RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 10 septembre 2024
Version : 0.1
Nombre de pages : 27

ORGANISMES DE RECHERCHE ET THINK TANKS

ÉTAT DE LA MENACE INFORMATIQUE

TLP:CLEAR

PAP:CLEAR

Table des matières

1 SYNTHÈSE

Le secteur de la recherche et des *think tanks* couvre un **périmètre large et hétéroclite**. Celui-ci comprend des entités publiques et privées de toute nature, dont certaines peuvent être des fondations, des organisations internationales ou des associations.

Ces entités sont ciblées par un vaste panel d'acteurs offensifs, ayant des objectifs d'espionnage stratégique ou industriel, mais également de déstabilisation, voire des objectifs lucratifs.

Les *think tanks* et organismes de recherche travaillant sur des thématiques liées aux questions stratégiques et de défense sont particulièrement ciblés par des attaquants en lien avec des États et cherchant à mener des **attaques à but d'espionnage**. Parmi ces derniers, les groupes d'attaquants liés à la Russie, à la Chine, à la Corée du Nord et à l'Iran représentent une menace pérenne. Le **contexte de l'invasion de l'Ukraine par la Russie** renforce encore ce ciblage avéré depuis des années. Les attaquants cherchent, par ces compromissions, à **connaître et anticiper les décisions stratégiques des États et des organisations internationales**, en ciblant des entités (les organismes de recherche et *think tanks*) étroitement liées et parfois commanditées par les États pour leur fournir des éléments de réflexion et de positionnement.

Les **organismes de recherche scientifique civils et militaires** sont également ciblés par des campagnes, parfois massives, cherchant à **exfiltrer des données scientifiques, techniques ou industrielles permettant d'obtenir des avantages compétitifs**. Les attaques connues de l'ANSSI comprennent notamment des compromissions liées à des modes opératoires réputés chinois ou nord-coréens.

La **menace à but de déstabilisation** peut également toucher les organismes de recherche et les *think tanks*, notamment dans le cadre de la guerre en Ukraine où ces entités sont ciblées de façon opportuniste dans le cadre de campagnes très réactives à l'actualité géopolitique.

Enfin, les **cybercriminels ayant des motivations lucratives** ciblent également, de façon opportuniste, ces entités pour y déployer des rançongiciels ou chercher à exfiltrer des données personnelles pouvant être ensuite revendues.

Cet État de la menace ciblant les organismes de recherche et les *think tanks* comporte également un volet dédié aux recommandations émises par l'ANSSI pour améliorer le niveau de sécurité de ces entités. **Ces recommandations ne sont pas exhaustives et doivent être adaptées et complétées dans le contexte de chaque entité.** En particulier, les entités concernées doivent s'assurer de répondre aux recommandations spécifiques à la protection numérique du potentiel scientifique et technique de la Nation [1].

1. SGDSN - ANSSI, Protection numérique du potentiel scientifique et technique de la Nation. 2018 [1]

2 PÉRIMÈTRE DU SECTEUR ET ENCADREMENT DE LA RECHERCHE AU NIVEAU RÉGLEMENTAIRE, NORMATIF ET CONTRACTUEL

2.1 Périmètre des entités du secteur de la recherche et des *think tanks*

L'analyse de la menace ciblant les organismes de recherche et les *think tanks* couvre un périmètre large. Celui-ci comprend à la fois des entités publiques et privées, des associations, des fondations ou encore des organisations internationales.

Le secteur de la recherche et de l'innovation se caractérise par une très grande diversité d'opérateurs : des laboratoires de recherche académique ou de recherche et développement du monde de l'industrie [2], aux très grandes infrastructures de recherche et aux centres de calcul intensif, en passant par les organismes d'accompagnement de la recherche, de valorisation et de transfert de technologie. L'ensemble de ces acteurs, communément appelé « la communauté scientifique », se réunit en consortium de recherche interdisciplinaire. Il travaille et contribue à l'augmentation des savoirs et à l'amélioration des connaissances et des techniques, méthodologies et théories dans tous les domaines scientifiques.

La recherche se déploie ainsi dans des milliers d'unités, de laboratoires R&D et dans des programmes transversaux et interdisciplinaires de toutes tailles, dont les activités peuvent couvrir tous les champs disciplinaires des sciences (tels que les mathématiques, la biologie, la santé, l'informatique, la physique ou la chimie), et des sciences humaines et sociales (que sont notamment le droit, l'économie, l'histoire, la science politique ou la sociologie). Les financements des activités de recherche peuvent provenir de la sphère publique (l'Union Européenne, l'État, les collectivités territoriales, les organismes de l'enseignement supérieur et de la recherche (« ESR ») et les agences de financement publiques) autant que de la sphère privée (les entreprises et le secteur privé sans but lucratif).

Cet état de la menace se concentre principalement sur les entités publiques et privées pour lesquelles les activités de recherche représentent le cœur d'activité.

À la lisière de cette large communauté scientifique se situent également les acteurs évoluant dans les *think tanks*, qui contribuent aux analyses des politiques publiques sociétales. Les *think tanks* sont le plus souvent des structures de droit privé. Ils ont pour objectif de produire des recherches directement utilisables par le politique. Ils sont parfois financés à cette fin par des organismes étatiques, notamment dans le domaine des relations internationales et stratégiques. Les chercheurs rattachés aux principaux *think tanks* occupent une place et une influence parfois importantes dans la prise de décision stratégique de l'État : ils sont en effet à l'interface du monde de la recherche et du monde politique, en lien avec des experts de nombreux pays autant qu'avec des administrations nationales parfois peu ouvertes sur l'extérieur. De récentes évolutions montrent une volonté de certaines universités et grandes écoles de se doter de *think tanks* dédiés.

2. Communément appelés départements ou laboratoires de « R&D ».

2.2 Encadrement de la recherche au niveau réglementaire, normatif et contractuel

Les organismes de recherche peuvent être de droit privé ou de droit public et agissent comme composantes ou partenaires de regroupements universitaires ou pôles universitaires d'innovation. L'étendue de leurs sujets de recherches est plus vaste. Ils peuvent traiter à la fois de questions stratégiques, de recherche biomédicale ou nucléaire, comme de thématiques de recherche fondamentale très diverses.

Les organismes de recherche peuvent être assujettis à tous les textes relatifs au cadre réglementaire de la sécurité du numérique qui englobe deux champs d'application : la sécurité des systèmes d'information et la confiance numérique. Certains peuvent relever de régimes de protection des informations sensibles et à diffusion restreinte, et être inclus dans le dispositif de protection du patrimoine scientifique et technique (PPST) définissant les exigences applicables aux zones à régime restrictif (ZRR) et/ou dans le périmètre de l'instruction interministérielle 901 qui définit les exigences applicables aux systèmes d'information sensibles ou « Diffusion restreinte » [1]. D'autres établissements peuvent relever de la protection des systèmes d'information des OIV ou des OSE et donc de la loi de programmation militaire 2014-2019 ou de la directive NIS (prochainement remplacée par la directive NIS2). Les établissements publics doivent, en outre, répondre à la politique de protection des systèmes d'information de l'État.

Tous ces établissements doivent également respecter la réglementation en vigueur concernant la protection des données à caractère personnel. En outre, le secteur de la recherche est engagé dans un système de normes et de standards internationaux concernant l'intégrité scientifique et l'éthique de la recherche. Ces normes sont autant soutenues par les politiques institutionnelles que par le système de financement des projets de recherche : leur bon respect s'inscrit ainsi dans les contrats d'engagement et de financement conclus avec les porteurs de projet. Ces clauses contractuelles conditionnent autant l'allocation des fonds que l'évaluation des protocoles de la recherche et de l'intégrité scientifique des chercheurs.

Cet État de la menace s'appuie sur des incidents observés ou traités par l'ANSSI, mais également sur des publications d'éditeurs de sécurité traitant des incidents auprès de nombreuses entités dans le monde entier. Il ne constitue pas un recensement exhaustif des attaques observées, mais donne une vision représentative et analytique de la menace informatique touchant les organismes de recherche et les *think tanks*. Les preuves de concept et menaces envisagées mais non encore observées par l'ANSSI ne font pas partie du périmètre d'étude. Ce document se concentre particulièrement sur les menaces d'origine cyber affectant les activités de recherche et d'innovation critique ainsi que les *think tanks*. Il écarte donc de son analyse la menace ciblant les missions d'enseignement des établissements de l'ESR.

Les recommandations associées à cet État de la menace visent à éclairer les organismes de recherche et les *think tanks* ainsi que leurs éventuels prestataires, afin de bâtir une défense et de se prémunir des menaces qui les affectent. Ces recommandations ne sont pas exhaustives et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel du système d'information considéré. En particulier, les entités concernées doivent s'assurer de répondre aux recommandations spécifiques à la protection numérique du potentiel scientifique et technique de la Nation [3] et de prendre en compte les exigences relatives à leurs cadres légaux et réglementaires spécifiques, qui ne sont pas détaillés de façon exhaustive dans cet État de la menace.

3. SGDSN - ANSSI, Protection numérique du potentiel scientifique et technique de la Nation. 2018 [1]

3 ATTAQUES À DES FINS D'ESPIONNAGE

3.1 Espionnage stratégique : ciblage de *think tanks* et d'organismes de recherche en relations internationales

Les *think tanks* et les centres de recherches en relations internationales et géopolitiques travaillent régulièrement en lien avec des entités publiques dans le domaine de la défense, des relations internationales, de la diplomatie et des politiques publiques. À ce titre, ils sont fréquemment ciblés par des attaquants liés aux intérêts stratégiques d'États qui cherchent à collecter des renseignements. Les chercheurs travaillant dans ces organisations sont détenteurs d'une expertise de haut niveau et occupent parfois des postes stratégiques dans des structures privées ou publiques, voire gouvernementales. Cette expertise constitue en soi une source d'intérêt pour les États adverses. En outre, par les projets qu'ils mènent en lien ou pour le compte d'entités publiques parfois sensibles, ils peuvent être ciblés dans l'objectif d'accéder à des informations protégées.

Ce positionnement explique le *tempo* élevé du ciblage [4] de ces entités et la variété des groupes d'attaquants qui pratiquent ces compromissions informatiques à but d'espionnage.

3.1.1 Attaques menées au moyen de modes opératoires d'attaque réputés russes

Les *think tanks* et organismes de recherche français et occidentaux, spécialisés sur les questions de défense et relations internationales, sont des cibles régulières des attaquants réputés liés aux intérêts de la Russie.

Ainsi, l'ANSSI a traité en 2023 la compromission d'un *think tank* travaillant sur des sujets d'intérêt stratégique et militaire. Plusieurs comptes de messagerie de personnels dirigeants ainsi que l'environnement *Cloud* de l'entité ont été compromis, permettant aux attaquants d'accéder à des informations d'intérêt stratégique et de se latéraliser vers d'autres entités, par le biais des relations d'approbation entre environnements *Active Directory*. Les traces d'outils employés par les attaquants ont permis de rattacher cette compromission, qui remonterait au moins à 2021, au mode opératoire d'attaque (MOA) APT28.

L'emploi du MOA APT28, lié en sources ouvertes et publiquement associé par l'Union européenne et ses États membres au renseignement militaire russe (GRU), confirme l'intérêt de celui-ci pour le ciblage d'entités liées au domaine de la défense et des intérêts stratégiques occidentaux, parmi lesquelles les *think tanks* traitant de sujets stratégiques [2].

Ce même *think tank* a été également compromis, dans un but probable d'espionnage, par un MOA réputé lié aux intérêts stratégiques chinois qui a pu se connecter à certains postes de travail et installer des outils malveillants sur le système d'information de la victime. Les investigations ont révélé d'autres compromissions, qui n'ont pu être rattachées à des modes opératoires identifiés.

4. Dans l'ensemble de cet État de la menace, le terme « ciblage » est employé pour décrire une tentative d'attaque (par exemple l'envoi d'un courriel d'hameçonnage) ou des actions réalisées en amont d'une compromission. Les termes « attaque » ou « compromission » sont employés pour décrire une action offensive ayant mené à un effet concret sur la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données présentes sur le système d'information.

Commentaire : la compromission d'un même think tank, au cours de la même période, par le biais d'au moins deux MOA réputés respectivement russe et chinois démontre le fort intérêt que représente cette entité pour des attaquants recherchant des informations stratégiques. Les travaux effectués par cette entité dans le cadre de commandes publiques peuvent être ciblés par les attaquants, qui tirent profit d'un niveau de sécurité inférieur aux commanditaires de ces travaux pour les compromettre et accéder à des données d'intérêt.

Le MOA APT28 a été impliqué dans plusieurs autres compromissions de *think tanks* français ou occidentaux liés aux questions stratégiques et militaires, notamment depuis 2022.

Ainsi, en avril 2017 l'OTAN Joint Air Power Competence Center situé en Allemagne aurait été compromis par un ressortissant russe qui aurait installé un code malveillant ayant des fonctions d'enregistrement de frappes au clavier (*keylogger*) et de capture d'écran sur plusieurs ordinateurs de ce *think tank* de l'OTAN. Les autorités des États-Unis d'Amérique ont émis un mandat d'arrêt et accusent le ressortissant russe Nikolaj Kozachek d'avoir installé ce maliciel et d'être un opérateur du MOA APT28 [3].

En 2022, l'ANSSI a eu connaissance du ciblage d'un autre *think tank* français travaillant sur des thématiques stratégiques et de défense par le biais du MOA APT28.

En 2023 l'ANSSI a eu connaissance d'une campagne d'hameçonnage ciblé à l'encontre de plusieurs chercheurs d'un autre *think tank* français travaillant sur des thématiques stratégiques par le biais du MOA APT28. Les opérateurs du MOA cherchaient à obtenir les identifiants personnels des chercheurs ciblés.

En 2023, un *think tank* français plus confidentiel a été ciblé par des campagnes d'hameçonnage reliées par l'ANSSI et un de ses partenaires aux MOA réputés liés à la Russie APT28 et Winter Vivern [5].

Commentaire : ces campagnes d'attaques menées au moyen du MOA APT28 montrent une persistance du ciblage des think tanks. Dans un contexte de tensions grandissantes entre la Russie et les pays membres de l'OTAN, notamment après le début du conflit mené par la Russie en Ukraine en 2014, ce secteur représente un intérêt constant pour des attaquants cherchant des informations stratégiques sur les sujets géopolitiques et de défense. La généralisation du conflit en Ukraine depuis l'invasion russe de février 2022 laisse envisager la poursuite d'une activité soutenue d'espionnage des organismes de recherche et think tanks travaillant sur les questions géopolitiques et stratégiques par des attaquants répondant aux intérêts du gouvernement russe.

Ces campagnes doivent cependant être comprises dans une victimologie plus large associée à ce mode opératoire, qui cible de façon récurrente et étendue le secteur de la défense dans les pays occidentaux dans un objectif d'espionnage.

D'autres modes opératoires d'attaque ont été employés pour cibler des *think tanks* au profit des intérêts stratégiques russes.

Le MOA réputé lié aux intérêts russes Callisto (également connu sous le nom de Star Blizzard), attribué publiquement par le NCSC-UK et ses partenaires des Five Eyes [6] au 18e centre du FSB [4], aurait également été activement employé en 2022 et 2023 pour cibler des *think tanks*, des ONG et des entités du secteur de la défense aux États-Unis et en Europe (notamment en Belgique, aux Pays-Bas et en Grande-Bretagne), afin de collecter des identifiants et mots de passe valides. Un rapport de l'éditeur Microsoft mentionne en décembre 2023 un ciblage de *think tanks*

5. Le mode opératoire d'attaque Winter Vivern est également documenté par le CERT-UA sous le nom de UAC-0114.

6. Les « Five Eyes » sont le nom donné à la coopération menée par les services de renseignement des États-Unis d'Amérique, du Canada, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande.

et d'institutions universitaires et de recherche par le biais de campagnes d'hameçonnage par courriel, cherchant à amener les cibles à renseigner leurs identifiants et mots de passe sur une interface de connexion usurpant un portail de gestion de subventions américain [5].

En 2022, l'ANSSI a également eu connaissance du ciblage d'un autre *think tank* français de premier plan par un autre MOA réputé lié aux intérêts russes. Ce ciblage ne semble pas avoir été suivi d'une compromission effective.

3.1.2 Attaques menées au moyen de modes opératoires d'attaque réputés nord-coréens

La Corée du Nord, soumise à de nombreuses sanctions internationales, cherche à assurer son indépendance stratégique par la maîtrise des technologies nucléaires et d'autres technologies militaires ou civiles à double usage.

À ce titre, de nombreuses campagnes liées à des modes opératoires d'attaque réputés nord-coréens ont été documentées ces dernières années, ciblant des institutions ou des chercheurs travaillant sur les questions de non-prolifération nucléaire. Ceux-ci sont en effet susceptibles d'orienter d'éventuelles prises ou retraits de sanctions internationales touchant la Corée du Nord sur ces sujets.

En juin 2023, l'ANSSI a été informée qu'un haut cadre d'un *think tank* français dédié aux questions stratégiques aurait fait l'objet d'un ciblage par hameçonnage opéré par au moyen du MOA réputé lié aux intérêts nord-coréens Kimsuky. Ce ciblage correspondrait à une campagne décrite par l'éditeur de sécurité SentinelLabs et aurait pour objectifs le vol d'identifiants et de mots de passe, ainsi que l'installation de code malveillant, en conduisant la cible à télécharger un document présenté comme un article à relire envoyé par un journaliste spécialiste de la Corée du Nord. SentinelLabs a mentionné dans son rapport le ciblage de personnels du Korea Risk Group, un *think tank* spécialisé dans les questions liées à la Corée du Nord, et considère que ce ciblage fait partie d'une campagne plus large concernant des *think tanks*, organismes de recherche universitaires et organisations gouvernementales en Europe, en Asie et aux États-Unis [6].

Confirmant ce ciblage important des organismes de recherche et *think tanks* travaillant sur des questions stratégiques et liées aux problématiques de prolifération nucléaire, le FBI, le Département d'État américain ainsi que plusieurs agences américaines et sud-coréennes ont publié le 1er juin 2023 une note conjointe pour mettre en lumière l'utilisation des réseaux sociaux par des attaquants nord-coréens afin de compromettre des organismes de recherche et *think tanks*. Évoquant plusieurs MOA réputés liés aux services du Bureau Général de Reconnaissance nord-coréen, en particulier le MOA Kimsuky, cette note relève que les opérateurs de ces MOA usurpent sur ces plateformes l'identité de journalistes, de recruteurs et d'universitaires pour mener leurs campagnes d'hameçonnage ciblé [7].

Commentaire : le ciblage d'organismes de recherche et de think tanks travaillant sur des thématiques stratégiques liées à la Corée du Nord, et particulièrement sur la question de la non-prolifération nucléaire, semble persistant et massif. Le secteur est ciblé dans le cadre de campagnes plus larges qui cherchent également à compromettre des entités du secteur gouvernemental. Si les États-Unis et la Corée du Sud semblent être les pays les plus ciblés par ces attaques, les chercheurs français travaillant sur ces thématiques doivent être considérés également comme des cibles potentielles. L'utilisation de techniques d'hameçonnage ciblé très crédibles et d'avatars sur les réseaux sociaux par des opérateurs de MOA nord-coréens est une pratique déjà documentée pour d'autres secteurs. Elle mérite une attention particulière pour des chercheurs amenés à échanger régulièrement avec de nouveaux contacts.

3.1.3 Attaques menées au moyen de modes opératoires d'attaque réputés iraniens

Le régime iranien, sous sanctions internationales et engagé dans de multiples rivalités géopolitiques, cherche à assurer sa stabilité en exerçant notamment une surveillance appuyée sur les dissidents et sur les chercheurs en relations internationales et spécialistes du Moyen-Orient. Pour cela, ses services emploient des MOA dont certains sont particulièrement actifs dans le ciblage de la communauté scientifique.

Depuis au moins 2021, plusieurs campagnes d'hameçonnage ciblant des spécialistes occidentaux du Moyen-Orient ont été associées au MOA Charming Kitten par des éditeurs de sécurité. Ces experts ont été ciblés de façon individuelle, *via* des invitations à des conférences ou des demandes d'interviews. Les opérateurs du MOA ont usurpé les identités de journalistes ou de chercheurs reconnus, parfois précédemment compromis, afin de crédibiliser leurs actions d'hameçonnage ciblé. Engagées à consulter un lien ou un document lié à leur sujet d'expertise, les victimes ont ensuite été compromises lorsqu'elles ont téléchargé à leur insu des charges malveillantes. Certaines victimes ont été amenées à renseigner leurs identifiants de connexion et mots de passe sur des applications de partage de documents (Dropbox notamment), permettant ensuite la compromission de leurs comptes utilisateurs, de pratiquer des exfiltrations de données et facilitant de futures attaques. La victimologie associée à ce MOA dans le secteur des *thinks tanks* et des relations internationales comprend des enseignants et enseignants-chercheurs en sciences politiques et de nombreux experts du Moyen-Orient situés en Europe (Belgique, Royaume-Uni, Allemagne), aux États-Unis mais également dans d'autres pays du Moyen-Orient [8].

En septembre 2022, un groupe de chercheurs en sécurité spécialistes de l'Iran a ainsi publié une analyse de plusieurs campagnes reliées aux opérateurs du MOA Charming Kitten ciblant des personnalités du monde de la recherche. Parmi les chercheurs dont l'identité aurait été usurpée pour mener des approches personnalisées, engager des conversations et amener les cibles jusqu'à la compromission de leurs matériels informatiques, figureraient des experts de la géopolitique du Moyen-Orient. Parmi les chercheurs impersonnifiés figure un chercheur français d'un organisme national de recherche, davantage spécialiste de questions scientifiques. Son identité aurait été usurpée sur LinkedIn pour construire des relations interpersonnelles avec d'autres chercheurs, jusqu'à inviter les cibles finales à cliquer sur des faux liens de visioconférence sur Zoom, installant ainsi des logiciels malveillants. Selon les chercheurs de CERTFA Lab ayant mené cette analyse, plusieurs chercheurs français auraient pu faire l'objet de ce type d'usurpation d'identité [9].

3.2 Espionnage industriel et scientifique : ciblage de centres de recherche civils et militaires

Les organismes de recherche publics sont fréquemment ciblés au moyen de modes opératoires d'attaque liés aux intérêts stratégiques d'États. Les laboratoires et les *start-ups* et *spin-off* qui en sont issus sont détenteurs d'informations et de données de recherche qui relèvent des intérêts scientifiques et économiques fondamentaux de la Nation. Leurs travaux, qui répondent souvent à la commande publique, influent sur les politiques publiques ainsi que sur la règlementation française ou européenne dans de très nombreux domaines (énergétique, sanitaire et médical, agro-alimentaire, aménagement du territoire, etc.). Ils développent également des technologies de pointe qui sont ensuite réutilisées dans le domaine industriel, dans des secteurs stratégiques

tels que la défense, les transports, les infrastructures énergétiques et le numérique (intelligence artificielle, cryptologie et cryptographie quantique, technologies des matériaux et composants etc.). Ainsi, ils représentent des cibles d'intérêt pour des attaquants cherchant à collecter des informations stratégiques dans ces domaines au profit de services de renseignement étrangers.

Au sein des vastes campagnes à but d'espionnage observées par l'ANSSI et de nombreux éditeurs de sécurité, ces institutions représentent une part importante des cibles de campagnes de reconnaissance ou des entités effectivement compromises. Les MOA réputés liés aux intérêts stratégiques chinois sont particulièrement actifs dans ce domaine.

3.2.1 Attaques menées au moyen de modes opératoires d'attaque réputés chinois

Plusieurs organismes de recherche ont été récemment ciblés au moyen de modes opératoires d'attaque réputés liés aux intérêts chinois, dans le cadre de larges campagnes de compromissions à but d'espionnage industriel et scientifique.

Ainsi, l'ANSSI a observé en 2021 le ciblage de plusieurs entités françaises ou internationales, effectué au moyen du MOA réputé lié aux intérêts stratégiques chinois APT31. Si certaines de ces entités semblent avoir uniquement fait l'objet d'opérations de reconnaissance, d'autres ont été effectivement compromises. Parmi ces entités figurent plusieurs organismes de recherche publics français. La compromission d'un prestataire de services numériques a également mis en évidence l'intérêt des attaquants pour les données des organismes nationaux de recherche hébergées par le prestataire.

Ces compromissions ont eu lieu depuis au moins octobre 2020 et ont été décrites par l'ANSSI dans un rapport publié en 2021. Si les organismes de recherche ne sont pas le seul secteur ciblé par le biais du MOA APT31, la présence de plusieurs entités du secteur dans la liste des cibles ou des victimes de ces opérations offensives indique l'intérêt que celles-ci représentent pour des attaquants cherchant à collecter massivement des informations stratégiques et scientifiques de nature très diverse, pouvant ensuite être exploitées par leur commanditaire [10].

Par ailleurs, plusieurs MOA réputés chinois auraient été employés pour cibler des entités russes du secteur de la défense depuis les années 2010, à des fins d'espionnage industriel et militaire. Les technologies avancées développées dans les centres de recherche liées aux industries de défense russes feraient l'objet d'une prédation au profit des intérêts chinois. Parmi les compromissions documentées, certaines concernent des entités de recherche spécialisées dans le développement d'équipements de communications satellitaires et de systèmes radio à finalité militaire. Ces compromissions de centres de recherche s'inscrivent dans des campagnes plus larges visant la base industrielle et technologique de défense (BITD) russe [11, 12]. Ce ciblage semble cohérent avec les besoins technologiques des services de sécurité et de l'armée chinoise.

Plus récemment et dans le contexte de l'invasion russe de l'Ukraine, l'éditeur de sécurité CHECKPOINT a documenté le ciblage d'au moins deux organismes de recherche russes (et potentiellement un au Belarus) impliqués dans le développement de technologies avancées de défense. Le ciblage aurait été réalisé au moyen du MOA réputé lié aux intérêts stratégiques chinois Twisted Panda, potentiellement lié aux MOA APT10 et Mustang Panda. Les attaquants auraient utilisé des outils offensifs inédits et sophistiqués, dans un but probable d'espionnage [13].

Les courriels d'hameçonnage ayant servi au ciblage de ces organismes de recherche auraient repris, selon CHECKPOINT, des thématiques liées aux sanctions américaines suivant le début de l'invasion de l'Ukraine et auraient contenu des liens vers un site imitant le ministère de la Santé

russe. La charge malveillante téléchargée suite à cette première étape de compromission aurait permis d'installer divers outils persistants capables d'explorer le système d'information compromis afin d'en extraire des données d'intérêt. Les organismes de recherche ciblés en Russie feraient partie du conglomérat de défense ROSTEC CORPORATION : leur ciblage peut indiquer une recherche d'informations de pointe par les attaquants, dans les domaines de spécialité de ces organismes (systèmes militaires, équipements électroniques et radars, systèmes aéronautiques, mais également équipements médicaux et systèmes de contrôle industriels) [14].

De nombreuses compromissions de systèmes d'informations d'universités asiatiques ou occidentales au moyen de MOA réputés liés à la Chine sont documentées par les éditeurs de sécurité. Ces compromissions récurrentes, explicables par l'hétérogénéité de ces infrastructures, leur niveau de sécurité parfois défaillant et une trop faible conscience de la menace, peuvent entraîner des conséquences très variées : les attaquants peuvent y rechercher des informations personnelles d'enseignants, d'enseignants-chercheurs, d'étudiants ou de personnels d'accompagnement de la recherche, utiles à de futures campagnes d'espionnage. Les données de recherche, parfois d'un haut niveau scientifique ou technologique, peuvent également être exfiltrées par les attaquants. Plusieurs compromissions ont montré l'installation d'outils de test d'intrusion légitimes, mais fréquemment employés à des fins malveillantes par des attaquants pour mener des actions sur des systèmes d'information et y maintenir des accès persistants, comme Cobalt Strike. Les informations disponibles sur ces attaques sont souvent trop lacunaires pour permettre d'identifier les objectifs précis des attaquants.

Commentaire : les données personnelles ou scientifiques traitées par les établissements d'enseignement supérieur, de recherche et d'innovation peuvent être d'intérêt pour des attaquants cherchant à collecter un maximum d'information permettant de mener de futures attaques, comme cela est fréquemment constaté lors d'attaques menées au moyen de MOA réputés liés aux intérêts chinois. La sécurisation de ces informations et une attention particulière portée aux outils de test d'intrusion et d'administration à distance pouvant être présents sur les réseaux des universités pourraient permettre de réduire le risque posé par ces attaques.

3.2.2 Attaques menées au moyen de modes opératoires d'attaque réputés nord-coréens

La Corée du Nord affiche de grandes ambitions dans certains domaines scientifiques et techniques, comme le nucléaire, l'armement ou l'aérospatial. Cependant, le pays est tenu sous embargo et n'a pas accès, de manière légale, aux équipements technologiques dont elle aurait besoin pour se développer en raison du double usage, civil et militaire, qui peut en être fait. La Corée du Nord a donc fréquemment recours à des moyens cyber-offensifs pour collecter des renseignements scientifiques lui permettant de chercher à combler son retard dans le développement de technologies de pointe, notamment balistiques.

Ainsi en mai 2021, l'INSTITUT CORÉEN DE RECHERCHE SUR L'ÉNERGIE ATOMIQUE (KAERI) a publiquement rapporté avoir été compromis *via* l'exploitation d'une vulnérabilité dans une passerelle VPN. Les autorités sud-coréennes et l'Institut de recherche ont indiqué avoir trouvé des indicateurs de compromission rattachant cette attaque au MOA réputé nord-coréen Velvet Chollima, également connu sous le nom de Kimsuky [15]. Le KAERI est un institut central dans le développement de la technologie nucléaire sud-coréenne et a contribué à la conception et production de réacteurs nucléaires, de technologies sur les radiations, les réacteurs, la sécurité nucléaire et les applications industrielles de la technologie nucléaire. Le KAERI possède des informations pouvant aider la Corée du Nord à maîtriser cette technologie.

Ciblage de la recherche médicale durant la pandémie de COVID-19

Lors de la pandémie de COVID-19, de nombreuses compromissions ont été observées, ciblant de façon globale l'industrie pharmaceutique et la recherche médicale. La recherche de vaccins et d'avantages industriels a mené à des compromissions d'entreprises pharmaceutiques et de recherche biomédicale, mais également d'hôpitaux universitaires, dans le monde entier. Ces compromissions ont pu être menées par le biais de modes opératoires d'attaque liés à plusieurs acteurs offensifs, ou non attribués.

En mai 2020, une attaque a entraîné la mise à l'arrêt du service de supercalculateurs britannique ARCHER, qui fournit des capacités de calcul aux chercheurs universitaires et industriels en Grande-Bretagne. Il était notamment utilisé à cette époque pour des recherches en lien avec le COVID-19. Cette attaque est concomitante avec des alertes publiées par les autorités américaines concernant des campagnes d'espionnage attribuées par les États-Unis d'Amérique à la Chine, dans le cadre de la recherche d'un vaccin contre le COVID-19. Les responsables du service ARCHER ont fait état d'intrusions sur leur système d'information et mentionné que cette compromission faisait, selon eux, l'objet d'une campagne d'espionnage plus vaste ciblant la communauté de la recherche en Grande-Bretagne et en Europe [16].

En 2023, l'ANSSI a été informée d'une campagne menée contre un organisme de recherche français, ayant conduit à la compromission de plusieurs comptes d'utilisateurs du VPN de l'entité, à des compromissions de comptes de messagerie ainsi qu'à l'exfiltration de plusieurs giga-octets de données dont certaines concerneraient des recherches passées ou présentes de l'institution. L'origine de ces attaques n'est pas connue.

3.3 Menaces liées à l'utilisation d'infrastructures de *Cloud computing*

Le développement récent de législations extra-territoriales ou de législations nationales relatives aux questions numériques par certains États représente également une menace, plus difficile à caractériser, pour de nombreux organismes de recherche et d'innovation et *think tanks*.

En effet, de nombreuses organisations du secteur utilisent des infrastructures de *Cloud computing* pour héberger leurs données. Elles sont également utilisatrices de suites collaboratives et bureautiques, souvent hébergées chez des opérateurs étrangers.

Les législations relatives à l'accès judiciaire ou extra-judiciaire aux données par les États peuvent avoir un impact significatif sur la sécurité des données dans le *Cloud*, en ce qu'il peut y avoir un décalage important entre l'endroit où sont effectivement stockées les données, l'implantation légale du fournisseur de services *Cloud* et l'entité cliente.

Le vol de *cookies* de session sur des plateformes de messagerie ou de travail collaboratif peut également amener à des compromissions de comptes utilisateurs dans ces organismes. Il peut être utilisé comme vecteur initial de compromission, mais également comme un moyen de latéralisation, particulièrement vers des ressources utilisées dans le *Cloud* [17]. La majorité des services *Cloud* de partage de documents et de travail collaboratif les plus populaires permettent en effet l'accès aux données à travers des délégations d'autorisation, notamment avec le protocole OAuth. Le même jeton « OAuth » (*token*) peut être utilisé pour tous les matériels d'un utilisateur.

Une menace grandissante concerne l'accès à ces jetons d'authentification, les attaquants tentant de les récupérer par ingénierie sociale. Une fois le jeton obtenu par un attaquant et copié, il peut potentiellement être utilisé à distance depuis un autre appareil sans être détecté.

Les organismes de recherche et les *think tanks* étant utilisateurs de ces services collaboratifs, peuvent par conséquent être ciblés par des attaquants ayant des objectifs d'espionnage. Ces vols de *cookies* de session ou de jetons d'authentification ont également été constatés chez des groupes d'attaquants aux motivations lucratives.

4 ATTAQUES À FINALITÉ DE DÉSTABILISATION

4.1 Ciblage du secteur dans le cadre de la guerre en Ukraine

Depuis le début de l'invasion de l'Ukraine par la Russie en février 2022, une recrudescence des attaques hacktivistes à finalité de déstabilisation a été observée, portée tant par des groupes pro-russes que pro-ukrainiens.

Les groupes soutenant l'invasion russe et pratiquant depuis février 2022 des attaques par déni de service distribué (DDoS) contre l'Ukraine ou des entités de pays soutenant l'Ukraine ont pu attaquer des entités du secteur de la recherche parmi d'autres cibles. Ainsi, le groupe hacktiviste Killnet a revendiqué des attaques contre des sites Internet de ministères ou d'organismes de recherche en Italie ou au Japon.

Certains groupes hacktivistes soutenant l'Ukraine ont, pour leur part, ciblé des organismes de recherche russes afin d'y mener des opérations de *hack and leak* et d'exposer des données sensibles.

Ainsi le 3 mars 2022 un groupe lié à Anonymous, v0g3lSec, a annoncé publiquement avoir pénétré un site Internet de l'INSTITUT DE RECHERCHE SPATIALE RUSSE (IKI), qui développe des outils expérimentaux pour la recherche spatiale. Par ce biais, les hacktivistes auraient exfiltré puis publié des documents de l'Agence spatiale russe (Roskosmos) hébergés sur un serveur partagé. Certains de ces documents concerneraient des missions lunaires. Le groupe aurait également défiguré un site hébergé sur un sous domaine de l'IKI [18].

Un organisme de recherche français a informé l'ANSSI en novembre 2023 d'une attaque par DDoS menée sur l'ensemble de ses sites Web sur plusieurs jours. Cette attaque, non revendiquée, aurait été contenue par l'organisme de recherche, n'occasionnant pas d'indisponibilité de ses sites internet.

Commentaire : les attaques menées par des groupes hacktivistes dans le contexte de l'invasion de l'Ukraine par la Russie ont un objectif de déstabilisation, qu'il s'agisse d'attaques par DDoS ou de hack and leak. Les centres de recherche et universités sont ciblés en tant qu'organisations publiques : l'interruption des activités ou la publication des données peuvent leur porter un préjudice d'image.

Les attaques par DDoS opérées par les groupes hacktivistes pro-russes sont menées de façon extensive contre tous types d'entités, du moment que ces attaques peuvent générer des retombées médiatiques : leur effet sur le fonctionnement des organisations ciblées reste le plus souvent très faible et ponctuel. Les données qui ont pu être publiées lors d'opérations de hack and leak par des groupes hacktivistes en soutien à la cause ukrainienne ne causent pas obligatoirement de préjudice de fond quant à la poursuite

de programmes de recherche mais visent probablement à générer un sentiment de vulnérabilité à ces institutions ainsi qu'à la population russe.

4.2 Attaques ayant des objectifs politiques

Dans le cadre des tensions géopolitiques au Moyen-Orient, des MOA réputés liés aux intérêts iraniens mènent des attaques à but de déstabilisation visant des entités israéliennes, parmi lesquelles figurent plusieurs universités. Ces attaques sont parfois menées sous la forme d'attaques par rançongiciel et comprennent une phase de publication de données internes (*lock and leak*), bien que de nombreuses analyses laissent penser que le but poursuivi n'est pas lucratif.

Ainsi en septembre 2021, l'éditeur de sécurité SENTINELONE a documenté une attaque menée au moyen du MOA réputé iranien Agrius, qui aurait servi à déployer le rançongiciel Apostle contre l'université israélienne de Bar-Ilan. Le chiffrement du système d'information aurait été précédé d'une exfiltration de données et de documents internes de l'université, publiés ensuite sur le site de divulgations de *leaks* Darkrypt comme preuve de la compromission. Cette attaque est cohérente avec d'autres compromissions par rançongiciel menées au moyen de MOA réputés iraniens contre des entités israéliennes. Ces attaques seraient, d'après plusieurs éditeurs de sécurité, davantage motivées par un objectif de déstabilisation (causée par l'interruption de l'activité des entités ciblées) qu'une recherche lucrative [19].

Plus globalement, les universités et institutions dépendant du secteur de l'éducation et de la recherche universitaire sont fréquemment visées par des attaques à but de déstabilisation, menées au nom d'objectifs politiques par des groupes hacktivistes. La défiguration de sites institutionnels, les attaques par DDoS ou les opérations de *hack and leak* soutiennent des revendications parfois très locales. Ces attaques portent essentiellement un préjudice d'image aux entités visées. Certains *think tanks* ont pu, occasionnellement, être également visés par ce type d'attaques. Les groupes hacktivistes les plus actifs ciblant (entre autres secteurs) les universités et institutions éducatives sont basés au Moyen-Orient et en Amérique du Sud.

Hors du contexte spécifique de la guerre en Ukraine, les entités européennes du secteur sont peu touchées par ces attaques à visée déstabilisatrices.

5 ATTAQUES À FINALITÉ LUCRATIVE

5.1 Compromissions au moyen de rançongiciels

À l'image de l'ensemble des secteurs, les organismes de recherche et *think tanks* peuvent être ciblés par des groupes cybercriminels opérant des rançongiciels à but lucratif. Ce ciblage est souvent opportuniste et dépend davantage de la vulnérabilité de l'établissement ciblé que de la nature de ses activités. Toutefois, la tendance au *Big Game Hunting* observée depuis les années 2020 (le ciblage d'établissements ayant potentiellement de grandes capacités de paiement) fait du secteur universitaire une cible privilégiée ce type d'attaque, quand bien même les capacités effectives de paiement de rançon par ces établissements est très aléatoire.

De nombreuses universités ont été touchées par des attaques par rançongiciel. Certaines auraient fait l'objet de demandes de rançon importantes, comme l'université de Pise en Italie, compromise en juin 2022 par le groupe cybercriminel ALPHV, qui aurait exigé une rançon de 4,5 millions de dollars [20].

Les compromissions par rançongiciel se doublent le plus souvent, depuis quelques années, d'exfiltration de données préalables, conférant aux attaquants des moyens de pression supplémentaires sur la victime : les groupes cybercriminels menacent en effet de publier les données exfiltrées en cas de non paiement de la rançon, et s'exécutent parfois après l'expiration du délai qu'ils ont eux-mêmes fixé. Si la plupart des données exfiltrées et publiées par les opérateurs de rançongiciels concernent les données personnelles des étudiants ou des personnels des établissements d'enseignement supérieur, les exfiltrations de données peuvent concerner également des données de recherche, si celles-ci ne sont pas correctement sécurisées.

En février 2022, l'Université de Neuchâtel en Suisse a ainsi été compromise par un rançongiciel. Les cybercriminels ont ensuite publié des données exfiltrées des systèmes d'information de l'université, parmi lesquelles des données sur les employés de l'université et les étudiants [21].

Plusieurs établissements d'enseignement supérieur français ou organismes de recherche ont fait l'objet, entre 2021 et 2024, de chiffrement ou de compromissions à but de chiffrement par des groupes cybercriminels. Les attaquants auraient utilisé des comptes étudiants compromis ou des vulnérabilités non corrigées dans des logiciels de supervision pour pénétrer les systèmes d'information de ces institutions. Pour certains établissements, ces attaques ont entraîné la perte définitive de données académiques.

Certaines compromissions au moyen de rançongiciels peuvent entraîner des conséquences importantes sur le fonctionnement des universités, en particulier si elles surviennent pendant des périodes où la disponibilité des services est cruciale. Ainsi, la compromission par rançongiciel de l'Université Paris-Saclay en août 2024, à quelques semaines de la rentrée universitaire, a entraîné des perturbations importantes de fonctionnement [22]. La survenue de cet incident au moment de la publication du « Classement de Shangaï » renforce également la pression sur l'université.

5.2 Compromissions au moyen d'*infostealers*

À la fin de l'année 2022, l'ANSSI a eu connaissance de nombreuses compromissions d'établissement d'enseignement supérieur par des rançongiciels. Les investigations menées ont également permis de mettre au jour des tentatives de compromission sur des environnements *Active Directory* de plusieurs entités, ainsi que de détecter plusieurs centaines d'*infostealers* (logiciels malveillants récupérant des identifiants et mots de passe) sur les équipements de nombreux établissements de l'enseignement supérieur et de la recherche.

L'ANSSI a également été informée en décembre 2023 de la compromission au moyen d'un *infostealer* de type *FakeUpdates* d'un institut de recherche sensible. Cette campagne aurait ciblé plus largement des entités en France et à l'étranger, de façon probablement opportuniste.

Enfin, des ventes d'authentifiants de messagerie ou de connexion à distance par VPN d'établissements supérieurs sont fréquemment constatées sur des forums cybercriminels, ou signalées à l'ANSSI dans le cadre d'utilisations malveillantes. Le nombre important d'utilisateurs des accès VPN peut rendre plus difficile l'identification de la source de compromission.

Commentaire : la menace d'attaques à but lucratif n'est pas spécifique au secteur de la recherche et aux think tanks. Toutefois, ces organisations peuvent être ciblées si leur niveau de sécurité n'est pas suffisamment élevé pour les en protéger. L'exfiltration de données sensibles par des attaquants pourrait alors mener à des conséquences plus importantes, en cas de revente de ces données sur des forums cybercriminels. Les données personnelles exfiltrées peuvent également servir ou être revendues à des fins d'hameçonnage

ciblé contre d'autres institutions, potentiellement mieux sécurisées. Enfin, les interconnexions entre différentes composantes de l'écosystème universitaire et de recherche français et international, rendent plus vulnérable l'ensemble du secteur à des propagations de compromissions d'un établissement à un autre.

5.3 Exploitation de vulnérabilités logicielles

Des entités du secteur de la recherche peuvent être concernées par des exploitations massives de vulnérabilités logicielles sur des produits utilisés de façon courante. Ainsi, lors des campagnes massives d'exploitation de vulnérabilités concernant les produits VPN Ivanti Connect Secure en janvier 2024 ou Palo Alto Networks PAN-OS en avril 2024, plusieurs organisations du secteur ont fait l'objet de compromissions avérées.

6 RECOMMANDATIONS

Les recommandations suivantes visent à éclairer les organismes de recherche et les *think tanks*, leurs tutelles institutionnelles ainsi que leurs éventuels prestataires, afin de bâtir une défense et de se prémunir des menaces détaillées précédemment. Ces recommandations ne sont pas exhaustives et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel du système d'information considéré. Elles ne se substituent pas aux réglementations spécifiques encadrant les activités des entités concernées.

Ces recommandations portent sur les thèmes suivants :

- la sensibilisation ;
- la maîtrise des risques ;
- la maîtrise des données ;
- les postes de travail et terminaux mobiles ;
- la messagerie ;
- les sauvegardes ;
- la veille sur les menaces.

6.1 Sensibilisation

R1

Sensibiliser le personnel

Organiser des sessions de sensibilisation dans l'optique de responsabiliser le personnel. Les objectifs majeurs sont de mettre l'accent sur les enjeux de cybersécurité et de protection du patrimoine scientifique, et de transmettre les bonnes pratiques à adopter face à une situation de cyber malveillance.

En particulier :

Pour les collaborateurs ayant un accès privilégié à de l'information stratégique, communiquer les précautions suivantes :

- ne pas ouvrir les messages dont la provenance ou la forme est inconnue, car il pourrait s'agir d'une tentative d'attaque (exemple : hameçonnage, rançongiciel) ;
- porter une attention particulière à la relation entre l'objet d'un courriel et son contenu (ex : pièce jointe, lien). Dans le cadre d'opérations de ciblage, les objets de courriels peuvent être manipulés pour se rapprocher de sujets traités par l'organisme de recherche ou le *think tank*, ou par des collaborateurs, afin de ne pas éveiller de doute et de pousser la cible à ouvrir l'élément joint (pièce jointe ou lien pointant vers des ressources spécifiques) contrôlé par l'attaquant ;
- se méfier des extensions de pièces jointes douteuses (exemples : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk), qui peuvent contenir des codes malveillants. Le cas échéant, demander à son service informatique de vérifier la nature d'un document au moyen d'un service dédié d'analyse de fichier [a] ;

- se méfier des tentatives d'approches malveillantes (tentative d'hameçonnage) *via* :
  - des médias sociaux ;
  - des messages reçus par SMS ou messageries instantanées (WhatsApp, Signal, Telegram, TikTok, Slack, Discord, Facebook Messenger, *etc.*) ;
  - des appels téléphoniques.
- être vigilant face aux URL visités depuis le poste de travail. En cas d'alerte de sécurité du navigateur Internet, notamment si le site Internet ne génère d'habitude pas d'alerte, avertir les services compétents en interne afin de qualifier l'avertissement ;
- ne pas connecter sur son poste de travail une clé USB trouvée par hasard ou reçue lors d'une rencontre professionnelle, car celle-ci pourrait être infectée par un logiciel malveillant ;
- Organiser des exercices adaptés au niveau de la menace afin d'accroître la vigilance du personnel face au risque de :
  - hameçonnage par messagerie électronique ;
  - compromission au moyen de supports USB ;
  - ingénierie sociale visant à collecter des informations sensibles.

Pour les organismes de rattachement, communiquer sur les chaînes d'alerte :

Les organismes doivent faire connaître à leurs communautés de travail le nom des contacts des experts cyber (ex : service « Helpdesk », RSSI, DPO, FSD, référent dédié à la protection des informations sensibles, etc.) chargés d'accompagner et de conseiller les communautés de travail, ainsi que leur chaîne de remontée et traitement des incidents.
Les personnels de recherche travaillant dans les organismes de recherche et les think tanks doivent connaître également :

- Les chaînes d'alerte des services de l'Etat, en particulier celle-du du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques appelé le CERT-FR (service de l'ANSSI joignable 7J/7, 24H/24 depuis la France métropolitaine au 3218 (service gratuit + prix d'un appel) ou 09 70 83 32 18 depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au +33 9 70 83 32 18, ou par mail : cert-fr@ssi.gouv.fr) à saisir pour tout incident de sécurité affectant le patrimoine scientifique et technique de la Nation ;
- Les missions de leurs référents/contacts qui leur sont dédiés au sein de l'ANSSI (Coordinateur sectoriel et délégués territoriaux), de la DGSI, de la DGE et de leur(s) ministère(s) de tutelle (HFDS, FSSI, etc.).

a. Les organismes de la fonction publique d'État pourront à cette fin utiliser le service d'analyse de fichiers mis en place par l'ANSSI : jecliqueoupas.cyber.gouv.fr. En cas d'utilisation d'un service commercial d'analyse de fichier, il conviendra de veiller à ce que ces vérifications n'entraînent pas de fuite de données sensibles.

6.2 Maîtrise des risques

R2

Mener une analyse de risques intégrant l'ensemble des prestataires et partenaires informatiques

Une analyse de risques doit être réalisée en prenant en compte les hébergeurs, sociétés de service, éditeurs de solutions sur lesquels s'appuie l'entité. Cette analyse de risques doit notamment mettre en exergue les risques numériques que ces entités externes feraient peser sur l'organisation tant sur le plan technique qu'organisationnel, ainsi que les impacts sur le secret professionnel ou tout autre secret en lien avec les activités de l'organisme de recherche ou du *think tank*. Cette analyse doit intégrer les menaces décrites dans ce document.

Ainsi, dans le cadre de l'utilisation d'un service numérique (échange de fichiers, messagerie, *etc.*), il convient de systématiquement s'interroger sur le niveau de confiance à accorder à ce service, dans l'optique de protéger les informations traitées au bon niveau. Cette évaluation du niveau de confiance à accorder à un service externe doit s'appuyer notamment sur l'origine du fournisseur du service, la localisation du service (en prenant en compte le contexte géopolitique du moment) ou encore son niveau de sécurisation (disponibilité, intégrité, confidentialité, traçabilité).

Il convient de rappeler que dans le cas où les prestations externalisées concernent des données sensibles, il est fortement recommandé que la prestation s'effectue depuis le territoire national en s'appuyant sur des prestataires qualifiés par l'ANSSI.

Dans le cadre de projets de recherche intégrant des partenariats avec des opérateurs critiques, les organismes de recherche veilleront à intégrer ces derniers dans leur analyse de risque. Le périmètre de l'écosystème numérique dans lequel sera effectuée le projet de recherche conjoint et les mesures de sécurité à mettre en œuvre pourront être précisés par voie contractuelle.

6.3 Maîtrise des données

R3

Identifier les informations et données sensibles ou à protéger selon la réglementation applicable

Il est nécessaire de réaliser un inventaire fin des données métier : format, emplacement, sensibilité, responsabilité, besoin d'en connaître, *etc.*

Une fois celui-ci réalisé, il est recommandé de mettre en œuvre une politique

d'accès (prenant en compte le principe du moindre privilège) adaptée aux différentes données identifiées. L'objectif est de réduire l'accès aux données identifiées comme sensibles et de limiter les fuites d'informations stratégiques traitées au sein de l'organisme de recherche ou du *think tank*.

En particulier, chaque organisme de recherche ou *think tank* doit s'attacher à :

- identifier parmi ses traitements de données, les informations sensibles à protéger au regard de la réglementation applicable, du risque d'atteinte à la confidentialité, de modification non désirée ou de perte de données ;
- adopter le marquage approprié de ces données : l'objectif du marquage est d'apporter la connaissance du niveau de sensibilité des informations à toute personne les manipulant. Dans le cas de fichiers informatiques, le marquage doit également figurer sur le nom du fichier et du répertoire de stockage ;
- initier et maintenir l'inventaire fin de ses données afin de faciliter le travail de protection des services administratifs travaillant à leur archivage sécurisé : format, emplacement, sensibilité, responsabilité, besoin d'en connaître *etc.*

Les données sensibles stockées sur des supports amovibles (clé USB, disque dur portable) doivent être systématiquement chiffrées.

6.4 Postes de travail et terminaux mobiles

R4

Sécuriser les postes de travail et les terminaux mobiles

Mettre en place des mesures organisationnelles et techniques permettant de sécuriser les moyens informatiques mis à la disposition du personnel des organismes de recherche ou des *think tanks*.

L'objectif est de réduire la surface d'attaque offerte par ces différents équipements (PC, tablette, téléphone mobile, périphérique de stockage *etc.*) et de limiter ainsi le risque de compromission des moyens informatique de l'entité.

En particulier :

- les moyens informatiques (PC, téléphone mobile, stockage) confiés aux utilisateurs sont réservés à un usage professionnel ;
- les moyens informatiques personnels ne doivent pas être utilisés à des fins professionnelles ;
- les moyens informatiques sont à jour vis-à-vis des vulnérabilités récentes ;
- les moyens informatiques sont équipés de protections contre les codes malveillants ;
- les utilisateurs ne disposent pas de droits d'administration ;
- l'installation d'applications est issue uniquement de sources maîtrisées (ex : magasin de logiciel interne) ;

- après une étude d'impact, et quand cela est maîtrisé, les modes de sécurité avancée sur les téléphones mobile sont activés quand cela est disponible, afin d'éviter l'installation d'outils de prise de contrôle à distance (RAT) ;
- les périphériques de stockage sont chiffrés, y compris le stockage amovible ;
- les risques liés à l'utilisation de support amovible sont traités ;
- les mots de passe stockés sur les systèmes (PC, téléphone mobile) sont protégés à l'aide de gestionnaires de mot de passe (ex : keepass…). Ils répondent aux recommandations de l'ANSSI (12 caractères minimum, contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux. Ils évitent de comporter des noms et des dates de naissance) ;
- les mots de passe utilisés sont complexes, non prédictibles et renouvelés dès qu'une compromission est suspectée.

Les personnels des organismes de recherche et *think tanks* doivent porter une attention particulière à leurs équipements informatiques (PC, téléphone mobile, stockage) en déplacement, notamment à l'étranger.

En particulier :

- s'informer préalablement sur les législations en vigueur concernant les contrôles aux frontières et l'accès aux données stockées dans ces équipements ;
- privilégier l'utilisation de matériels dédiés aux déplacements et ne contenant que les données non sensibles strictement nécessaires aux missions à effectuer ;
- pour les besoins de connexion Internet lors des déplacements, privilégier l'utilisation d'équipement réseau fournissant une connexion 4G (éventuellement au moyen d'un routeur fourni par l'organisme de recherche). Il convient de rappeler que les réseaux Wi-Fi publics peuvent porter atteinte à la confidentialité des données transitant sur ces derniers.

6.5 Messagerie

R5

Porter une attention particulière aux règles de redirection de courriels

Dans le cadre de la compromission d'un compte de messagerie, l'attaquant pourrait créer des règles de recopie et de redirection de courriels vers une messagerie sous son contrôle. Ainsi, il est recommandé de faire une revue régulière de ces règles lorsqu'elles existent.

R6

Activer l'authentification multi-facteurs sur les accès à la messagerie

Dans le contexte de fuites de données massives d'identifiants et des mots de passe associés, puis de leur revente sur l'Internet sombre, il est recommandé d'activer

l'authentification multi-facteurs sur les accès à la messagerie.

6.6 Sauvegardes

R7

Faire régulièrement des sauvegardes hors-ligne

Il est fortement recommandé de procéder à des sauvegardes fréquentes et régulières des supports stratégiques de l'organisme de recherche ou du *think tank* (documents de recherche par ex.) afin d'anticiper une indisponibilité des services externalisés sur lesquels peut s'appuyer l'organisation (ex : services de *cloud computing*). Le bon fonctionnement de ces sauvegardes doit être régulièrement testé.

De plus, il est fortement recommandé de mettre en œuvre des mesures permettant d'assurer la confidentialité et l'intégrité des sauvegardes stockées.

6.7 Veille sur les menaces

R8

Pratiquer une veille active sur les menaces

Afin de rester informés sur les menaces émergentes et d'adopter les mesures de sécurité nécessaires à la bonne anticipation de la menace, il est important pour les organismes de recherche ou *think tanks* concernés par le présent document, ou pour les entités ayant en charge l'informatique de ces entités, de mener une veille active sur le site du CERT-FR ou tout autre site spécialisé permettant de suivre l'évolution des menaces en matière de cybersécurité.

6.8 Références à consulter pour la sécurisation des organismes de recherche et les *think tanks*

L'ANSSI et ses partenaires mettent à disposition du public de nombreuses références en matière de sensibilisation des utilisateurs et de conseils pour sécuriser des systèmes d'information professionnels. Parmi celles-ci, les organismes de recherche et les *think tanks* pourront particulièrement consulter :

6.8.1 Sensibilisation des personnels

- Cybermalveillance.gouv.fr, *Kit de sensibilisation - Assistance aux victimes de cybermalveillance*, 21 janvier 2020 [23] [23]
- ANSSI, *Guide d'hygiène informatique*, 1er janvier 2017 [24]
- Consulter les « Flash Ingérence » régulièrement publiés par la DGSI [25]

6.8.2 Sécurisation des systèmes d'information

- SGDSN - ANSSI, *Protection numérique du potentiel scientifique et technique de la Nation. Guide méthodologique*, avril 2018 [1]
- ANSSI, *Comprendre et anticiper les attaques DDoS*, 1er mars 2015 [26]
- ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*, 11 novembre 2017 [27]
- ANSSI, *Cartographie du système d'information*, 1er novembre 2018 [28]
- ANSSI, *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*, 1er janvier 2020 [29]
- ANSSI, *Recommandations relatives à l'interconnexion d'un système d'information à Internet*, 19 juin 2020 [30]
- ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, 11 mai 2021 [31]
- ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*, 2 octobre 2023 [32]
- ANSSI, *Recommandations relatives à l'authentification multifacteur et aux mots de passe*, 8 octobre 2021 [33]
- ANSSI, *Sauvegarde des systèmes d'information*, 25 octobre 2023 [34]
- ANSSI, *Menaces liées aux vols de cookies et contre-mesures*, 25 mai 2022 [17]
- ANSSI, *Recommandations sur le nomadisme numérique*, 23 novembre 2023 [35]

7 Références

[1] SGDSN. *Protéger le potentiel scientifique et technique de la nation*. 22 novembre 2022.
URL : http://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation.

[2] Conseil de l'Union européenne. *L'UE impose les toutes premières sanctions à la suite de cyberattaques*. 30 juillet 2020.
URL : https://www.consilium.europa.eu/fr/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

[3] Security Affairs. *Russian APT28 Hacker Accused of the NATO Think Tank Hack in Germany*. 20 juin 2022.
URL : https://securityaffairs.com/132452/hacking/apt28-hacked-nato-think-tank.html.

[4] NCSC-UK. *Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-Phishing Campaigns*. 7 décembre 2023.
URL : https://www.ncsc.gov.uk/news/star-blizzard-continues-spear-phishing-campaigns.

[5] Microsoft. *Star Blizzard Increases Sophistication and Evasion in Ongoing Attacks*. 7 décembre 2023.
URL : https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/.

[6] SentinelOne. *Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign*. 4 mai 2023.
URL : https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/.

[7] US Federal Bureau of Investigation. *North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media*. 1er juin 2023.
URL : https://media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERING.PDF.

[8] GovInfoSecurity. *Iranian APT Gang Phishes Middle East Experts*. 14 juillet 2021.
URL : https://www.govinfosecurity.com/iranian-apt-gang-phishes-middle-east-experts-a-17073.

[9] CERTFA. *Charming Kitten : Can We Have a Meeting ?* 8 septembre 2022.
URL : https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/.

[10] ANSSI. *Campagne d'attaque du mode opératoire APT31. Description et contre-mesures.* 25 novembre 2021.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/.

[11] Dr.WEB. *Study of Targeted Attacks on Russian Research Institutes*. 2 avril 2021.
URL : https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf.

[12] Palo Alto Networks. *BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger*. 22 décembre 2015.
URL : https://unit42.paloaltonetworks.com/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/.

[13] CHECKPOINT. *Twisted Panda : Chinese APT Espionage Operation against Russian's State-Owned Defense Institutes*. 19 mai 2022.
URL : https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/.

[14] CHECKPOINT. *Twisted Panda : Chinese APT Espionage Operation against Russian State-Owned Defense Institutes*. 19 mai 2022.
URL : https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/.

[15] SECURITY AFFAIRS. *North Korean APT Kimsuky Hacked South Korea's KAERI Agency*. 19 juin 2021.
URL : https://securityaffairs.com/119147/apt/kimsuky-apt-hacked-south-korea-kaeri.html.

[16] DARK READING. *UK Supercomputing Service ARCHER Still Offline After Monday Attack*. 15 mai 2020.
URL : https://www.darkreading.com/attacks-breaches/uk-supercomputing-service-archer-still-offline-after-monday-attack.

[17] ANSSI. *Menaces liées aux vols de cookies et contre-mesures – CERT-FR*. 25 mai 2022.
URL : https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-005/.

[18] VICE. *Hackers Breach Russian Space Research Institute Website*. 3 mars 2022.
URL : https://www.vice.com/en/article/z3n8ea/hackers-breach-russian-space-research-institute-website.

[19] SENTINELONE. *New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education*. 30 septembre 2021.
URL : https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/.

[20] SECURITY MAGAZINE. *University of Pisa Suffers Ransomware Attack | Security Magazine*. 15 juin 2022.
URL : https://www.securitymagazine.com/articles/97826-university-of-pisa-suffers-ransomware-attack.

[21] ICT JOURNAL. *Cyberattaque contre l'Université de Neuchâtel : des données volées publiées sur le darkweb (update)*. 28 février 2022.
URL : https://www.ictjournal.ch/news/2022-02-28/cyberattaque-contre-luniversite-de-neuchatel-des-donnees-volees-publiees-sur-le.

[22] UNIVERSITÉ PARIS-SACLAY. *FAQ Piratage – Université Paris-Saclay*. 21 août 2024.
URL : https://www.universite-paris-saclay.fr/piratage/.

[23] CYBERMALVEILLANCE.GOUV.FR. *Kit de sensibilisation - Assistance aux victimes*. 21 janvier 2020.
URL : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation.

[24] ANSSI. *Guide d'hygiène informatique*. 1er septembre 2017.
URL : https://cyber.gouv.fr/hygiene-informatique.

[25] DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE. *Conseil aux entreprises : flash ingérences*.
URL : https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/contre-espionnage/conseils-aux-entreprises-flash-ingerence.

[26] ANSSI. *Comprendre et anticiper les attaques DDoS*. 1er mars 2015.
URL : https://cyber.gouv.fr/guide-ddos.

[27] ANSSI. *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*. 11 novembre 2017.
URL : https://cyber.gouv.fr/guide-dns.

[28] ANSSI. *Cartographie du système d'information*. 1er novembre 2018.
URL : https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation.

[29] ANSSI. *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*. 1er janvier 2020.
URL : https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[30] ANSSI. *Recommandations relatives à l'interconnexion d'un système d'information à Internet*. 19 juin 2020.
URL : https://cyber.gouv.fr/guide-interconnexion-si-internet.

[31] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information*. 11 mai 2021.
URL : https://cyber.gouv.fr/guide-admin-si.

[32] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*. 2 octobre 2023.
URL : https://cyber.gouv.fr/guide-admin-si-ad.

[33] ANSSI. *Recommandations relatives à l'authentification multifacteur et aux mots de passe*. 8 octobre 2021.
URL : https://cyber.gouv.fr/guide-authentification.

[34] ANSSI. *Sauvegarde des systèmes d'information*. 25 octobre 2023.
URL : https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

[35] ANSSI. *Recommandations sur le nomadisme numérique*. 23 novembre 2023.
URL : https://cyber.gouv.fr/guide-nomadisme-numerique.

Version 0.1 – 10 septembre 2024

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité