être déployées contre d'autres menaces.

189. Les cybercapacités du Royaume-Uni sont intégrées à l'ensemble des opérations de défense, en adéquation avec le concept opérationnel intégré Integrated Operating Concept 2025.[36] Elles nous permettront de préserver notre avantage concurrentiel de guerre sur nos adversaires et de mieux collaborer avec nos alliés et partenaires. Nous poursuivrons le Programme de changement d'intégration multidomaines de la défense Defence Multi-Domain Integration Change Programme, conçu pour regrouper les capacités des différents domaines et assurer une meilleure intégration avec d'autres instruments de notre puissance nationale, renforçant notre avantage militaire sur nos adversaires. Des cyberspécialistes hautement qualifiés, une cybersensibilisation globale des effectifs de défense, des cybercapacités de pointe et résilientes feront du domaine cyber un des principaux éléments des activités de défense.

[36] Ministère de la Défense britannique, Integrated Operating Concept (2020)

Grandes enquêtes des services répressifs sur les cybercrimes

Opération Imperil : Op Imperil est le nom donné à une enquête menée conjointement par la cellule régionale du crime organisé South East Regional Organised Crime Unit (SEROCU) et le FBI, sur un site Web qui vendait des renseignements personnels et bancaires compromis se rapportant à des victimes de cyberattaques. Cette activité a permis à d'autres éléments malveillants d'acheter des données à caractère personnel, pour commettre des fraudes et diverses infractions liées à l'utilisation abusive des ordinateurs. Cette importante enquête a abouti à l'identification des comptes bancaires, des paiements utilisés pour l'infrastructure technique et du propriétaire du site Web basé au Pakistan. Le FBI a pu secrètement se saisir du site Web puis en stopper la publication. La cellule South East Regional Organized Crime Unit a arrêté le principal suspect au Royaume-Uni, découvrant qu'il avait ouvert un compte bancaire aux États-Unis au nom du propriétaire du site Web pour blanchir des fonds d'origine criminelle. Le suspect britannique a commis une fraude importante en utilisant certaines données compromises de la victime, en ouvrant des comptes bancaires sous d'autres noms, en utilisant des comptes bancaires compromis pour payer des vacances de luxe, faire de fausses demandes auprès de l'administration britannique du travail et des retraites se soldant pour l'État par une perte de plus de 90 000 GBP. Le suspect a été inculpé de neuf chefs d'accusation et condamné à une peine d'emprisonnement de quatre ans, réduite à la suite d'un aveu précoce de culpabilité. Le juge a décerné une mention élogieuse à l'équipe d'enquêteurs. La confiscation et l'application à vie de la loi sur les produits de la criminalité Proceeds Of Crime Act sont en cours d'approbation au moment de la publication du présent document.

Opération Nipigon : il s'agissait d'une enquête de la Met Police sur un ressortissant bulgare soupçonné d'avoir créé des pages d'hameçonnage sur mesure ayant causé, selon les estimations, plus de 40 millions GBP de pertes au Royaume-Uni. Il a été identifié à la suite d'une enquête sur un autre cybercriminel bien connu, condamné à 10 ans de détention en 2018. Il se servait des pages d'hameçonnage créées par le ressortissant bulgare pour concrétiser ses propres velléités délictuelles. L'enquête ouverte à la suite de l'identification d'une adresse e-mail importante liée au suspect a mené, après des recherches longues et complexes, à un engagement avec les autorités bulgares puis à l'arrestation et à l'extradition du suspect. Après divulgation complète, ce dernier a plaidé coupable à la lecture de toutes les accusations criminelles et écopé d'une peine d'emprisonnement de neuf ans et demi.

Opération Leasing : En 2020 la NCA mène une enquête sur des alertes à la bombe terroristes, lancées contre les services de santé britanniques du NHS au plus fort de la pandémie de COVID-19 et pour lesquelles les auteurs exigent un paiement en Bitcoin (BTC). Le suspect identifié et appréhendé par la NCA en collaboration avec les autorités allemandes, n'a pas échappé à la condamnation par un tribunal allemand.

Le 12 avril 2020, un ressortissant italien vivant en Allemagne envoie un courriel sur le réseau TOR, indiquant son intention de bombarder un hôpital du NHS à moins que ne lui soit versée la somme de 10 millions GBP en Bitcoin.

Attribuant rapidement à l'événement le statut de priorité élevée, la NCA charge des agents spécialistes du cybercrime d'en identifier l'auteur et de prévenir toute attaque potentielle.

L'auteur avait également envoyé des courriels menaçant d'attaquer des députés et de bombarder des manifestants de Black Lives Matter à Londres. Malgré qu'il ait rédigé ses courriels en anglais, les techniques cybernétiques spécialisées, l'analyse comportementale et linguistique auxquelles ont recouru les enquêteurs de la NCA leur ont permis de déduire que la langue maternelle du délinquant était probablement l'allemand.

En collaboration avec les autorités allemandes, les agents de la NCA ont pu localiser à une adresse à Berlin l'ordinateur à partir duquel avaient été envoyés les courriels. Grâce à la collaboration internationale et malgré des efforts importants pour masquer son identité et son adresse, le suspect a été identifié et placé sous surveillance par les forces de l'ordre allemandes. Le suspect a été arrêté le 15 juin 2020, accusé de tentative d'extorsion et placé en détention provisoire. Reconnu coupable le 26 février 2021, il a été condamné à trois ans de prison.

Agir dans le cyberespace pour lutter contre le terrorisme

Campagne de lutte contre Daesh :
Le travail conjoint du ministère de la Défense britannique et du GCHQ contre Daesh illustre la manière dont nous avons activement réagi, pour contrer les menaces de ceux qui font mauvais usage de l'Internet et des canaux de communication modernes.

Daesh a consacré beaucoup de temps et d'énergie à la technologie, pour créer des contenus médiatiques visant à radicaliser, à attirer de nouvelles recrues et à inspirer des attaques terroristes aux quatre coins du monde. Les attaques survenus à Londres et à Manchester ne sont que deux exemples de l'impact de cette approche constaté dans toute l'Europe depuis quelques années. Daesh s'est également servi des systèmes de communication modernes pour commander et contrôler ses opérations sur le champ de bataille. Ils lui ont permis d'intervenir avec souplesse, à l'échelle nécessaire et rapidement, tout en présentant un danger encore plus grave pour les populations qu'ils cherchaient à contrôler et en maximisant sa portée sur l'ensemble de son califat autoproclamé.

Au cours de la bataille de Mossoul, capitale autoproclamée de Daesh, nous avons eu recours à des cyberoutils et cybertechniques dans le cadre d'opérations menées aux côtés des militaires à l'appui de la coalition, dans le cadre d'une campagne plus vaste et à spectre complet. Ces opérations ont eu des résultats de vaste envergure. Perturber les communications, dégrader la propagande, provoquer la méfiance au sein des groupes et le déni de l'équipement et des réseaux utilisés dans le cadre de leurs opérations, figuraient tous parmi les moyens capables de réduire l'efficacité de Daesh. Nous avons également pu utiliser des cybertechniques pour promouvoir les messages du gouvernement du Royaume-Uni auprès des cibles ou encore, signaler leurs activités aux personnes susceptibles de leur fournir ou de leur avoir fourni de l'aide sans s'en douter. Ces opérations ont largement contribué aux efforts de la coalition visant à réprimer la propagande de Daesh, entraver sa capacité de coordonner des attaques et protéger les forces de la coalition sur le champ de bataille.

Andrew, membre de la National Cyber Force

J'ai toujours été fasciné par les toutes dernières technologies de pointe. Avant de travailler pour les services de renseignement, je me suis engagé dans la police et je suis passé de policier sur le terrain à un poste de spécialiste de la criminalistique numérique, chargé de chercher des preuves dans les appareils électroniques des suspects. Ce travail me plaisait vraiment, mais j'avais envie de savoir quelles opportunités existaient ailleurs.

Je ne suis pas allé à l'université après l'école et depuis le début, ma carrière est plutôt menée par ma curiosité naturelle, comme c'est le cas de tous mes collègues qui entrent dans la National Cyber Force. Leurs parcours professionnels sont très variés. Vous y trouverez des experts techniques de haut niveau en son centre, mais aussi un ancien directeur de succursale de supermarché, un instituteur et un pompier. Une chose est sûre, nous avons tous l'esprit ouvert, soif d'apprendre et pour objectif commun d'assurer la sécurité du pays en considérant les menaces et opportunités liées aux technologies émergentes pour la sécurité nationale.

En tant que policier, j'étais extrêmement fier d'aider les gens sur un plan personnel. Aujourd'hui, en tant que membre de cette équipe unique de la National Cyber Force, je fais partie d'une force pour le bien d'envergure mondiale.

Concrétiser notre ambition

190. Cette stratégie ne vaudra rien à moins d'être associée à une approche rigoureuse quant à la mise en œuvre de ses objectifs, au suivi et à l'évaluation des progrès réalisés par rapport à ces derniers et à des mécanismes permettant d'en ajuster le cap au besoin. Ce chapitre explique comment nous entendons l'exécuter.

Rôles et responsabilités de l'ensemble du gouvernement

191. La Cyberstratégie nationale fera partie des stratégies secondaires par lesquelles seront collectivement concrétisées les ambitions de la Revue intégrée. Le National Security Council assurera la surveillance ministérielle de ces stratégies, contrôlant la mise en œuvre et considérant l'équilibre global ainsi que l'orientation de la stratégie du Royaume-Uni. Les progrès par rapport aux objectifs de la stratégie seront également évalués au moyen du Government Planning and Performance Framework (Cadre de planification et de performance du gouvernement) et des Outcomes Delivery Plans (Plans d'exécution des résultats).

192. Tous les ministres participent aux efforts visant à faire en sorte que le Royaume-Uni renforce sa position de cyberpuissance responsable et démocratique, capable de protéger et de promouvoir ses intérêts dans et à travers le cyberespace. Cette liste comprend des ensembles précis de responsabilités associées à des ministres occupant des postes de premier plan, pour mettre en œuvre ou coordonner un ou plusieurs des cinq axes de notre Cyberstratégie nationale ou superviser nos plus importantes cybercapacités et cyberdécisions.

- Le **Chancelier du duché de Lancastre,** avec le soutien du **Paymaster General** (Trésorier-payeur général), assure un leadership global sur l'ensemble des ministères afin d'assurer une réponse efficace du gouvernement face aux cybermenaces et la réalisation de nos ambitions en tant que cyberpuissance. Il est notamment responsable de l'élaboration et de la mise en œuvre de la Cyberstratégie nationale, du programme de soutien par l'investissement et de la coordination des efforts du gouvernement en matière de cyberrésilience. Il est également globalement responsable de la politique intersectorielle et de la coordination liées à la cybersécurité et à la résilience de l'infrastructure critique

nationale du Royaume-Uni. Lorsqu'elles s'imposent, le Chancelier du duché de Lancastre est le président par défaut des réunions ministérielles des Salles de briefing du Cabinet Office (COBR) sur les cyberincidents.

- **La Secrétaire d'État aux Affaires intérieures** joue un rôle déterminant dans la mise en œuvre de l'ensemble de la Cyberstratégie nationale et dans la réponse aux cyberincidents, conformément à ses responsabilités en matière de sécurité intérieure. Aux côtés de la Secrétaire d'État aux Affaires étrangères, du Commonwealth et du Développement et du secrétaire d'État à la Défense, elle dirige le travail du gouvernement pour détecter, perturber et dissuader nos adversaires et en assure la coordination globale. Elle est également spécifiquement responsable de la lutte contre la cybercriminalité.
- **La Secrétaire d'État aux Affaires étrangères, du Commonwealth et du Développement** est officiellement responsable du quartier général des communications GCHQ et par conséquent, du National Cyber Security Centre (Centre national de la cybersecurité). Elle dirige le travail du gouvernement pour améliorer le leadership mondial du Royaume-Uni dans le domaine cyber et assume la responsabilité particulière à l'égard du processus d'attribution des cyberincidents, du régime de cybersanctions et de l'engagement international vis-à-vis des cyberincidents de haut niveau. Elle dirige également le travail du gouvernement pour détecter, perturber et dissuader nos adversaires, aux côtés de la Secrétaire d'État aux Affaires intérieures et du Secrétaire d'État à la Défense.
- Le **Secrétaire d'État à la Défense** dirige le travail du gouvernement pour détecter, perturber et dissuader nos adversaires, aux côtés de la Secrétaire d'État aux Affaires étrangères, du Commonwealth et du Développement et de la Secrétaire d'État aux Affaires intérieures.
- **La Secrétaire d'État aux Affaires étrangères, du Commonwealth et du Développement et le secrétaire d'État à la défense** sont responsables de la National Cyber Force, dans le cadre d'un effort commun unissant la défense et le renseignement.
- La **Secrétaire d'État au Numérique, à la Culture, aux Médias et aux Sports** est responsable de la cybersécurité des organisations de l'ensemble de l'économie, en matière de politique numérique et relevant des aspects pertinents de croissance, d'innovation et de compétences de la Cyberstratégie nationale. Elle dirige le travail du gouvernement pour renforcer l'écosystème cyber du Royaume-Uni et prendre l'initiative des technologies essentielles au cyberpouvoir.
- Les **ministres des ministères responsables de l'infrastructure critique nationale** sont responsables de la politique de cybersécurité et de cyberrésilience de leurs secteurs.
- **Tous les ministres** doivent assurer la surveillance de la cybersécurité de leur ministère et la mise en œuvre des mesures d'atténuation qui conviennent. Un ministère qui supervise un élément du secteur public ou privé (comme le DLUHC et l'administration locale ou le DEFRA et les fournisseurs d'eau), est responsable des activités de cyberpolitique et de cyberassurance relatives à ce secteur.

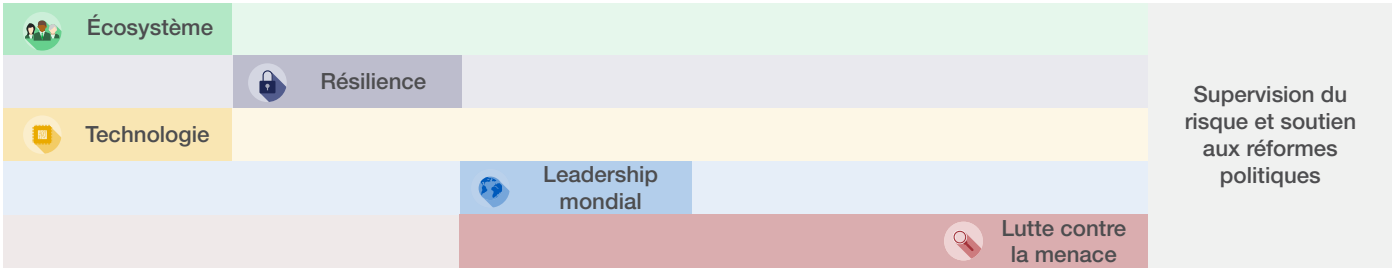
193. Le Deputy National Security Adviser for Intelligence, Security and Resilience (Conseiller adjoint à la sécurité nationale pour le renseignement, la sécurité et la résilience) est le principal responsable de la stratégie. Il en dirigera l'exécution sur l'ensemble du gouvernement au niveau officiel, avec l'appui des hauts fonctionnaires concernés des différents ministères.

Responsabilités ministérielles

Premier ministre

Ministre du numérique	Chancelier du duché de Lancastre*	Ministre des Affaires étrangères	Ministre de la Défense	Ministre de l'Intérieur	Tous les secrétaires d'État

Coordination et leadership liés aux axes stratégiques



Soutien opérationnel et d'exécution sur l'ensemble de la stratégie

*assure un leadership global sur l'ensemble des ministères afin de garantir une réponse efficace du gouvernement face aux cybermenaces et la réalisation de nos ambitions en tant que cyberpuissance.

Investir dans notre cyberpouvoir

194. Au cours des trois prochaines années, le gouvernement investira 2,6 milliards GBP dans le domaine cyber et l'informatique héritée. Cette somme s'ajoute à l'investissement important dans la National Cyber Force. Elle comprend une augmentation de 114 millions GBP du National Cyber Security Programme (Programme national de cybersécurité), le budget annuel consacré aux capacités construites dans le cadre de la stratégie de 2016 étant désormais placé sous la gestion du ministère, sur des bases permanentes. Les programmes internationaux seront mis en œuvre par l'intermédiaire du Conflict, Stability and Security Fund (CSSF - Fonds pour les conflits, la stabilité et la sécurité), pour aider les pays partenaires à renforcer leur cyberrésilience et à lutter contre les cybermenaces. Parallèlement, des investissements revus à la hausse ont également été annoncés dans les domaines de la recherche et du développement (R&D), du renseignement, de la défense, de l'innovation, de l'infrastructure et des compétences, dont tous joueront un rôle dans la constitution du cyberpouvoir du Royaume-Uni.[37]

Mesurer le succès

195. La stratégie sera régie par un cadre de performance en constante évolution, relevant des hauts fonctionnaires responsables et du National Security Council. Ce cadre servira à éclairer les discussions avec les parlementaires et d'autres organismes chargés de superviser le travail de la communauté de la sécurité nationale. Conformément à l'approche de la Stratégie nationale de cybersécurité 2016-2021, les informations sensibles qu'il contient empêche d'en faire un document public, mais le gouvernement publiera des rapports d'étape annuels.

196. Ce cadre de performance :

- expliquera clairement comment les activités mèneront aux divers objectifs décrits dans la stratégie ;
- veillera à la responsabilisation liée à l'exécution de la stratégie ;
- assurera la transparence des progrès du pays vers la réalisation des objectifs énoncés dans la stratégie ;
- illustrera la manière dont l'activité doit s'adapter pour s'aligner sur la stratégie ;
- permettra de savoir quelles activités sont efficaces pour réaliser les ambitions stratégiques et faire en sorte que ces enseignements soient appliqués à l'avenir ;
- fournira une vue d'ensemble des activités des cinq axes, en réduisant les doublons, en identifiant les forces et les faiblesses du cyberpouvoir du pays ;
- veillera à ce que la stratégie fournisse un soutien cybernétique à toutes les catégories de la société.

[37] HM Treasury, Autumn Budget and Spending Review 2021 (2021) (Trésor public, budget et revue des dépenses automnaux)

Prochaines étapes

197. Cette stratégie a été conçue pour guider l'action, non seulement des membres du gouvernement responsables du domaine cyber et des diverses politiques connexes (voir l'annexe A), mais aussi des personnes et organisations de l'ensemble de la société responsables de l'effort cybernétique national ou pour lesquelles il présente un intérêt. C'est d'autre part le début d'un dialogue que nous souhaitons poursuivre, pour veiller à ce que la pertinence de nos objectifs et priorités soit préservée au cours des cinq à dix prochaines années. Nous utiliserons la publication de cette stratégie comme une plateforme d'échange avec les secteurs public, privé et tertiaire du Royaume-Uni et vous encourageons à transmettre vos commentaires à ce sujet à ukcyberstrategy@cabinetoffice.gov.uk. Nous soumettrons un rapport annuel sur les progrès réalisés dans la mise en œuvre de cette stratégie.

Annexe A : La cybernétique intégrée au programme plus général du gouvernement

Le but de la Cyberstratégie nationale est d'appuyer et d'amplifier un éventail d'autres priorités du gouvernement pour l'ensemble de ses programmes de sécurité, de défense, de politique étrangère et économique. À son tour, cette stratégie reposera sur les capacités plus générales développées par le biais de notre système d'éducation, de compétences et de notre approche nationale en matière de politique industrielle numérique et

technologique, de recherche et de croissance des entreprises. Les éléments suivants comptent parmi ses principaux stratégies et plans pertinents :

- **Revue intégrée**, dont les efforts nationaux pour améliorer la résilience, traiter les menaces étatiques, le crime organisé grave et le terrorisme, maintenir notre avantage stratégique grâce à la science et à la technologie et façonner l'ordre international.
- **National Data Strategy**. La stratégie nationale sur les données définit notre vision pour exploiter le pouvoir de l'usage responsable des données afin de dynamiser la productivité, de créer de nouvelles entreprises et de nouveaux emplois, d'améliorer les services publics, de soutenir une société plus juste et de favoriser les découvertes scientifiques afin de faire du Royaume-Uni le précurseur de la prochaine vague d'innovation. Il s'agit notamment de transformer la manière dont le gouvernement utilise les données, pour améliorer le rendement et les services publics en éliminant les obstacles au partage des données entre les ministères et en améliorant la qualité des données dont ils disposent. Cette démarche est essentielle pour appuyer notre cyberprogramme et notamment, pour être sûr de pouvoir colliger et utiliser des données de bonne qualité sur les cyberincidents.
- **Le Plan for growth** (Plan de croissance) dans le cadre de l'initiative **Build Back Better** pour rebâtir une société plus performante grâce à un soutien et à des investissements complémentaires dans les infrastructures, les compétences et l'innovation et à la stratégie d'innovation **Innovation Strategy**, laquelle définit nos ambitions pour une économie axée sur l'innovation.
- **Le Plan for Digital Regulation** (Plan de réglementation numérique), lequel définit notre approche pro-innovation en matière de réglementation des technologies numériques susceptible de stimuler la prospérité et d'instaurer la confiance en leur utilisation.
- **La National AI Strategy** (Stratégie nationale relative à l'IA), dont le but est de préparer le Royaume-Uni à la prochaine décennie transformatrice de l'IA en investissant dans les besoins à long terme de l'écosystème de l'IA, en appuyant la transition vers une économie axée sur l'IA et en veillant à ce que le Royaume-Uni définisse une gouvernance nationale et internationale adaptée aux technologies de l'intelligence artificielle. Elle inclut également des mesures visant à soutenir l'innovation en matière de cybersécurité des systèmes d'IA, tout en protégeant le public et en instaurant la confiance en leur utilisation.
- La prochaine **National Resilience Strategy** (Stratégie de résilience nationale), qui se concentrera en partie sur la façon dont le Royaume-Uni gardera une longueur d'avance sur les menaces technologiques et restera résilient dans le cyberespace.
- La prochaine **Digital Strategy** (Stratégie numérique), laquelle énoncera une vision claire des ambitions du gouvernement, qui entend tirer parti d'un nouvel appétit pour la transformation numérique, accélérer la croissance et continuer à bâtir une économie numérique plus inclusive, concurrentielle et novatrice pour l'avenir, en s'appuyant sur les dix priorités technologiques du DCMS pour mieux définir les ambitions du gouvernement dans le secteur du numérique.
- **La Net Zero Strategy** (Stratégie net zéro), pour veiller à ce que notre économie prospère et axée sur l'innovation soit sobre en carbone.
- **Le Beating Crime Plan** (Plan de lutte contre la criminalité), qui définit les mesures prises pour restaurer la confiance dans le système de justice pénale et concrétiser notre vision commune d'une Grande-Bretagne plus sûre, où la criminalité et le nombre de victimes diminuent.[38]

[38] Home Office, Beating Crime Plan (2021)(Plan de lutte contre la criminalité)

Deux autres publications soutiennent directement la Stratégie nationale de cybersécurité. Elles définissent la manière dont chaque partie de la stratégie sera mise en œuvre.

- La prochaine **Government Cyber Security Strategy** (Stratégie de cybersécurité du gouvernement), laquelle expose les plans plus détaillés d'amélioration de la sécurité du gouvernement et du secteur public pour étayer la stratégie nationale.
- La prochaine **Incentives & Regulations Review 2021** (Revue des incitatifs et règlements), qui d'une part exposera nos conclusions quant à l'efficacité du travail entrepris pour favoriser les améliorations dans le domaine de la cybersécurité au sein de l'économie dans son acception la plus générale et de l'autre, expliquera comment nous proposons de mettre en œuvre les éléments opérationnels et organisationnels de l'axe de résilience.

Annexe B : NIS Regulations (Règlementation relative aux réseaux et systèmes d'information) – stratégie nationale

Introduction

Stratégie nationale relative aux réseaux et systèmes d'information

1. La National Cyber Strategy est désignée comme la stratégie nationale britannique aux fins du Règlement 2 de la règlementation Network and Information Systems (NIS) Regulations 2018 du Royaume-Uni.

2. Cette annexe fournit de plus amples détails, notamment :

- sur les rôles et responsabilités des principales autorités responsables de la mise en œuvre de la règlementation NIS au Royaume-Uni et
- une liste des principales autorités concernées.

Règlementation NIS R.-U.

3. En 2016, la Commission européenne a convenu d'une Directive visant à harmoniser la sécurité des réseaux et systèmes d'information au sein de l'Union européenne (UE). Le gouvernement du Royaume-Uni a approuvé cette Directive.

4. Le 20 avril 2018, le gouvernement présentait au Parlement la nouvelle Network and Information Systems (NIS) Regulations 2018. Cette règlementation est entrée en vigueur le 10 mai 2018.

5. La règlementation NIS a établi un nouveau régime réglementaire au Royaume-Uni, exigeant que les opérateurs désignés de services essentiels (OSE) et les fournisseurs de services numériques pertinents (RDSP) mettent en place des mesures techniques et organisationnelles pour sécuriser leurs réseaux et systèmes d'information.

6. Elle s'applique à des secteurs vitaux pour notre économie, notre société et dont le fonctionnement dépend largement des réseaux et systèmes d'information, comme l'énergie, les transports, l'eau potable, les soins de santé et les infrastructures numériques.

7. Les principaux fournisseurs de services numériques (moteurs de recherche, services de cloud computing et marchés en ligne) sont aussi couverts.

8. La règlementation NIS établit :

- **un cadre national** pour soutenir la mise en œuvre, dont une stratégie nationale ;
- des **autorités compétentes** sectorielles jouant le rôle de régulateurs ;
- Le National Cyber Security Centre (NCSC) en tant que point de contact unique **Single Point of Contact** (SPOC) et l'équipe d'experts en sécurité informatique **Computer Security Incident Response Team** (CSIRT) chargée de répondre aux incidents.

9. Les progrès sont évalués tous les deux à cinq ans, au moyen de rapports rétrospectifs.

Principaux rôles et responsabilités

Cadre national

10. Secrétariat général du gouvernement, le Cabinet Office est responsable de la cyberstratégie nationale, laquelle comprend la stratégie nationale relative aux réseaux et systèmes d'information NIS National Strategy. Par ailleurs, le Cabinet Office est aussi globalement responsable de l'amélioration de la sécurité et de la résilience de l'infrastructure critique nationale.

11. Le Department for Digital, Culture, Media and Sport (DCMS - ministère du Numérique, de la Culture, des Médias et des Sports) est responsable de la mise en œuvre globale de la règlementation NIS, coordination des autorités pertinentes et du NCSC incluse. Le DCMS fournit les conseils permettant aux autorités compétentes de soutenir la mise en œuvre plus générale de la règlementation NIS au Royaume-Uni.

Single Point of Contact (SPOC - Point de contact unique)

12. Point de contact national d'échange avec les partenaires internationaux [de l'UE] sur la règlementation NIS, chargé de coordonner les demandes d'action ou d'information et de la présentation des statistiques annuelles sur les incidents. Le National Cyber Security Centre est le point de contact unique (SPOC) du Royaume-Uni.

Computer Security Incident Response Team (CSIRT - Équipe d'experts en sécurité informatique chargée de répondre aux incidents).

13. Au Royaume-Uni la fonction CSIRT est assurée par le National Cyber Security Centre. Elle est chargée de la surveillance des incidents de cybersécurité à l'échelle nationale, de fournir des analyses en temps réel des menaces, de défendre contre les cyberattaques nationales, de fournir des conseils techniques et de répondre aux cyberincidents majeurs pour contribuer aux mesures visant à limiter au maximum les préjudices consécutifs.

14. Le NCSC assure l'actualisation du cadre de cyberévaluation Cyber Assessment Framework (CAF) axé sur les résultats et fournit des conseils détaillés sur les questions de cybersécurité en tant qu'autorité technique nationale.

Autorités compétentes

15. Elles sont responsables de la surveillance et de l'application de la règlementation NIS dans leurs secteurs, de la désignation et de l'évaluation de la conformité des opérateurs de services essentiels (OSE) et fournisseurs de services numériques pertinents (RDSP) aux exigences de la règlementation NIS. Elles sont répertoriées à l'annexe 1 de la règlementation NIS et à la section 3 sous forme de liste.

Opérateurs de services essentiels (OSE) et Relevant Digital Service Providers (RDSP - Fournisseurs de services numériques pertinents)

16. Les OSE ou RDSP qui satisfont aux seuils de désignation du secteur concerné ou ont été désignés par l'autorité compétente en vertu du règlement 8(3) de la règlementation NIS, doivent se conformer aux exigences de la règlementation NIS.

17. Il s'agit par conséquent :

- de prendre des mesures techniques et organisationnelles adaptées à la situation et proportionnées, pour gérer les risques posés à la sécurité du réseau et des systèmes d'information ;
- de prendre des mesures adaptées à la situation et proportionnées pour empêcher et limiter au maximum l'impact des incidents nuisant à la sécurité du réseau et des systèmes d'information ;
- d'informer l'autorité compétente concernée de tout incident ayant une incidence substantielle sur leurs services ;
- de satisfaire aux conditions d'inspection en vertu de la règlementation NIS et
- de se conformer aux notes d'information, avis de mise en conformité et de sanction.
- Les RDSP sont également censés s'enregistrer auprès de l'Office du commissaire à l'information (ICO).

Autres autorités pertinentes :

18. Le gouvernement du Royaume-Uni travaille à la mise en œuvre de la règlementation NIS en étroite collaboration avec les administrations décentralisées et d'autres autorités pertinentes, comme les ministères responsables.

19. Le Centre for the Protection of National Infrastructure (CPNI - Centre de protection de l'infrastructure nationale) donne des conseils sur la sécurité physique et du personnel connexe.

Liste des principales autorités de mise en œuvre de la règlementation NIS

Autorités nationales	
Règlementation NIS R.-U.	Ministère du Numérique, de la Culture, des Médias et des Sports (DCMS)
Cyberstratégie nationale, R.-U.	Cabinet Office (Secrétariat général du gouvernement)
Point de contact unique (SPOC) au Royaume-Uni	National Cyber Security Centre (Centre national de la cybersécurité)
UK Computer Security Incident Response Team (CSIRT - Équipe d'experts en sécurité informatique chargée de répondre aux incidents)	National Cyber Security Centre (Centre national de la cybersécurité)

Autorités compétentes					
Secteur	**Sous-secteur**	**Angleterre**	**Pays de Galles**	**Écosse**	**Irlande du Nord**
Énergie	Électricité	Mixte : Department for Business, Energy, and Industrial Strategy (ministère des Affaires, de l'Énergie et de la Stratégie industrielle) et Ofgem, régulateur des marchés du gaz et de l'électricité			Department of Finance (ministère des Finances)
	Pétrole	Department for Business, Energy, and Industrial Strategy (ministère des Affaires, de l'Énergie et de la Stratégie industrielle)			Department of Finance (ministère des Finances)
	Gaz	Mixte : Department for Business, Energy, and Industrial Strategy (ministère des Affaires, de l'Énergie et de la Stratégie industrielle) et Ofgem, régulateur des marchés du gaz et de l'électricité[39]			Department of Finance (ministère des Finances)
Transport	Air	Mixte : Department for Transport (ministère des Transports) et Civil Aviation Authority (CAA - Autorité aéronautique civile)			
	Rail	Department for Transport (ministère des Transports)			Department of Finance (ministère des Finances)
	Eau	Department for Transport (ministère des Transports)			
	Voirie	Department for Transport (ministère des Transports)		Ministres écossais	Department of Finance (ministère des Finances)
Services médicaux	Établissements de santé	Department of Health and Social Care (ministère de la Santé et des Affaires sociales)	Ministres gallois	Ministres écossais	Department of Finance (ministère des Finances)
Eau potable	Eau potable	Department for Environment, Food and Rural Affairs (ministère de l'Environnement, de l'Alimentation et des Affaires rurales)	Ministres gallois	Drinking Water Quality Regulator for Scotland (Autorité de règlementation de la qualité de l'eau potable en Écosse)	Department of Finance (ministère des Finances)
Infrastructure numérique	Infrastructure numérique	Office of Communication (Ofcom)			

[39] Dans certains cas exceptionnels le Department for Business, Energy, and Industrial Strategy est la seule autorité compétente. Pour de plus amples détails, consulter les annexes 1 et 2 de la règlementation Network and Information Systems Regulations 2018.

Annexe C : Glossaire

Action Fraud – centre de signalement des fraudes et cybercrimes où les citoyens et organisations victimes d'escroquerie, de tromperie ou d'un cybercrime doivent signaler les fraudes en Angleterre, au Pays de Galles et en Irlande du Nord. En Écosse, ces signalements sont effectués auprès de Police Scotland.

Active Cyber Defence (ACD - Cyberdéfense active) – aide les organisations à détecter les vulnérabilités et à y remédier, à gérer les incidents ou à automatiser la perturbation des cyberattaques. Certains services sont principalement destinés au secteur public. D'autres sont plus largement accessibles au secteur privé ou aux citoyens, en fonction de leur applicabilité et de leur viabilité.

Analyse prospective « Horizon-scanning » – examen systématique de l'information afin d'identifier les menaces, les risques, les nouveaux enjeux et opportunités dans le but de mieux se préparer et d'intégrer l'atténuation et l'exploitation dans le processus d'élaboration des politiques.

Authentification – processus de vérification de l'identité ou d'autres attributs d'un utilisateur, processus ou appareil.

Autorités compétentes – organes règlementaires décrits dans la règlementation Network and Information Systems (NIS) Regulations 2018. La NIS couvre différents secteurs dont diverses autorités compétentes sont responsables.

COBR – Cabinet Office Briefing Rooms (Salles de briefing du Cabinet Office). L'intervention du gouvernement central du Royaume-Uni en cas d'urgence est étayée par le recours aux COBR. La réponse centralisée est activée, surveillée et coordonnée depuis ces emplacements physiques se situant généralement à Westminster. Ils servent de point de convergence à la réponse du gouvernement et de source de conseils faisant autorité au service des intervenants locaux.

Crypt-Key (CK) – terme évoquant l'utilisation par le Royaume-Uni de la cryptographie pour protéger l'information et les services critiques sur lesquels comptent le gouvernement, l'armée et la communauté de sécurité nationale du Royaume-Uni, notamment pour lutter contre les attaques de nos adversaires les plus compétents.

Cryptographie – science ou étude de l'analyse et du déchiffrage des codes et chiffrements ; cryptoanalyse.

Cryptomonnaie – monnaie et système de paiement numériques, ex. Bitcoin.

Cyber Assessment Framework (CAF - Cadre de cyberévaluation) – il fournit une approche systématique et exhaustive pour évaluer à quel point l'organisation responsable parvient à gérer les cyberrisques menaçant les fonctions essentielles.

Cyberattaque – exploitation délibérée et à des fins malveillantes de systèmes informatiques, d'entreprises et de réseaux qui dépendent du numérique.

Cybercrime – infraction dépendant de l'informatique (infractions ne pouvant être commises qu'en utilisant un périphérique informatique, le périphérique servant à la fois d'outil pour les commettre et de cible aux infractions) ou infraction facilitée par les technologies de l'information et de la communication (infraction pouvant être commise sans périphérique informatique, c'est le cas de la fraude financière, mais dont l'ampleur et la portée changent considérablement en cas de recours aux TIC).

Cyberincident – événement constituant ou susceptible de constituer une menace pour un ordinateur, un dispositif connecté à l'Internet ou un réseau ou encore aux données traitées, stockées ou transmises sur ces systèmes, susceptible de nécessiter une réponse visant à en atténuer les conséquences.

Cybermenace – toute occurrence susceptible de compromettre la sécurité des ou d'être préjudiciable aux systèmes d'information et appareils connectés à l'Internet (matériel, logiciels et infrastructure connexes), à leurs données et aux services qu'ils fournissent, principalement par des moyens cybernétiques.

Cyberoffensive – ajouter, supprimer ou manipuler des données sur des systèmes ou des réseaux pour provoquer un effet physique, virtuel ou cognitif. Les opérations de cyberoffensive exploitent souvent des vulnérabilités techniques, utilisent les systèmes ou réseaux à des fins que leurs propriétaires et opérateurs n'envisageraient et n'approuveraient pas et peuvent éventuellement recourir à la tromperie ou aux fausses déclarations.

Cyberrisque – possibilité qu'une cybermenace donnée exploite les vulnérabilités d'un système d'information au point de lui être préjudiciable.

Cyberrésilience – capacité globale des systèmes, des organisations et des citoyens à résister aux cyberévénements et, en cas de préjudice, à s'en remettre.

Cyber Security Body of Knowledge (CyBOK) – unique en son genre, cette ressource fournit pour la première fois un ensemble porteur de connaissances couvrant l'ampleur et la profondeur du domaine de la cybersécurité et montrant à quel point il rassemble un large éventail de disciplines.

Cybersécurité – protection contre les accès non autorisés, préjudices ou utilisations abusives des systèmes connectés à l'Internet (matériel, logiciels et infrastructure associée compris), de leurs données et des services qu'ils fournissent. Sont également concernés les dommages causés intentionnellement par l'exploitant du système ou accidentellement, faute d'avoir suivi les procédures de sécurité ou après avoir été manipulé pour les causer.

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

Écosystème cyber – ensemble des infrastructures, des personnes, des processus, des données, des technologies de l'information et des communications interconnectés, auxquels s'ajoutent l'environnement et les conditions ayant une incidence sur ces interactions.

Five Eyes – alliance de renseignement entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Elle facilite le partage d'informations afin de protéger le mieux possible les citoyens contre les menaces.

Fournisseurs de services gérés – tiers fournissant un ensemble de services définis à un client et assumant la responsabilité de l'exploitation, de l'entretien et de la sécurisation de ces services.

GCHQ – Government Communications Headquarters, quartier général des communications du gouvernement britannique, centre des activités de renseignement du gouvernement et de l'autorité technique nationale National Technical Authority (NTA).

Gestion des incidents – gestion et coordination des activités entreprises pour enquêter sur l'occurrence avérée ou possible d'un cyberévénement préjudiciable, susceptible de compromettre ou de nuire à un système ou à un réseau et pour y remédier.

GFCE – Forum mondial sur la cyber-expertise.

Gouvernement décentralisé ou administration décentralisée – législatures et exécutifs séparés d'Écosse, du Pays de Galles et d'Irlande du Nord à la suite de la décentralisation. Responsables de nombreuses questions de politique intérieure, ils ont le pouvoir de légiférer dans leurs pays.

Government Cyber Coordination Centre (GCCC - Centre de cybercoordination du gouvernement) – Coentreprise proposée associant le GSG, le CDDO et le NCSC afin d'en regrouper les fonctions et domaines d'expertise respectifs, dans le but de mieux coordonner les efforts de cybersécurité opérationnelle sur l'ensemble du gouvernement, de transformer la manière dont ce dernier utilise les données de cybersécurité et les renseignements sur les menaces et d'améliorer concrètement sa capacité de se « défendre à l'unisson ».

ICANN – Internet Corporation for Assigned Names and Numbers (Société pour l'attribution des noms de domaine et des numéros sur Internet). Elle coordonne les noms de site Internet et les adresses IP.

Informatique héritée – l'informatique héritée regroupe les systèmes et leurs composants logiciels et matériels ne bénéficiant plus du support du fournisseur, couverts par une prolongation de support et/ou des dispositions de support sur mesure.

Infrastructure critique nationale – éléments essentiels de l'infrastructure (à savoir les biens, installations, systèmes, réseaux ou processus et les travailleurs essentiels qui les utilisent et les facilitent), dont la perte ou la compromission pourraient avoir :

a. d'importantes répercussions négatives sur la disponibilité, l'intégrité ou l'exécution de services essentiels et notamment des services dont l'intégrité, si elle est compromise, pourrait entraîner de nombreux pertes humaines ou blessés, sans oublier d'importantes répercussions économiques ou sociales et/ou

b. une incidence importante sur la sécurité nationale, la défense du pays ou le fonctionnement de l'État.

Intelligence artificielle – technologie par laquelle un système informatique est codé pour « penser pour lui-même », s'adapter et fonctionner de manière autonome. Le recours à l'IA pour exécuter des tâches plus complexes, comme le diagnostic médical, la découverte de médicaments et la maintenance prédictive est de plus en plus fréquent.

Internet des objets – totalité des dispositifs, véhicules, bâtiments et autres éléments dont l'électronique, les logiciels et capteurs communiquent et échangent des données sur l'Internet.

Internet – réseau informatique planétaire offrant diverses installations d'information et de communication, constitué de réseaux interconnectés utilisant des protocoles de communication standardisés.

Intégrité – dans le domaine de la sécurité de l'information, l'intégrité d'une information est préservée si celle-ci n'a pas été modifiée accidentellement ou délibérément et si elle est exacte et complète.

Jumeau numérique – réplique virtuelle ou représentation d'actifs, de processus, de systèmes ou d'institutions dans les environnements construits, sociétaux ou naturels. En donnant un aperçu du comportement des actifs physiques complexes et des citoyens, il aide les organisations à améliorer la prise de décision et à optimiser les processus. Les changements dans le monde réel sont reproduits par le jumeau et vice versa, les changements du jumeau peuvent se reproduire automatiquement dans le monde réel.

Le Plan for Digital Regulation (Plan de règlementation numérique) – définit l'approche globale du gouvernement en matière de gouvernance des technologies numériques visant à stimuler la croissance et l'innovation.

Les Operational Technologies (OT - Technologies opérationnelles) – associent le matériel au logiciel pour surveiller, contrôler et automatiser les processus physiques, surtout dans les secteurs industriels comme l'énergie, la fabrication, l'eau et les transports.

Micro-cogénération – production à petite échelle d'énergie par les particuliers, PME et communautés.

National Cyber Security Centre (NCSC - Centre national de la cybersécurité) – autorité technique du Royaume-Uni pour les cybermenaces, ce centre assure une réponse nationale unifiée aux cyberincidents afin de limiter au maximum les préjudices en découlant, de contribuer à la reprise et d'en tirer les enseignements pour l'avenir.

NCA – National Crime Agency (Agence nationale de lutte contre la criminalité).

Network and Information Systems (NIS) Regulations 2018 – cette règlementation du Royaume-Uni prévoit des mesures légales pour booster le niveau de sécurité (cyberrésilience et résilience physique) des réseaux et systèmes d'information chargés d'assurer les services essentiels et numériques.

OCDE – l'Organisation de coopération et de développement économique est une organisation économique intergouvernementale.

Opérateurs de services essentiels – organisations au sein de secteurs vitaux qui dépendent fortement des réseaux d'information. C'est notamment le cas des services publics, des soins de santé, des transports et de l'infrastructure numérique, tels que les identifient les critères de la règlementation Network and Information Systems (NIS) Regulations 2018.

OTAN – Organisation du traité de l'Atlantique Nord.

Rançongiciel – ce type de logiciel malveillant empêche l'utilisateur d'accéder à ses fichiers, à son ordinateur ou à ses appareils tant qu'une rançon n'a pas été versée.

Revue intégrée – « Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy », décrit la vision du gouvernement quant au rôle que jouera le Royaume-Uni dans le monde au cours de la prochaine décennie et l'action du gouvernement à l'horizon 2025.

Réponse aux incidents – activités mises en œuvre pour traiter les effets à court terme, directs d'un incident et éventuellement, faciliter la reprise à court terme.

Secure by Design – (Sécurisé de façon native) logiciel, matériel et systèmes conçus, de A à Z, pour être sécurisés.

Système autonome – série de réseaux IP dont le cheminement est asservi à une entité ou à un domaine en particulier.

Systèmes de contrôle-commande industriels (ICS) – système informatique utilisé pour contrôler des procédés industriels tels que la fabrication, la manutention, la production et la distribution des produits ou des actifs d'infrastructure.

Technologie Blockchain – moyen particulier de stocker des données. Une blockchain est un genre de registre distribué – type de technologie de stockage append-only (ajout seul), inviolable.

Technologies quantiques – la technologie quantique est basée sur les principes de la physique quantique. L'amélioration de la compréhension et de la maîtrise d'« effets quantiques », comme la superposition et l'enchevêtrement, aboutira à une nouvelle vague de progrès qui sous-tendront notre économie et notre société : détection, transmission et chiffrement des données, synchronisation et calcul.

Villes connectées – communauté intégrant les technologies de l'information, de communication et les dispositifs IdO pour recueillir et analyser les données afin de fournir de nouveaux services à l'environnement bâti et d'améliorer la qualité de vie des citoyens.

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.

Vulnerability Reporting Service – service de signalement des vulnérabilités par lequel une organisation peut être alertée de failles de sécurité avant qu'elles ne soient exploitées par des attaquants.

Vulnérabilité – bogue informatique présentant un potentiel exploitable par les attaquants.