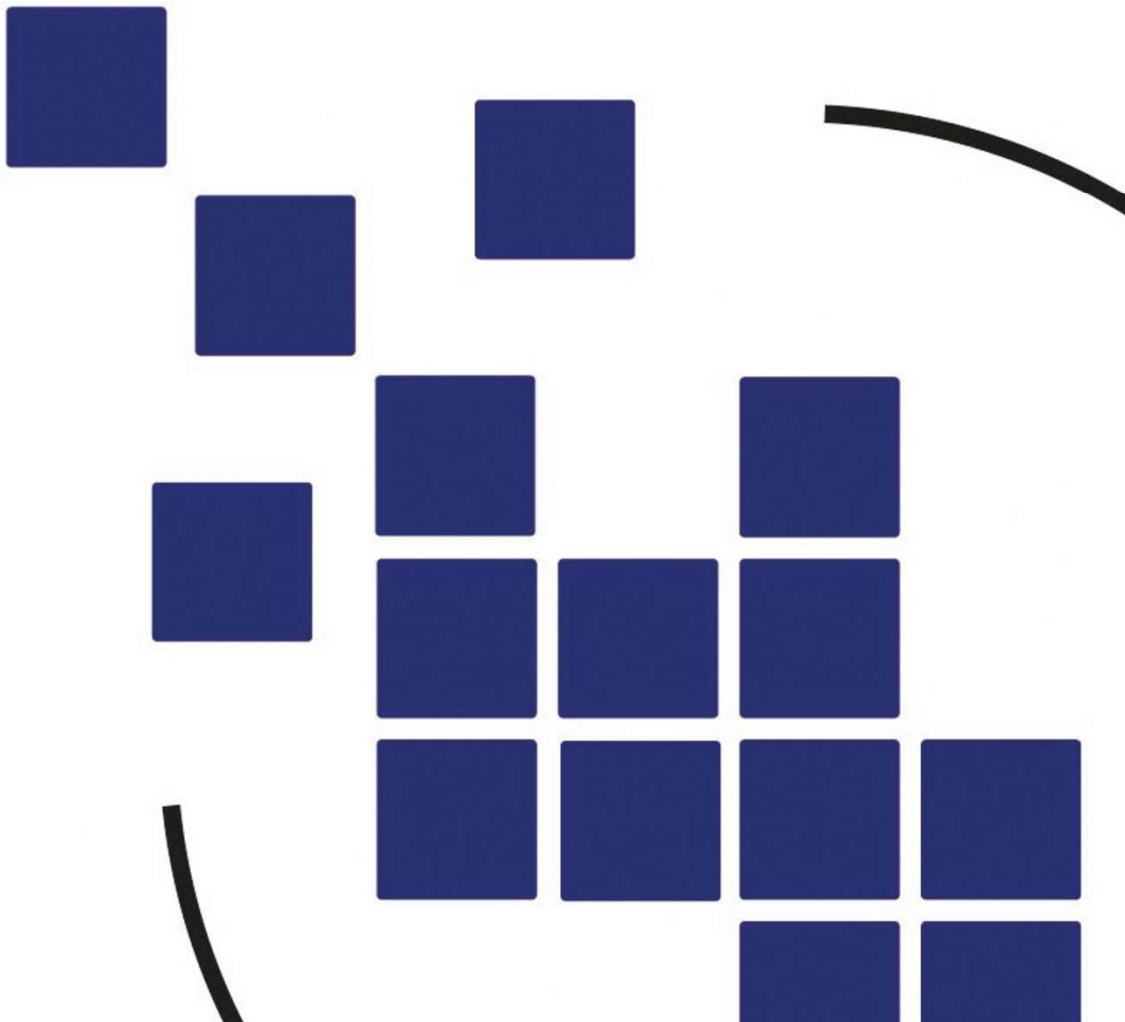
Pall Mall Process

PROCESSUS DE PALL MALL

LIGNES DIRECTRICES À L'INTENTION DE L'INDUSTRIE DE L'INTRUSION CYBER

Pour lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché



Section 1 – Préface

1. Nous, États, encourageons vivement les entités privées actives dans l'industrie des capacités d'intrusion cyber disponibles sur le marché à suivre les présentes lignes directrices à l'intention de l'industrie de l'intrusion cyber, volontaires et non contraignantes, afin de lutter contre les menaces posées par la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché. Nous soutenons l'application des présentes lignes directrices dans nos territoires respectifs, conformément aux cadres juridiques nationaux et aux limites inhérentes aux juridictions nationales. Les lignes directrices détaillées ci-dessous sont établies sans préjudice des obligations existantes en vertu du droit national ou international et dans le respect des cadres juridiques nationaux et internationaux applicables régissant le développement, la facilitation, l'acquisition, le transfert et l'usage de capacités d'intrusion cyber disponibles sur le marché.

2. Les présentes lignes directrices sont publiées dans le contexte du Processus de Pall Mall, une initiative multipartite lancée en 2024 afin de faire face aux problématiques soulevées par la prolifération et l'usage irresponsable de capacités d'intrusion cyber disponibles sur le marché, notamment en ce qui concerne la sécurité, le rôle des médias et de la presse et les droits de l'Homme, tel que le droit de ne pas faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée et le droit à la liberté d'expression. Des États, des organisations internationales, des entreprises, des universitaires et des représentants de la société civile ont fourni des recommandations en réponse à cette question de plus en plus préoccupante. Dans le cadre de ce travail itératif, des États ont volontairement adopté le Code de bonnes pratiques à destination des États de 2025, qui établit des principes directeurs et met en avant les actions envisageables concernant le développement, la facilitation, l'acquisition, le transfert et l'usage de capacités d'intrusion cyber disponibles sur le marché.

3. Les outils et les services d'intrusion cyber peuvent être développés et utilisés à des fins légitimes s'ils sont mis au point de manière légale et s'accompagnent de garanties et de mécanismes de supervision adéquats, conformément au Code de bonnes pratiques à destination des États du Processus de Pall Mall et à la législation applicable. Bien que les États soient responsables de la réglementation, de l'achat et de l'usage de ces capacités, l'industrie de l'intrusion cyber, notamment les investisseurs, les financiers, les développeurs, les acheteurs et les fournisseurs, doivent prendre des mesures suffisantes, notamment celles définies ci-après à la section 4, pour veiller à ce que ces capacités soient développées de manière responsable et vendues avec des garanties adéquates afin de respecter les droits de l'Homme et le droit international applicable, de prévenir les usages irresponsables et de limiter leur prolifération. Ces garanties doivent être efficaces tout au long du cycle de vie des capacités.

4. La prolifération des capacités d'intrusion cyber disponibles sur le marché, par leur transfert volontaire ou involontaire, suscitent des inquiétudes quant à leur éventuel usage irresponsable.

4.a. Aux fins du Processus de Pall Mall, le terme « usage irresponsable » par un acteur étatique ou non étatique désigne notamment un usage qui menace la sécurité, le respect

des droits de l'Homme et les libertés fondamentales ou la stabilité du cyberespace, sans garanties ni mécanisme de supervision adéquats, ou d'une manière qui soit incompatible avec le droit international applicable, notamment le droit international des droits de l'Homme, ou avec les normes volontaires et non contraignantes que prévoit le cadre des Nations Unies pour un comportement responsable des États dans le cyberespace, en tenant dûment compte, le cas échéant, du droit national.

4.b. Aux fins du processus de Pall Mall, le terme « prolifération » désigne la dissémination incontrôlée des capacités d'intrusion cyber disponibles sur le marché parmi les acteurs étatiques ou non étatiques d'une manière qui facilite grandement l'accès à ces outils et à ces services ou qui améliore sensiblement leur efficacité en vue de leur usage irresponsable.

4.c. Les capacités d'intrusion cyber disponibles sur le marché ne doivent pas être utilisées pour cibler des individus ou des groupes sur le fondement de motifs discriminatoires, ou pour porter atteinte aux libertés fondamentales ou aux droits de l'Homme, notamment le droit à la liberté d'expression, le droit de participer à la vie publique, le droit de réunion pacifique et le droit de ne pas faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée.

5. L'industrie de l'intrusion cyber englobe une grande variété d'entreprises qui proposent des produits et des services qui évoluent et se diversifient constamment. Elle comprend notamment un écosystème interconnecté de chercheurs, de développeurs, de courtiers, de revendeurs, d'investisseurs, de financiers, de sociétés et d'opérateurs.

5.a. Les progrès technologiques dans le domaine de l'automatisation et des grands modèles de langage sont susceptibles d'influer sur le développement, l'accessibilité, l'extensibilité, la rapidité, la précision et les effets potentiels des capacités d'intrusion cyber. Ils pourraient contribuer aux activités tout au long du cycle de vie des capacités d'intrusion cyber disponibles sur le marché, notamment la recherche de vulnérabilités, le développement d'exploits, le soutien opérationnel et l'automatisation des activités d'intrusion cyber. Ces évolutions technologiques peuvent être mises à profit pour améliorer la précision, les capacités de défense et la résilience systémique. Bien que le Processus de Pall Mall ne s'applique pas aux développeurs de ces nouvelles technologies, les fournisseurs de ces technologies pourraient s'appuyer sur les présentes lignes directrices.

6. L'industrie de l'intrusion cyber doit jouer, et joue déjà, un rôle important dans la limitation des risques de prolifération et d'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché. Les présentes lignes directrices définissent des principes et des mesures pratiques à destination de tous les acteurs pertinents de l'industrie qui participent au financement, au développement, à la facilitation, à l'exportation, à la vente, à l'acquisition et à l'exploitation de capacités d'intrusion cyber disponibles sur le marché.

7. En complément du Code de bonnes pratiques à destination des États, et en s'appuyant sur les quatre piliers sous-tendant le Processus de Pall Mall, à savoir la responsabilité, la transparence, la précision et la supervision, les présentes lignes directrices donnent des recommandations pratiques devant être adoptées par les États et appliquées par le

secteur privé (voir section 4) pour décourager les activités irresponsables dans l'ensemble du marché des capacités d'intrusion, améliorer la transparence pour les autorités de régulation, les fournisseurs et les clients et offrir une vision claire aux entreprises actives au sein de l'industrie de l'intrusion cyber ou en périphérie de celle-ci. Ces actions doivent encourager les pratiques responsables dans l'ensemble de l'industrie de l'intrusion cyber.

8. Rien dans les présentes lignes directrices ne porte atteinte aux obligations existantes en vertu du droit international, notamment du droit international des droits de l'Homme et du droit international humanitaire. De plus, rien dans les présentes lignes directrices ne nécessite la divulgation d'informations sensibles, d'informations d'État classifiées ou d'informations dont la diffusion porterait atteinte à la prévention ou à la détection d'infractions pénales ou aux enquêtes ou poursuites en la matière.

Section 2 – Principes fondateurs

9. Les présentes lignes directrices complètent et soutiennent les objectifs du cadre des Nations Unies pour un comportement responsable des États dans le cyberespace. Cela inclut les normes volontaires et non contraignantes formulées respectivement en 2015 (A/70/174) par le Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et en 2021 (A/76/135) par le Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, qui ont été adoptées par consensus par l'Assemblée générale des Nations Unies, et plus récemment le Rapport final du groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025). La mise en œuvre des normes adoptées par consensus doit se poursuivre dans le cadre du Mécanisme mondial des Nations Unies.

10. Les rapports de 2015 et 2021 des Groupes d'experts gouvernementaux des Nations Unies incluent la norme 13 c), selon laquelle les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies numériques ; la norme 13 i), selon laquelle les États devraient s'attacher à prévenir la prolifération des techniques et des outils numériques malveillants et l'utilisation de fonctionnalités cachées malveillantes ; et la note 13 j), selon laquelle les États devraient encourager le signalement responsable des vulnérabilités numériques.

11. Nous reconnaissons que les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (ci-après dénommés les « Principes directeurs des Nations Unies ») s'appliquent aux entreprises actives dans l'industrie de l'intrusion cyber, indépendamment de leur taille, de leur secteur d'activité, de leur lieu d'implantation, de leur régime de propriété ou de leur structure. Les Principes directeurs des Nations Unies sont fondés sur la reconnaissance des obligations existantes qui incombent aux États de respecter, protéger et mettre en œuvre les droits de l'Homme et les libertés fondamentales et de l'obligation pour les entreprises de se conformer à toutes les lois applicables et de respecter les droits de l'Homme. Ils reconnaissent également la nécessité que les droits et obligations s'accompagnent de voies de recours efficaces en cas de violation.

12. Les Principes directeurs des Nations Unies s'appliquent notamment à toute entreprise étant en contact avec l'industrie de l'intrusion cyber ou étant active dans cette industrie.

12.a. Les acteurs privés qui financent le marché de l'intrusion cyber ou le développement, la facilitation, l'acquisition, le transfert ou l'usage de capacités d'intrusion cyber disponibles sur le marché, ou qui investissent dans ce marché ou dans ces domaines, doivent veiller à ce que les entités qu'ils financent agissent conformément aux cadres internationaux, notamment aux cadres définis dans les présentes lignes directrices et dans les Principes directeurs des Nations Unies.

13. La société civile et les autres acteurs privés qui supervisent le marché de l'intrusion cyber, notamment les chercheurs indépendants et les entreprises de renseignement sur les cybermenaces et de technologies de lutte contre ces menaces, jouent un rôle crucial dans la détection, l'identification et la révélation d'activités et d'usages irresponsables ainsi que dans la divulgation des vulnérabilités et dans la facilitation de l'accès à des recours pour les victimes. Nous encourageons une plus grande coopération entre les États, l'industrie de l'intrusion cyber et ces entités de supervision, dans le respect des réglementations nationales et des restrictions relatives aux informations sensibles, afin de lutter contre l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché. L'industrie de l'intrusion cyber ne doit pas prendre part à des activités qui empêchent la société civile d'exercer ces fonctions de supervision.

14. Nous reconnaissons les contributions d'instruments multilatéraux comme les Principes directeurs de l'Organisation de coopération et de développement économiques (OCDE) à l'intention des entreprises multinationales sur la conduite responsable des entreprises. L'industrie de l'intrusion cyber doit appliquer les dispositions de cet instrument concernant la diligence requise en matière de droits de l'Homme.

Section 3 : Définitions

15. Aux fins du processus de Pall Mall et des présentes lignes directrices, nous reconnaissons les définitions suivantes. De plus, les définitions et les lignes directrices ci-dessous se concentrent sur les activités commerciales réalisées à des fins d'intrusion cyber, et n'ont pas vocation à s'appliquer aux entités, aux activités, aux outils ou aux services développés aux seules fins de la résilience en matière de cyberdéfense, de la recherche universitaire, de l'analyse criminelle numérique ou des tests de sécurité, notamment aux tests d'intrusion, aux programmes de chasse aux vulnérabilités et aux activités menées dans le cadre de processus de divulgation coordonnée des vulnérabilités ou en soutien à ces processus.

15.a. Les capacités d'intrusion cyber disponibles sur le marché désignent les composants, les outils, les plateformes ou les services professionnels d'ordre technique et technologique, notamment les logiciels espions disponibles sur le marché, mis à disposition par l'industrie de l'intrusion cyber pour permettre d'accéder à des systèmes informatiques, comme des réseaux, des services, des comptes, des logiciels, des appareils mobiles, ou aux données stockées sur ceux-ci, ou d'opérer au sein de ces systèmes. Ces capacités peuvent être proposées selon un modèle de commerce interentreprises, dans le

cadre d'une chaîne d'approvisionnement, ou directement aux utilisateurs finaux selon un modèle entreprise-client. Elles comprennent notamment :

15.a.i. les capacités opérationnelles : les produits, plateformes, infrastructures, composants clé-en-main ou les services gérés conçus pour permettre (ou réaliser) l'accès initial à un système ou à des données ciblées, ainsi que la commande et le contrôle, la collecte, l'extraction, l'altération ou la disruption de ce système ou de ces données ;

15.a.ii. la recherche de vulnérabilités . l'activité qui vise à détecter et à analyser les faiblesses ou les failles potentielles dans des systèmes informatiques, tels que des logiciels ou des réseaux, qui pourraient être exploitées pour compromettre la confidentialité, l'intégrité et la disponibilité des systèmes de données ;

15.a.iii. le développement d'exploits : le processus de recherche, de conception et de création de logiciels ou de techniques qui tirent parti de vulnérabilités pour obtenir un comportement imprévu dans un système informatique (par exemple obtenir un accès sans y être autorisé, exécuter du code ou compromettre l'intégrité du système) ;

15.a.iv. les services d'intrusion cyber : par exemple les services d'accès à la demande ou de capacités à la demande.

15.b. L'industrie de l'intrusion cyber désigne l'écosystème d'entités commerciales, d'entreprises et d'individus qui participent au financement, à la recherche, au développement, à la vente, à l'intégration, à la revente ou à l'exploitation de capacités d'intrusion cyber disponibles sur le marché. Elle comprend notamment :

15.b.i. les développeurs ou fournisseurs de produits : les entités qui créent, développent, produisent ou vendent des capacités d'intrusion cyber disponibles sur le marché ;

15.b.ii. les intermédiaires : les entités qui servent de facilitateurs commerciaux ou technologiques entre l'offre et la demande de capacités d'intrusion cyber disponibles sur le marché, notamment les courtiers et les revendeurs (voir les définitions aux alinéas 15.d.i et 15.d.ii) ;

15.b.iii. les intégrateurs : les entités qui réalisent pour le compte de clients l'intégration technique de capacités d'intrusion cyber disponibles sur le marché ;

15.b.iv. le soutien opérationnel : les entités qui fournissent pour le compte de clients un soutien opérationnel pour les capacités d'intrusion cyber disponibles sur le marché ;

15.b.v. les investisseurs ou financiers : les entités et individus qui fournissent du capital, des crédits ou d'autres ressources financières à l'industrie de l'intrusion cyber, comme les fonds de capital-risque, les fonds de capital-investissement, les gestionnaires de grande fortune, les investisseurs de détail et les structures offshore.

15.c. L'accès non autorisé désigne le fait d'accéder sans en avoir le droit à tout ou partie d'un système informatique.

15.d. Les intermédiaires sont des entités ou des individus opérant au sein de la chaîne d'approvisionnement des capacités d'intrusion cyber disponibles sur le marché pour faciliter, permettre, ou soutenir le développement, la vente ou l'exploitation de capacités d'intrusion cyber disponibles sur le marché. Ils comprennent notamment :

15.d.i. les courtiers : les entités ou les individus qui facilitent à la fois la mise en contact de chercheurs et de clients entre eux ; l'acquisition, la revente et l'échange d'informations sur les vulnérabilités, les exploits ou les capacités d'intrusion cyber disponibles sur le marché entre les chercheurs et les clients ; et la mise en contact de chercheurs et de clients ;

15.d.ii. les revendeurs : les entités qui acquièrent ou qui reconditionnent des capacités d'intrusion cyber disponibles sur le marché à des fins de revente, de commercialisation ou de distribution à des utilisateurs finaux, soit directement, soit en qualité d'intermédiaire local d'acquisition ;

15.d.iii. les agents de vente : les entités qui fournissent des services de mise en relation ou de vente à des fournisseurs de capacités d'intrusion cyber disponibles sur le marché en l'échange d'une commission.

15.e. L'exploitation désigne le déploiement, l'usage ou la maintenance d'une capacité d'intrusion cyber disponible sur le marché. L'exploitation de capacités d'intrusion cyber disponibles sur le marché peut comprendre une infrastructure d'appui et inclure notamment :

15.e.i. des services d'accès à la demande : des capacités d'intrusion cyber disponibles sur le marché qui fournissent le vecteur d'accès permettant aux utilisateurs finaux d'accéder à des systèmes informatiques ;

15.e.ii. des services de capacité à la demande : des capacités d'intrusion cyber disponibles sur le marché qui développent, entretiennent et mettent à disposition des logiciels d'intrusion destinés à être utilisés contre des cibles pour le compte d'un client.

Section 4 : Lignes directrices

16. Nous, États, encourageons vivement l'industrie de l'intrusion cyber à mettre en œuvre et à suivre les présentes lignes directrices.

17. **Respect des dispositions réglementaires et des normes** – Responsabilité de veiller à ce que toutes les activités concernées soient menées de manière légale et responsable, conformément aux cadres juridiques nationaux et internationaux applicables. De plus, l'industrie de l'intrusion cyber ne doit pas vendre des capacités d'intrusion cyber disponibles sur le marché à des acteurs non étatiques irresponsables et illégitimes agissant en qualité d'utilisateurs finaux. Ce respect des dispositions réglementaires et des normes implique de :

17.a. Respecter les droits de l'Homme, en limitant le risque de violations graves des droits de l'Homme et en remédiant à ces violations lorsqu'elles surviennent, conformément aux Principes directeurs des Nations Unies. Cela s'applique aux incidences négatives sur les

droits de l'Homme qu'une entreprise peut avoir ou auxquelles elle peut contribuer par le biais de ses propres activités, ou qui peuvent découler directement de ses activités, produits ou services ou de ses relations commerciales.

17.b. Procéder à l'enregistrement des entreprises d'intrusion cyber dans le registre national des entreprises pertinent, le cas échéant, conformément au droit national applicable. Le cas échéant, les entités doivent s'assurer que leur enregistrement dans le registre est exact et transparent, en fournissant les informations spécifiques demandées par les autorités nationales (comme leur adresse et leur propriété effective). Nous attirons l'attention sur le fait qu'une restructuration, un changement de marque, un changement de juridiction ou des transferts d'intérêt ne suffisent pas à eux seuls pour rompre un lien avec une entité. Toute séparation d'une autre entité doit être démontrée par des éléments clairs et vérifiables, conformément au droit applicable.

17.c. Respecter les exigences nationales en matière de contrôle des exportations, des sanctions en la matière et des autres exigences de contrôle du commerce applicables aux technologies cyber à double usage, ainsi que les obligations juridiques nationales et internationales applicables, lors du développement, du transfert et de la vente de capacités d'intrusion cyber disponibles sur le marché. Cela devrait impliquer notamment de :

17.c.i. respecter toute la réglementation applicable en matière de contrôle des exportations, notamment en obtenant, lorsque cela est nécessaire, l'autorisation préalable des pouvoirs publics pour l'exportation et le transfert de capacités d'intrusion cyber disponibles sur le marché ;

17.c.ii. présenter l'ensemble de la structure organisationnelle d'une entité, y compris de ses filiales et de sa propriété effective, aux autorités compétentes lorsqu'elles en font la demande et lorsque l'autorité nationale compétente l'exige.

17.d. Appliquer la réglementation et les exigences nationales, régionales et internationales en matière de cybersécurité. Le cas échéant, selon l'entité, le produit et le modèle de distribution concerné, l'industrie de l'intrusion cyber doit mettre en œuvre des normes ou des mécanismes de contrôle des risques comme les normes ISO/IEC 27001 et 27002 (gestion de la sécurité de l'information) ou la norme ISO/IEC 15408 (évaluation de la cybersécurité). Le respect de ces normes limite les risques d'exploitation, renforce la confiance et favorise une gestion responsable des vulnérabilités.

17.e. Mettre en place des normes responsables au sein des entreprises. Ces normes doivent être approuvées au plus haut niveau de l'entreprise et intégrées dans les politiques et procédures opérationnelles. Elles doivent être communiquées à l'ensemble du personnel et peuvent, le cas échéant, faire l'objet d'une communication aux clients du secteur public, aux partenaires commerciaux et à d'autres parties concernées, sous réserve des restrictions de confidentialité, des restrictions contractuelles et des autres restrictions applicables relatives aux informations sensibles, sauf si cette communication externe risque d'entraîner la divulgation d'informations opérationnelles sensibles.

18. **Diligence requise** - Un processus continu et intégré visant à améliorer la transparence, qui évalue les activités menées par l'industrie de l'intrusion cyber pour repérer les incidences des entreprises sur les droits de l'Homme, prévenir ces incidences et en atténuer les effets, et rendre compte de la manière dont les entreprises y remédient. Cela implique de vérifier que les activités du personnel et des sous-traitants, des clients et des partenaires au sein de la chaîne de valeur ne favorisent pas les usages irresponsables. Cette vérification doit passer par une approche globale conforme aux Principes directeurs des Nations Unies. Les processus de diligence requise et d'évaluation des risques doivent prendre en compte les évolutions significatives des capacités concernées. Les entreprises doivent évaluer si ces évolutions augmentent significativement l'accessibilité, l'autonomie, l'extensibilité, la rapidité, la précision, l'adaptabilité ou les effets potentiels, ou si elles modifient les risques d'usages irresponsables ou de prolifération. Cela implique notamment de :

18.a. Créer un processus d'évaluation des risques relatifs aux prestataires au sein de la chaîne de valeur des capacités d'intrusion cyber disponibles sur le marché, notamment en recueillant des informations sur les fournisseurs, les prestataires et les sous-traitants potentiels, afin de fournir des données à l'appui d'une évaluation interne des risques concernant leurs pratiques en matière de cybersécurité, leur respect des droits de l'Homme et du droit international applicable et le risque de prolifération. Ce processus doit faire l'objet d'un examen et d'une mise à jour périodiques tout au long de la relation commerciale. Parmi les informations sur les prestataires peuvent notamment figurer les éléments suivants :

18.a.i. Nom, numéro d'immatriculation, numéro d'identification fiscale, adresse, coordonnées et date d'immatriculation.

18.a.ii. Informations sur la structure de propriété, notamment les bénéficiaires effectifs, les investisseurs et la direction, ces informations étant vérifiées, dans la mesure du possible, auprès de sources indépendantes.

18.a.iii. Informations sur les activités commerciales, notamment les territoires dans lesquels le prestataire est autorisé à exercer son activité.

18.a.iv. Nomenclature des logiciels ou évaluation des pratiques en matière de cybersécurité, lorsque les produits fournis risquent d'entraîner un risque de cybersécurité.

18.b. Lorsqu'il sollicite une autorisation pour la commercialisation, la vente, l'exportation et le transfert à l'international de capacités d'intrusion cyber disponibles sur le marché visées par la réglementation en matière de contrôle des exportations applicable à l'entreprise et à la transaction concernées, l'industrie de l'intrusion cyber doit recueillir les informations utiles concernant les clients et les utilisateurs finaux existants ou potentiels, pour évaluer si ces capacités sont ou pourraient être destinées, en tout ou en partie, à être utilisées dans le cadre d'une répression interne, notamment en combinaison avec des activités transfrontalières visant à faire taire la dissidence ou à exercer des représailles contre des personnes à l'étranger, ou si ces capacités sont ou pourraient être utilisées par des personnes ou des entités responsables ou complices d'abus graves, de violations des droits de l'Homme ou de violations du droit international humanitaire. Les informations

sur les clients doivent inclure les éléments visés par la réglementation en matière de contrôle des exportations, notamment :

18.b.i. Les informations sur l'utilisateur final (entité, rôle, responsabilité et mandat). Lorsqu'un client est une institution publique, la diligence requise doit tenir compte des mandats classifiés et des considérations de sécurité. La diligence requise ne doit pas imposer de divulguer des informations opérationnelles, des objectifs opérationnels ou des informations classifiées.

18.b.ii. Le cadre réglementaire et sa mise en œuvre pratique dans le territoire dont dépend le client, notamment des éléments permettant de déterminer si ce cadre permet une supervision indépendante des activités de cybersurveillance et d'intrusion cyber.

18.b.iii. Les pratiques en matière de sécurité de l'information, évaluées au regard des risques de prolifération. Lorsque le client est une institution publique, la diligence requise doit tenir compte des mandats classifiés et des restrictions de confidentialité, des restrictions contractuelles et des autres restrictions relatives aux informations sensibles, ainsi que du secret d'enquête et du secret judiciaire, mais elle doit permettre d'évaluer le risque d'incidences préjudiciables sur les droits de l'Homme ou de violations du droit international.

18.b.iv. Des éléments permettant de déterminer si le client a l'intention de servir d'intermédiaire, c'est-à-dire de procéder à une revente ou d'agir comme courtier.

18.c. Instaurer un processus formalisé d'identification et de vérification du personnel et des sous-traitants, prévoyant notamment l'obligation de recueillir des informations de base sur les candidats à l'embauche, les salariés et les sous-traitants, afin d'étayer les décisions de recrutement au regard des risques de prolifération, en tenant notamment compte de toute participation antérieure à des activités de prolifération. Ce processus doit être conforme à la législation applicable en matière de respect de la vie privée, de protection des données et de droit du travail, et il doit reposer sur des informations accessibles qui peuvent être vérifiées de manière raisonnable et légale. Ce processus peut notamment impliquer de :

18.c.i. Vérifier tout potentiel cumul d'emplois, tout autre conflit d'intérêt et, pour les cadres supérieurs et les sous-traitants, toute association antérieure avec des entités condamnées ou toute allégation d'activités irresponsables. Le cumul d'emplois ne saurait être considéré en soi comme la preuve d'un risque de prolifération ou d'usage irresponsable.

18.c.ii. Procéder à un réexamen périodique des salariés ayant accès à des capacités sensibles, notamment suite à un changement de poste ou à un constat défavorable.

18.d. Établir des processus d'évaluation des risques, les étayer et les mettre en application pour fournir des données à l'appui de la vérification a) des fournisseurs, prestataires et sous-traitants potentiels, b) des clients potentiels, et c) des candidats à l'embauche. Cela doit se faire dans le respect des législations applicables en matière de respect de la vie privée, de protection des données et de droit du travail. Ce processus doit déterminer les

risques au regard de normes établies concernant les activités et les usages irresponsables, notamment les incidences préjudiciables sur les droits de l'Homme, en tenant compte de la gravité et de la probabilité de ces incidences.

18.e. Veiller à ce que la diligence requise soit un processus continu intégré au cycle de vie des capacités d'intrusion cyber disponibles sur le marché et à l'industrie de l'intrusion cyber, appliqué aux clients et intégré à la chaîne de valeur et d'approvisionnement dans son ensemble. Dans les entreprises spécialisées en intrusion cyber, les processus de diligence requise doivent être supervisés par les structures de gouvernance au plus haut niveau de l'entreprise, pour autant qu'elles existent, et s'appuyer sur des renseignements externes fiables et vérifiés concernant les menaces, ainsi que sur des allégations crédibles d'abus. Les arrangements contractuels avec les clients doivent inclure des clauses de « refus » et de « résiliation » (voir 18.f.).

18.f. Veiller à ce que les opérations commerciales concernées soient suspendues et à ce qu'aucune vente ni aucun transfert n'ait lieu et à ce qu'aucune assistance ne soit fournie lorsque des processus d'évaluation des risques, internes ou externes, crédibles et étayés, démontrent qu'il existe soit un risque grave d'usage irresponsable, soit qu'un usage irresponsable, un abus grave ou des violations des droits de l'Homme ont déjà eu lieu. Toute autre suspension ou cessation, ou toute reprise des opérations commerciales, doit être décidée en fonction des résultats de cette évaluation et rester conforme à la législation applicable et au cadre contractuel pertinent. Les contrats doivent être rédigés de manière à ce que la législation applicable et le cadre contractuel n'empêchent pas la suspension ou la résiliation du contrat lorsqu'il existe un risque élevé d'usage irresponsable.

19. **Gestion des risques** - Agir avec précision pour limiter les risques, notamment en matière de droits de l'Homme, que représente un usage irresponsable, délibéré ou non des capacités d'intrusion cyber disponibles sur le marché par les clients, les fournisseurs, les chaînes d'approvisionnement, les salariés ou les sous-traitants, et en atténuer les conséquences. Cela implique notamment de :

19.a. Mettre en œuvre des contrôles techniques concernant l'accès à l'information. Cela implique notamment de :

19.a.i. Garantir la mise en place, en tant que de besoin, du chiffrement, de l'authentification et d'autres mesures utiles à la sécurité de l'information.

19.a.ii. Cloisonner les structures pour les équipes chargées des capacités en interne, notamment celles dédiées à la recherche de vulnérabilités et au développement d'exploits, ainsi que pour l'accès des opérateurs à ces capacités.

19.a.iii. Lorsque cela est pertinent pour des raisons de sécurité, restreindre l'accès des chercheurs ou des opérateurs aux activités des autres équipes, sur la base du besoin d'en connaître ;

19.a.iv. Assurer la vérification des personnes chargées de la supervision des produits, des services ou des éléments technologiques ou commerciaux essentiels, pour limiter le risque

d'usage, de divulgation ou de transfert d'informations couvertes par la propriété exclusive, que cela soit intentionnel ou non.

19.a.v. Cloisonner l'accès pour les clients qui utilisent les produits et services.

19.b. Le cas échéant, veiller à ce que les activités menées en utilisant des capacités d'intrusion cyber disponibles sur le marché soient nécessaires, légales, proportionnelles aux besoins, tels que défini par les autorités compétentes, et conçues pour être exécutées avec précision, selon les modalités suivantes :

19.b.i. Veiller à la minimisation des données, en renforçant les capacités nécessaires à la conduite d'opérations calibrées et en tenant compte du contexte général, du risque de conséquences imprévues et du risque de répercussions indiscriminées sur un nombre important de personnes.

19.b.ii. Limiter les incidences préjudiciables sur les personnes et les tiers, en renforçant les capacités ou en veillant à ce qu'elles soient utilisées dans le cadre d'opérations nécessaires, légales, proportionnelles aux besoins et non discriminatoires, en se fondant sur une compréhension approfondie de l'environnement cyber dans lequel ces capacités seront utilisées, de manière sécurisée et pour une durée limitée.

19.b.iii. Veiller à ce que les systèmes soient conçus pour faciliter le respect des cadres juridiques nationaux en assurant une gestion appropriée des informations en lien avec les autorisations régissant l'usage des capacités d'intrusion cyber disponibles sur le marché.

19.c. Veiller à ce que les salariés soient juridiquement contraints de prévenir tout usage irresponsable ou toute prolifération des capacités d'intrusion cyber disponibles sur le marché par le personnel, par :

19.c.i. Des accords de confidentialité, qui ne doivent pas entraver la coopération avec les autorités compétentes, la protection des lanceurs d'alerte, et le signalement de cas présumés de violations juridiques ou d'incidences préjudiciables sur les droits de l'Homme, sans préjudice des obligations juridiques relatives à la protection des informations classifiées.

19.c.ii. Des règles interdisant la vente ou l'exploitation de capacités d'intrusion cyber disponibles sur le marché à titre individuel, ainsi que des procédures claires pour transmettre les dossiers, le cas échéant, aux services de police et de justice.

19.c.iii. Des règles pour interdire ou restreindre les activités de recherche de vulnérabilités et de développement d'exploits en dehors du travail au sein de l'entreprise sans l'autorisation ou l'accord préalable de l'employeur.

19.d. Veiller à ce que les clients et les fournisseurs soient juridiquement contraints de prévenir tout usage irresponsable ou toute prolifération des capacités d'intrusion cyber disponibles sur le marché, selon les modalités suivantes :

19.d.i. Les contrats avec les clients prévoient clairement un engagement de la part du client à n'utiliser les capacités d'intrusion cyber disponibles sur le marché qu'avec l'autorisation des autorités compétentes.

19.d.ii. Des dispositions contractuelles interdisent le transfert de capacités d'intrusion cyber disponibles sur le marché à d'autres parties que celles autorisées.

19.d.iii. Le cas échéant, des dispositions contractuelles autorisent le fournisseur ou le prestataire à mettre un terme à l'accès aux capacités d'intrusion cyber disponibles sur le marché.

19.d.iv. Des restrictions contractuelles concernant la revente, le transfert ou la sous-licence doivent s'appliquer de manière équitable à tous les acheteurs, intermédiaires et utilisateurs ultérieurs.

19.e. Mettre en place des mesures de formation continue et de sensibilisation à l'intention du personnel, des sous-traitants et des clients au sujet des droits de l'Homme concernés, ou de toute autre norme applicable en matière de droit international et de cybersécurité à l'égard desquelles ils seront tenus responsables, en tenant notamment compte des mises à jour découlant des processus de diligence requise et d'évaluation des risques décrits dans les présentes lignes directrices. Cela inclut notamment la formation aux procédures prévues au sein de l'entreprise pour faire remonter des cas présumés d'activité irresponsable.

19.f. Entretenir des relations transparentes et ouvertes avec les clients qui se procurent des capacités d'intrusion cyber disponibles sur le marché, dans la mesure du possible, tout en respectant les informations sensibles (par exemple, fournir des détails sur les composants des logiciels dans une nomenclature des logiciels, comprendre les dépendances techniques et communiquer sur ce sujet, et définir les risques d'activités irresponsables).

19.g. Les obligations en matière de confidentialité et la protection des informations couvertes par la propriété exclusive ne doit pas empêcher les autorités judiciaires compétentes de vérifier l'intégrité, la fiabilité et la traçabilité des informations concernées, lorsque le droit national l'exige. L'industrie de l'intrusion cyber ne doit pas empêcher les parties et leurs conseillers techniques respectifs d'exercer leurs droits.

20. **Suivre le respect des obligations** - Surveiller les activités de la chaîne d'approvisionnement et les activités finales grâce à un suivi continu pour garantir le respect des normes et l'adoption de réponses appropriées en cas de non-respect des normes en matière d'activités responsables. Il s'agit notamment de :

20.a. Mettre en place un suivi continu de l'accès aux capacités d'intrusion cyber disponibles sur le marché, le cas échéant, notamment selon les modalités suivantes :

20.a.i. Établir un cadre solide pour surveiller la gestion de l'accès, conformément aux normes relatives aux activités responsables, notamment les droits de l'Homme et d'autres normes applicables en matière de droit international et de cybersécurité.

20.a.ii. Instaurer en interne des journaux du système immuables concernant le volet entreprise pour comprendre qui au sein de l'entreprise modifie les capacités ou les composants ou y accède, et à quel moment.

20.a.iii. Allouer des ressources suffisantes pour surveiller des indicateurs externes fiables, notamment les renseignements sur les menaces, les études indépendantes en matière de sécurité, la télémétrie internet et les signalements d'incidents, ainsi que pour recenser et traiter les allégations publiques ou les preuves d'un potentiel usage irresponsable, afin de mener rapidement une enquête. Cela suppose notamment de déclarer de manière publique qu'une enquête a eu lieu, dans le respect de toutes les obligations de confidentialité.

20.a.iv. Le suivi doit prendre en compte les évolutions des technologies émergentes qui peuvent modifier considérablement l'efficacité, l'accessibilité ou les potentiels abus concernant les capacités d'intrusion cyber disponibles sur le marché ou permettre de contourner les garanties en place.

20.b. Réaliser une vérification régulière des clients, des salariés, des sous-traitants, des prestataires et des opérateurs, au regard des normes en matière d'activités irresponsables, notamment :

20.b.i. Suivre les incidences négatives des activités. Cela doit se fonder sur des indicateurs qualitatifs et quantitatifs et s'appuyer sur le retour d'expérience de sources internes et externes, ainsi que sur les échanges avec ces sources, notamment les organisations de la société civile, les chercheurs, les organisations de soutien aux victimes et les représentants de parties prenantes touchées par l'usage irresponsable de ces outils.

20.b.ii. Sous réserve des mandats classifiés, des considérations de sensibilité, du secret d'enquête et du secret judiciaire, ainsi que des restrictions contractuelles, faire régulièrement appel à un tiers indépendant disposant, le cas échéant, d'une habilitation de sécurité étatique appropriée, comme par exemple des auditeurs agréés, des cabinets externes spécialisés dans la conformité ou des organisations non gouvernementales reconnues ; ils seront chargés d'assurer un contrôle impartial, de mener des évaluations indépendantes et de faire part de leurs recommandations. Pour ce faire, les entreprises spécialisées en intrusion cyber peuvent établir un mécanisme de surveillance indépendant en matière d'éthique et de droits de l'Homme, qui soit proportionnel à leur taille, leur structure et leur profil de risques, pour passer en revue leurs activités à haut risque. L'accès à des informations judiciaires, d'enquête, sensibles ou classifiées ne peut être accordé sans l'autorisation des autorités nationales.

20.c. Établir un processus de signalement et le rendre public pour permettre aux parties prenantes concernées de signaler des activités ou des usages irresponsables et clarifier les conséquences qu'encourt l'auteur d'actes irresponsables.

20.c.i. Des allégations crédibles d'incidences sur les droits de l'Homme doivent faire l'objet d'une enquête rapide, interne, impartiale et, le cas échéant, indépendante, sous réserve des mandats classifiés, des considérations de sensibilité et des restrictions contractuelles.

Ces processus doivent s'accompagner de procédures pour enquêter sur les cas présumés d'activités ou d'usages irresponsables et, si nécessaire, de mesures de suivi, comme une nouvelle formation, un renforcement de la surveillance, des vérifications ponctuelles par des auditeurs, une restriction de l'accès, la fin du contrat ou son non-renouvellement, ou d'autres actions appropriées.

20.c.ii. En plus du processus de signalement, l'industrie de l'intrusion cyber doit envisager de définir un processus pour répondre aux allégations d'activités ou d'usages irresponsables. Lorsque des informations crédibles laissent présumer une activité ou un usage irresponsable, les participants doivent mener un examen rapide, étayé et fondé sur les risques, conserver, dans la mesure du possible, les registres et journaux pertinents, et mettre en œuvre des mesures provisoires appropriées, comme le renforcement de la surveillance, le cas échéant, des restrictions d'utilisation ou la suspension des mises à jour ou de l'assistance.

20.c.iii. L'industrie de l'intrusion cyber doit signaler toute activité illégale présumée à l'autorité publique compétente lorsque la législation applicable l'exige et le permet, et elle doit coopérer avec les autorités judiciaires compétentes conformément à la législation applicable et aux décisions de justice légitimes, notamment en conservant les preuves et par le biais des voies d'entraide judiciaire, dans le cadre des enquêtes relatives à l'utilisation illégale des capacités d'intrusion cyber disponibles sur le marché. Le droit de ne pas s'incriminer soi-même dans le cadre des procédures pénales n'est pas remis en cause.

20.c.iv. L'industrie de l'intrusion cyber doit envisager de prendre des mesures visant à offrir des procédures de réparation ou des voies de recours judiciaires et extrajudiciaires aux parties prenantes concernées touchées par des atteintes aux droits de l'Homme qu'elle a directement causées ou auxquelles elle a contribué. Sans préjudice des voies de recours prévues par le droit national, les procédures de réparation et les voies de recours doivent être conçues et mises en œuvre avec la participation effective des détenteurs de droits concernés ou de leurs représentants légitimes, et elles doivent tenir compte de leurs besoins, de leurs points de vue et de leurs préférences.