CyberDico de l'ANSSI FR/EN

Qu'est-ce que c'est ?

Le CyberDico de l'ANSSI liste, par ordre alphabétique, des mots, expressions et sigles du domaine de la cybersécurité. Il présente leur traduction ainsi que leur définition en français et en anglais.

PRECISION POUR LA LECTURE DU CYBERDICO

- Lorsque les différentes traductions sont synonymes et peuvent être utilisées de manière indifférenciée, elles sont séparées par une barre oblique.
- Lorsque les différentes traductions renvoient à des significations distinctes, elles sont dissociées sur plusieurs lignes et commentées.
- Sont entre crochets, des éléments pouvant compléter le mot ou l'expression.
- Sont entre parenthèses, les sigles à utiliser selon les règles décrites dans les règles générales de traduction.
- La colonne « Terme » : désigne le terme le plus souvent employé dans le langage courant. Il peut être en français ou en anglais.

Règles générales de traduction

- Les traductions se font en anglais britannique.
- Lorsque le sigle fait référence à une réalité franco-française (ANSSI, OIV, LPM, ARCEP…), le sigle français doit être utilisé *a minima* pour la première occurrence dans la version traduite. - Dans la suite du texte, le prestataire de traduction utilisera au choix le sigle français ou la description en anglais.
- En aucun cas on ne peut inventer de sigle en anglais.
- Lorsqu'un sigle équivalent existe en anglais, on l'utilise dans la version traduite (RGPD = GDPR ; OSE = OES ; RSSI = CISO…).
- Mots et expressions sans équivalent anglais : le terme est réécrit en français (italique)

Le CyberDico a vocation à évoluer et à être mis à jour régulièrement.

A

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Accès de proximité (Accès local)	Close access	Englobe les attaques par wifi, ondes.	Includes wifi and wave attacks.
Accès local (accès de proximité)	Close access	Attaques avec accès physique au réseau.	Attacks with physical access to the network.
Actes de cybermalveillance	Cybermalicious activities/actions	Une cybermalveillance représente toute infraction commise par voie numérique. Il peut s'agir de phishing ou hameçonnage, de piratage d'un compte ou d'un équipement, d'usurpation d'identité, d'attaque par rançongiciel, etc.	Cybermaliciours activities are any crime committed through digital means. It can include phishing, account or equipment hacking, identity theft, ransomware attacks, etc.
Adware	Logiciel publicitaire/ publiciel	Code ayant pour finalité d'afficher des bandeaux publicitaires par le biais du navigateur Internet de l'utilisateur. Remarque : Ce code est très souvent perçu comme une méthode envahissante. Il engendre dans de nombreux cas d'autres effets sur le système, comme l'apparition de fenêtres surgissantes (popups), la dégradation de la bande passante ou de la performance de la machine de l'utilisateur.	Code used to display advertising banners via the user's Internet browser. Note: This code is often perceived as an intrusive method. In many cases, it has other effects on the system, such as the appearance of pop-ups, and degradation of the user's bandwidth or machine performance.
L'Agence	The Agency	Sans objet	Sans objet
[L'] Agence nationale de la sécurité des systèmes d'information	ANSSI, [the] French Cybersecurity Agency L'acronyme « ANSSI » est conservé en anglais. On n'utilise jamais « the » devant ANSSI. Ne pas utiliser d'acronyme anglais.	L'ANSSI est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Son action vise à construire et organiser la protection de la Nation face aux cyberattaques. Rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN), l'Agence est un service du Premier ministre, dont les activités sont exclusivement défensives.	ANSSI is the national authority for cybersecurity and cyberdefense. Its role is to build and organize the nation's protection against cyber attacks. Reporting to the General Secretary for National Defense and Security (SGDSN), the Agency is a department of the Prime Minister, whose activities are exclusively defensive in nature.
Analyse du risque numérique	Digital risk analysis	L'analyse de risque vise à apprécier les risques numériques qui pèsent sur une organisation - qu'elle soit publique ou privée - et à identifier les mesures de sécurité à mettre en œuvre pour les maîtriser. L'ANSSI, avec le soutien du Club EBIOS, publie une méthode dédiée à cet exercice : EBIOS Risk Manger.	Digital Risk analysis aims to assess the digital risks facing an organization - whether public or private - and to identify the security measures to be implemented to control them. ANSSI, with the support of the EBIOS Club, publishes a method dedicated to this exercise: EBIOS Risk Manger.
Article scientifique [1]	Paper	Article à l'état de projet, soumission.	Sans objet

Article scientifique [2]	Publication	Article publié dans une revue scientifique.	Sans objet
Assistance capacitaire	Capacity building	Développement capacitaire, renforcement capacitaire	Capacity development, capacity building
Attaque homme-du-milieu	Adversary-in-the-middle/AitM	Catégorie d'attaque où une personne malveillante s'interpose dans un échange, et de manière transparente pour les utilisateurs ou les systèmes.	A type of attack in which a malicious person interposes himself in an exchange, and in a way that is transparent to users or systems.
Attaque par saisie d'authentifiants volés	Credential stuffing	Type d'attaque par force brute exploitant des authentifiants précédemment exposés.	A type of attack in which the perpetrator collects stolen account credentials and then uses them to gain unauthorized access to accounts on other systems through large scale automated login requests.
Audit	Audit	Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure les exigences d'un référentiel sont satisfaites.	Systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which the requirements of a standard have been met.
Authenticité	Authenticity	L'information est attribuée à son auteur légitime.	The information is attributed to its legitimate author.
Authentification	Authentication	L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.	The purpose of authentication is to verify the identity claimed by an entity. Generally speaking, authentication is preceded by identification, which enables the entity to be recognized by the system through an element with which it has been endowed. In short, to identify oneself is to communicate one's identity, and to authenticate oneself is to provide proof of one's identity.

[L'] Autorité de régulation des communications électroniques et des postes (ARCEP)	ARCEP, the Electronic Communications and Postal Services Regulatory Authority/[the] Electronic Communications and Postal Services Regulatory Authority (ARCEP)	Sans objet	Sans objet
Australian Cyber Security Centre	Centre australien de Cybersécurité (ACSC)	Sans objet	Sans objet
Australian Signals Directorate	Direction australienne des transmissions (ASD)	Sans objet	Sans objet

B

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Backdoor	Porte dérobée	Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur de se connecter à une machine distante, de manière furtive.	Concealed access, either software or hardware, enabling a malicious user to connect to a machine by stealth. A backdoor can also be the cause of an incorrect protocol implementation.
Back-office	Service d'appui, post-marché, arrière-guichet	Support informatique et logistique d'un ou plusieurs guichets.	IT and logistical support for one or more counters.
Balayage de ports	Port scanning	Technique qui consiste à envoyer des paquets de données sur les différents ports d'une machine, puis à en déduire les états (la disponibilité) de ces ports en fonction de la réponse retournée, si elle existe.	Technique that consists of sending data packets to the various ports of a machine, then deducing the status (availability) of these ports based on the response returned, if any exist.
Big Data	Mégadonnées ou données massives	Données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés.	The sheer volume of structured and unstructured data requires appropriate analysis tools.
Blockchain	Chaîne de blocs	Véritable registre de comptes numériques reposant sur la confiance, la chaîne de blocs (blockchain), permet une gestion collaborative et sans intermédiaire (État, banque, notaire, etc.) des transactions qui s'opèrent entre différents acteurs. Cette technologie repose sur un procédé cryptographique qui assemble ces transactions pour former des « blocs » qui, une fois validés par ce même procédé, sont ajoutés à la chaîne de blocs à laquelle ont accès les utilisateurs. On compte parmi ces transactions l'échange de cybermonnaie (ou monnaie cryptographique) comme le bitcoin auquel on doit la popularisation de la Blockchain.	Veritable register of digital accounts based on trust, the blockchain enables collaborative management of transactions between different players, without intermediaries (governments, banks, notaries, etc.). This technology is based on a cryptographic process that assembles these transactions to form "blocks" which, once validated by the same process, are added to the blockchain to which users have access. These transactions include the exchange of cybercurrencies (or cryptocurrencies) such as bitcoin, to which we owe the popularization of the blockchain.
Blog	Blogue (anciennement Bloc-notes), cybercarnet	Site Internet, souvent personnel présentant en ordre chronologique de courts articles ou notes, souvent accompagnés de liens vers d'autres sites.	Internet site, often personal, presenting short articles or notes in chronological order, often accompanied by links to other sites.
Bombardement de courriels	Mail bombing	Envoi d'une grande quantité de courriels à un destinataire unique dans une intention malveillante. Forme particulière de déni de service contre les systèmes de courriers électroniques.	Sending a large number of e-mails to a single recipient with malicious intent. A particular form of denial of service against e-mail systems.
Bombe programmée, bombe logique	Logic bomb	Logiciel malveillant conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont	Malware designed to cause damage to a computer system and triggered when certain conditions are met. Some viruses

		réunies. Certains virus contiennent une fonction de bombe logique : déclenchement à date fixe, ou quand une adresse réticulaire (URL) particulière est renseignée dans le navigateur.	contain a logic bomb function: triggered on a fixed date, or when a particular reticular address (URL) is entered in the browser.
Boot	Amorce	Processus de démarrage (ou redémarrage) d'un ordinateur via un matériel (par exemple, le bouton de démarrage sur l'ordinateur) ou via une commande logicielle.	Process of starting (or restarting) a computer via hardware (e.g. the start button on the computer) or via a software command.
Bootkit		Maliciel qui infecte le processus de démarrage du système d'exploitation et permet ainsi d'en prendre le contrôle.	Malware that infects the operating system's boot process, enabling it to be taken over.
Botnet	Réseau de machines zombies	Réseau de machines distinctes (ordinateurs ou téléphones intelligents) utilisé à des fins malveillantes (attaques DDoS, campagnes de pourriels, diffusion de programmes malveillants) et souvent à l'insu de leurs utilisateurs légitimes.	A botnet is a network of compromised machines at the disposal of a malicious individual (the master). This network is structured in such a way as to enable its owner to transmit orders to all or some of the machines in the botnet, and to operate them at will. Some botnets can reach considerable numbers of machines (several thousand). These machines can be used for illicit trade or malicious actions against other machines.
Box	Boitier multiservice	Appareil permettant d'accéder, à partir de terminaux, à plusieurs services de communication (Internet, téléphonie, télévision et stockage).	Device enabling terminal-based access to several communication services (Internet, telephony, television and storage).
Bug	Bogue	Défaut de conception ou de réalisation se manifestant par des anomalies de fonctionnement.	Defects in design or construction resulting in malfunctions.
Bug bounty program	Programme de chasse aux vulnérabilités	Appel à des spécialistes qui recherchent des vulnérabilités dans des applications ou des configurations de serveur en échange d'une gratification pour les découvertes et remontées.	Call on specialists to search for vulnerabilities in applications or server configurations, in exchange for a fee for discoveries and reports.
BYOD (Bring Your Own Device)	AVEC (Apportez Votre Equipement personnel de Communication)	Se dit de l'utilisation dans un cadre professionnel, d'un matériel personnel comme un téléphone intelligent ou un ordinateur.	Refers to the professional use of personal equipment such as a smartphone or computer.

C

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Canal caché	Covert channel	Canal de communication qui permet à un processus malveillant de transférer des informations d'une manière dissimulée. Le canal assure une communication par l'exploitation d'un mécanisme qui n'est pas censé servir à la	A communication channel that enables a malicious process to transfer information in a concealed way. The channel ensures communication by exploiting a mechanism that is not supposed to be used for

		communication.	communication.
Canular	Hoax	Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.	True or false information, often transmitted by e-mail or in a forum, encouraging recipients to perform operations or take initiatives that are often harmful.
Capacités de détection	Detection Capabilities/ detection capacities	Capacité de supervision de la sécurité global et maîtrisé. Pour faire de la détection, les experts de se basent sur leur expertise de la menace stratégique et sur leur connaissance des techniques d'attaque de masse. Les experts cherchent ainsi à détecter des marqueurs techniques propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé.	Comprehensive, controlled security monitoring capability. Our detection experts draw on their expertise in strategic threats and their knowledge of mass-attack techniques. They seek to detect technical markers specific to certain attackers, such as the IP address of a malicious server or the name of a booby-trapped website.
Enregistreur de frappes, capteur clavier	Keylogger, keystroke logger	Logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au clavier.	Software or hardware used by a malicious user to capture what a person types on the keyboard.
Cartographie du risque [1]	Risk mapping	Représentation visuelle (exemple : radar, diagramme de Farmer) des risques issus des activités d'appréciation du risque.	Visual representation (e.g. radar, Farmer diagram) of risks resulting from risk assessment activities.
Certification	Certification	La certification est l'attestation de la robustesse d'un produit, basée sur une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI, selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques.	Certification is the attestation of a product's robustness, based on a conformity analysis and penetration tests carried out by a third-party evaluator under the authority of ANSSI, according to a scheme and a reference framework adapted to users' security needs and taking account of technological developments.
Chatbot	Agent conversationnel	Sans objet	Sans objet
Cheval de Troie	Trojan Horse	Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.	A program that gives the impression of having a useful function, but on the other hand has a hidden, potentially malicious function.
Chiffrement	Encryption	Transformation cryptographique de données produisant un cryptogramme.	Cryptographic transformation of data to produce a cryptogram.
Chiffrement asymétrique [2]	Asymetric cryptography	Le chiffrement asymétrique est un protocole de cryptographie qui utilise deux clés distinctes.	Asymmetric cryptography, otherwise known as public-key cryptography, relies on pairs of corresponding public and private keys to encrypt and decrypt messages.
Chiffrement symétrique [2]	Symmetric key cryptography	Le chiffrement symétrique permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un	Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key.

		même mot clé.	
CISA (Cybersecurity and Infrastructure Security Agency)	Agence américaine pour la cybersécurité et la sécurité des infrastructures	CERT National américain	U.S. National CERT
Cloud	Infrastructure nuagique	Modèle permettant un accès aisé, généralement à la demande, et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.	Model enabling easy, generally on-demand, network-based access to a set of shared, configurable computing resources.
Code d'exploitation	Exploit	Tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.	All or part of a program that enables a vulnerability or set of vulnerabilities in a software program (system or application) to be used for malicious purposes.
Code malveillant	Malicious code	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau. Maliciel/logiciel malveillant	Any program developed for the purpose of causing harm to or through a computer system or network. Malware/malicious software.
Communications Security Establishment	Centre de la sécurité des télécommunications canadien (CSE)		
Computer Emergency Response Team (CERT)	Equipe de réponse aux attaques cyber (CERT)	Centre de réponse aux incident cyber. Nom déposé. On utilise généralement directement le sigle.	Cyber incident response center.
Computer Security Incident Response Team (CSIRT)	Equipe de réponse aux attaques cyber (CSIRT)	Centre de réponse aux incidents cyber, appellation privilégiée en Europe. On utilise généralement directement le sigle.	Cyber incident response center.
[La] Commission nationale de l'informatique et des libertés (CNIL)	CNIL, the French Data Protection Authority (DPA) / [the] French Data Protection Authority (CNIL) / [the] French DPA	La CNIL est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Ainsi, elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.	The CNIL is responsible for ensuring the protection of personal data contained in computer files and processing, whether public or private. It is therefore responsible for ensuring that information technology serves the citizen and does not infringe on human identity, human rights, privacy or individual or public freedoms.
Confiance numérique	Digital trust	La transformation numérique de la société amène à un développement massif des échanges par voie dématérialisée, mettant en exergue le besoin d'un cyberespace de confiance à même de garantir la sécurité de ces échanges, en assurant notamment la fiabilité des informations transmises, l'innocuité des services utilisés et plus largement le respect de la vie privée des citoyens.	The digital transformation of society is leading to massive growth in electronic exchanges, highlighting the need for a trusted cyberspace capable of guaranteeing the security of these exchanges, in particular by ensuring the reliability of the information transmitted, the safety of the services used and, more generally, respect for citizens' privacy.

[Le] Conseil de l'économie et de l'information du digital (CEIDIG)	CEIDIG, the Digital Economy and Information Council/[the] Digital Economy and Information Council (CEIDIG)	Sans objet	Sans objet

Cookie	Témoin de connexion	Petit fichier installé sur le disque dur lors de la consultation d'un site Internet, qui permet au serveur de mémoriser des informations sur l'internaute et son comportement.	Small file installed on the hard disk when an Internet site is consulted, enabling the server to memorize information about the surfer and his behavior.
Cross-Site Request Forgery, CSRF	Injection de requêtes illégitimes par rebond	Attaque provoquant l'envoi de requêtes, par la victime, vers un site vulnérable, à son insu et en son nom.	Attack causing the victim to send requests to a vulnerable site, without their knowledge and on their behalf.
Cryptanalyse	Cryptanalysis	Processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement.	The process of decrypting cryptographically protected data without possessing the encryption keys.
Cryptographie	Cryptography	La cryptographie permet la transformation, au moyen d'un algorithme de chiffrement, d'un message clair en un message chiffré dans le but d'assurer la disponibilité, la confidentialité et l'intégrité des données échangées. Deux interlocuteurs peuvent ainsi échanger de manière confidentielle et sécurisée, pourvu qu'ils possèdent la clé leur permettant de chiffrer et/ou de déchiffrer leurs messages. La cryptographie sert aussi d'autres applications telles que l'authentification et la signature (numérique) des messages, ayant toutes pour finalité – chiffrement compris – le traitement, le stockage ou la transmission sécurisée de données.	Cryptography uses an encryption algorithm to transform a clear message into an encrypted one, in order to ensure the availability, confidentiality and integrity of the data exchanged. In this way, two parties can communicate confidentially and securely, provided they possess the key enabling them to encrypt and/or decrypt their messages. Cryptography is also used for other applications, such as authentication and (digital) signature of messages, all of which - including encryption - have the purpose of processing, storing or transmitting data securely.
Cryptologie	Cryptology	Science englobant la cryptographie et la cryptanalyse.	Science encompassing cryptography and cryptanalysis.
Cryptomonnaie	Cryptocurrency	Le terme cybermonnaie désigne une monnaie virtuelle qui permet aux usagers d'échanger de l'argent de façon anonyme et sans intermédiaire. Son fonctionnement repose un registre de comptes numériques – la blockchain – qui valide les transactions et émet la devise selon des principes cryptographiques. Plusieurs cybermonnaies sont aujourd'hui en circulation parmi lesquelles la plus connue : le bitcoin.	Cybercurrency is a virtual currency that enables users to exchange money anonymously and without intermediaries. Its operation is based on a register of digital accounts - the blockchain - which validates transactions and issues the currency according to cryptographic principles. Several cybercurrencies are in circulation today, including the best-known: bitcoin.
Cyberattaque	Cyber attack	Une cyberattaque consiste à porter	A cyberattack is the attack on

	(cyberattack, cyber-attack)	atteinte à un ou plusieurs systèmes informatiques dans le but de satisfaire des intérêts malveillants. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou liés par réseaux, connectés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des moyens de communication comme les smartphones, les tablettes et les objets connectés. La sécurité de ces dispositifs informatiques est mise en danger soit par voie informatique (virus, logiciel malveillant, etc.), soit par manipulation, soit par voie physique (effraction, destruction). Les quatre grandes finalités des cyberattaques sont : l'appât du gain, la déstabilisation, l'espionnage et le sabotage.	one or more computer systems, with the aim of satisfying malicious interests. It targets various IT devices: computers or servers, isolated or linked by networks, connected or not to the Internet, peripheral equipment such as printers, or communication devices such as smartphones, tablets and connected objects. The security of these IT devices is jeopardized either by computer attacks (viruses, malware, etc.), manipulation or physical attacks (break-ins, destruction). The four main purposes of cyberattacks are: greed, destabilization, espionage and sabotage.
Cybercriminalité, Cybercrime	Cyber crime	Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.	Acts that contravene international treaties or national laws, using networks or information systems as a means of committing a crime, or targeting them.
Cyberdéfense	Cyber defence, cyberdefence	Ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels.	All the technical and non-technical measures enabling a State to defend its essential information systems in cyberspace.
Cyberespace	Cyberspace	Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.	A communication space formed by the worldwide interconnection of automated digital data processing equipment.
Cybersécurité	Cyber security	Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.	The desired state of an information system, enabling it to withstand events originating in cyberspace that could compromise the availability, integrity or confidentiality of the data stored, processed or transmitted, and the related services that these systems offer or make accessible. Cybersecurity calls on information systems security techniques, and is based on the fight against cybercrime and the implementation of cyberdefense.
Cybersaquatting	Accaparement de noms de domaine	Enregistrer un nom de domaine dans le seul but de bloquer toute attribution ultérieure de ce nom au profit de titulaires plus naturels ou légitimes.	Register a domain name for the only purpose of blocking any subsequent allocation of this name to more natural or legitimate holders.

D

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Darknet, Dark web	Internet clandestin (terme officiel) / Internet caché/sombre	Internet qui nécessite l'utilisation d'un protocole particulier (chiffrement, proxy etc).	Internet that requires the use of a specific protocol (encryption, proxy, etc.).
Débridage système	Jailbreak	Action de contourner les protections d'un système pour supprimer les restrictions d'utilisation mises en place par le constructeur.	The action of bypassing a system's protections to remove the restrictions on use put in place by the manufacturer.
Deep Web	Internet profond	Internet inaccessible au moteur de recherche.	Internet inaccessible to the search engine.
Défiguration, barbouillage	Defacement	Altération par un attaquant de l'apparence ou du contenu d'un site Internet. L'attaquant peut faire figurer des informations, des slogans ou des images sans lien avec l'objet du site attaqué. Les attaques par défiguration sont souvent menées à des fins de déstabilisation. Des *hacktivistes* peuvent y avoir recours.	Alteration by an attacker of the appearance or content of a website. The attacker may include information, slogans or images unrelated to the purpose of the site under attack. Defacement attacks are often carried out for destabilization purposes. Hacktivists may resort to them.
Délégué[/e] à la protection des données	Data Protection Officer (DPO)	Sans objet	Sans objet
Délégué[/e] ANSSI à la sécurité numérique	ANSSI Regional Officer	Intitulé du poste des agents de la division coordination territoriale.	Sans objet
Démonstration de faisabilité	Proof of Concept (POC)	Démonstration de la faisabilité d'une attaque utilisant une vulnérabilité donnée.	Demonstration of the feasibility of an attack using a given vulnerability.
Déni de service [distribué]	[Distributed] Denial of Service (DDoS)	DDoS est souvent utilisé en français. Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. https://cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos	DDoS is often used in French. Action having the effect of preventing or severely limiting a system's ability to provide the expected service. https://cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos
Department of Homeland Security	Département de la Sécurité intérieure (DHS)	Sans objet	Sans objet
Department of Justice	Département de la Justice (DoJ)	Sans objet	Sans objet
Dépassement ou débordement de mémoire	Buffer overflow	Technique d'exploitation d'une vulnérabilité dans le code d'un programme qui ne vérifie pas correctement la taille de certaines données qu'il manipule.	Technique for exploiting a vulnerability in the code of a program that does not correctly check the size of certain data it manipulates.

Déstabilisation	Destabilisation	Action visant à fragiliser l'équilibre ou le bon fonctionnement de processus et d'institutions avec une volonté de résonnance.	Action designed to undermine the stability or proper functioning of processes and institutions with a view to resonance.
Détection [d'intrusion]	Intrusion detection	Il est préférable d'utiliser en français l'expression complète « Détection d'intrusion ».	It is preferable to use the full expression "intrusion detection".

Détection d'attaques [1]	Attack detection	Service de supervision de la sécurité global et maîtrisé. Recherche de marqueurs techniques propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé.	Comprehensive, controlled security monitoring service. Search for technical markers specific to certain attackers, such as the IP address of a malicious server or the name of a booby-trapped website.
Directeur[/rice] général [de l'ANSSI]	Director-General [of ANSSI]	Sans objet	Sans objet
Directive Sécurité des réseaux de l'information (SRI)	Directive on security of Network and Information Systems (NIS)/NIS Directive	La directive NIS 2 vise à renforcer le niveau de cybersécurité des tissus économique et administratif des pays membres de l'UE.	The NIS 2 directive aims to reinforce the level of cybersecurity of the economic and administrative fabric of EU member countries.
Dispositif de vigilance renforcée	Strengthened/enhanced /heightened vigilance measures	Sans objet	Sans objet
Domain name system, DNS	Système d'adressage par domaines	Système de bases de données et de serveurs assurant la correspondance entre les noms de domaine ou de sites utilisés par les internautes et les adresses numériques utilisables par les ordinateurs. Par exemple, le DNS établit la correspondance entre le domaine « cert.ssi.gouv.fr » et l'adresse 213.56.176.2. Ce système permet aux internautes d'utiliser, dans la rédaction des adresses, des noms faciles à retenir au lieu de la suite de chiffres du protocole IP.	System of databases and servers ensuring correspondence between domain or site names used by Internet users and numerical addresses usable by computers. For example, DNS maps the domain "cert.ssi.gouv.fr" to the address 213.56.176.2. This system enables Internet users to use easy-to-remember names when writing addresses, instead of the sequence of numbers used in the IP protocol.
DNS pharming	Dévoiement de serveur DNS	Modification d'un serveur DNS, dans le but de rediriger un nom de domaine vers une adresse IP différente de l'adresse légitime.	Modification of a DNS server to redirect a domain name to an IP address other than the legitimate one.
DNSSEC	Domain Name System Security Extensions	Extension pour la sécurité du protocole DNS	DNS protocol security extension
Donnée(s) à caractère personnel	Personal data (toujours au singulier)	Toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise. Une personne physique peut être identifiée directement (exemple : nom et prénom) ; indirectement (exemple : par un numéro de	Any information relating to an identified or identifiable natural person. But because it concerns individuals, they must retain control over it. A natural person can be identified directly (e.g. first and last name) or indirectly (e.g. by a telephone or license plate number, an identifier such

		téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).	as a social security number, a postal or e-mail address, but also by voice or image).

E

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
EBIOS Risk Manager	EBIOS Risk Manager	Méthode d'analyse de risque française de référence, permet aux organisations de réaliser une appréciation et un traitement des risques.	French risk analysis method, enables organizations to assess and treat risks.
Elevation de privilège	Privilege escalation	Obtention de privilège supérieur par exploitation d'une vulnérabilité. Par exemple, si un utilisateur local accède à des droits normalement réservés à l'administrateur, il y a élévation de privilège. Une élévation de privilège est souvent recherchée par une personne malveillante lorsqu'elle a réussi à s'introduire sur un système d'information en usurpant l'identité d'un utilisateur légitime.	Obtaining higher privileges by exploiting a vulnerability. For example, if a local user gains access to rights normally reserved for the administrator, this constitutes an elevation of privilege. An elevation of privilege is often sought by a malicious person who has succeeded in gaining access to an information system by usurping the identity of a legitimate user.
Espionnage	Espionage	Type d'attaque consistant pour un attaquant à prendre pied discrètement dans le système d'information de la victime pour en exfiltrer de l'information stratégique pour l'entreprise. Une telle attaque, souvent sophistiquée, peut durer plusieurs années avant d'être détectée.	A type of attack in which an attacker discreetly gains a foothold in the victim's information system, extracting information of strategic importance to the company. Such an attack, often sophisticated, can last several years before being detected.
Espiogiciel	Spyware	Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.	Software whose purpose is to collect and transmit to third parties information on the environment in which it is installed, and on the usual uses of the system's users, without the knowledge of the owner or user.
Etat de l'art	State of the art / State-of-the-art (avec traits d'union) si utilisé comme adjectif.	Ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.	A set of publicly accessible best practices, technologies and reference documents relating to information systems security, and the information that is obviously derived from them. These documents may be posted on the Internet by the information systems security community, disseminated by reference organizations, or be of regulatory origin.

Etat de la menace	Threat assessment	L'état de la menace caractérise, sur une période et un périmètre donnés, la nature et le niveau de risque atteints selon différentes variables telles que le type de menace, les acteurs concernés, les tendances observées, les modes opératoires à l'œuvre, les objectifs visés ou encore les moyens disponibles. Pour dresser ce panorama, l'ANSSI s'appuie sur une typologie de la menace en quatre catégories : cybercriminalité, déstabilisation, espionnage, sabotage.	Over a given period and perimeter, the threat assessment characterizes the nature and level of risk involved, based on various variables such as the type of threat, the actors involved, the trends observed, the modus operandi at work, the objectives targeted and the resources available. To draw up this overview, ANSSI has divided the threat into four categories: cybercrime, destabilization, espionage and sabotage.
European Union Agency for Cybersecurity	Agence de l'Union européenne de la cybersécurité (ENISA)	Sans objet	Sans objet
Évènements de sécurité	Security events	Evènements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.	Events brought to the attention of ANSSI and handled by operational teams.
Exécution de code arbitraire	Remote code execution (RCE)	Mise en œuvre de commandes à distance sur un ordinateur, à l'insu de son utilisateur légitime.	Implementation of remote commands on a computer, without the knowledge of its legitimate user.
Exfiltration de données	Data exfiltration (Data est toujours au singulier)	Vol ou transfert non autorisé des données depuis un terminal ou un réseau.	Theft or unauthorized transfer of data from a terminal or network.

F

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Faille, faille de sécurité	Vulnerability, security flaw, security breach	Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.	Vulnerability in a computer system enabling an attacker to undermine its normal operation, or the confidentiality or integrity of the data it contains.
Faux positif	False positive	Qualification erronée d'un évènement en tant qu'évènement de sécurité d'origine cyber.	Misclassification of an event as a cyber security event.
Federal Bureau of Investigation	Bureau Fédéral d'Investigation (FBI)	Sans objet	Sans objet
Federal Intelligence Service	Service fédéral de renseignement allemand (BND)	Sans objet	Sans objet
Federal Office for Information Security	Office fédéral de la sécurité des technologies de l'information (BSI)	Sans objet	Sans objet
Fournisseur d'accès à Internet (FAI)	Internet Service Provider (ISP)	Entreprise ou personne dont l'activité est d'offrir un accès à des services de communication au public en ligne, autrement dit à l'internet.	A company or person whose business is to provide access to online public communication services, in other words to the Internet.

Force-brute	Brute-force attack	Technique d'attaque consistant à utiliser un nombre exhaustif d'authentifiant générés aléatoirement afin de deviner le bon mot de passe.	An attack technique that uses an exhaustive number of randomly generated authenticators to guess the correct password.
Fraude à la carte bancaire	Skimming	Activité frauduleuse qui vise à pirater des cartes bancaires, notamment depuis des distributeurs de billets.	Fraudulent activity aimed at pirating bank cards, particularly from cash dispensers.
Front-office	Service de clientèle, guichet	Interface permettant d'accéder aux services en ligne.	Interface for accessing online services.

G

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Gestion de crise	Crisis management	Sans objet	Sans objet
Government Communications Headquarters	Quartier-général des communications du gouvernement (GCHQ)	Sans objet	Sans objet
Government Communications Security Bureau	Bureau néo-zélandais de la sécurité des communications du gouvernement (GCSB)	Sans objet	Sans objet
Guide technique	Technical guide	Sans objet	Sans objet

H

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Hachage (ou fonction de hachage)	Hash Function	Fonction cryptographique qui transforme une chaîne de caractères de taille quelconque en une chaîne de caractères de taille fixe et généralement inférieure. Cette fonction satisfait entre autres deux propriétés :la fonction est « à sens unique » : il est difficile pour une image de la fonction donnée de calculer l'antécédent associé. La fonction est « sans collision » : il est difficile de trouver deux antécédents différents de la fonction ayant la même image.	Cryptographic function that transforms a chain of characters of any size into a chain of characters of a fixed and generally smaller size. Among other things, this function satisfies two properties: the function is "one-way": for a given image of the function, it is difficult to calculate the associated antecedent. The function is "collision-free": it is difficult to find two different antecedents of the function with the same image.
Hacktiviste, Hacktivisme	Hacktivist, Hacktivism	Individus ayant pour 'objectif de véhiculer des messages et idéologies en ayant recours à différentes cyberattaques pour amplifier l'écho de leur action.	Individuals whose aim is to convey messages and ideologies by using cyber attacks to amplify the impact of their actions.
Hameçonnage ciblé	Spearphishing	Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne	This attack is generally based on the usurpation of the sender's identity, and uses strong social engineering to link the e-mail subject and message body to the activity of the targeted person or

		ou de l'organisation ciblée.	organization.
Homologation de sécurité	Security accreditation	L'homologation est délivrée par une autorité d'homologation pour un système d'information avant sa mise en service opérationnel. L'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré. Elle est imposée pour les systèmes d'information traitant des informations classifiées (IGI 1300) ou pour les télé-services dans le cadre du Référentiel Général de Sécurité (RGS).	Certification is issued by a certification authority for an information system before it is put into operational use. Certification identifies, achieves and maintains an acceptable level of security risk for the information system in question. It is mandatory for information systems handling classified information (IGI 1300), or for teleservices within the framework of the Référentiel Général de Sécurité (RGS).
Hub	Concentrateur	Dispositif informatique placé au nœud d'un réseau étoile, qui concentre et distribue les communications des données.	Computer device placed at the node of a star network, which concentrates and distributes data communications.

I

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Iframe	Cadre en ligne	L'iframe ou inline frame est une balise HTML utilisée pour insérer un document HTML dans une page HTML.	An iframe or inline frame is an HTML tag used to insert an HTML document into an HTML page.
Incident de sécurité	Security incident, event	Un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc. Dans la taxonomie de l'ANSSI : Evènements de sécurité pour lesquels l'ANSSI confirme qu'un acteur malveillant a conduit des actions avec succès sur le système d'information de la victime.	A security incident is an event that affects the availability, confidentiality or integrity of an asset. Example: illegal use of a password, theft of computer equipment, intrusion into a file or application, etc. in ANSSI taxonomy: Security events for which ANSSI confirms that a malicious actor has successfully carried out actions on the victim's information system.
Incident majeur	Major incident	Dans la taxonomie de l'ANSSI, un incident majeur est un incident dont la gravité et l'impact nécessite une intervention importante de l'ANSSI.	In ANSSI's taxonomy, a major incident is one whose severity and impact require a major intervention by ANSSI.
Indicateur de compromission (IOC) ou marqueur technique	Indicator of compromise (IOC) or Technical marker	Information technique, telle que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé, permettant de détecter et de caractériser une attaque. Le partage de ces éléments de connaissance permet notamment d'empêcher des compromissions futures. En revanche, de telles informations ne doivent parfois pas être	Technical information, such as the IP address of a malicious server or the name of a booby-trapped website, used to detect and characterize an attack. Sharing this knowledge helps prevent future compromises. On the other hand, such information may not need to be communicated if the attack has been prosecuted.

		communiquées si l'attaque a été judiciarisée.	
Infecter [1]	To contaminate	Notion de propagation.	
Infecter [2]	To infect	Localisé.	
Infogérance	Managed services, IT outsourcing	Prise en charge contractuelle, par un prestataire extérieur, d'une partie ou de la totalité des ressources informatiques d'une entreprise.	Contractual outsourcing of all or part of a company's IT resources.
Informatique en nuage	Cloud computing	Modèle permettant l'accès, généralement à la demande et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.	Model enabling access, generally on demand and via a network, to a set of shared and configurable IT resources.
Infrastructure de clés publiques (ICP)	Public key infrastructure (PKI)	Outil cryptographique permettant de garantir l'authenticité des clés publiques par la signature électronique d'autorités de certification organisées de façon hiérarchique. Une ICP est l'un des outils fondamentaux d'une IGC.	Cryptographic tool used to guarantee the authenticity of public keys through the electronic signature of hierarchically organized certification authorities. A PKI is one of the fundamental tools of a PKI.
Infrastructure de gestion de clés (IGC)	Public Key Infrastructure (PKI)	Ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs.	Organized set of components providing cryptographic key and public key certificate management services for a community of users.
Ingénierie sociale	Social engineering	Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes. Remarque : Il s'agit, pour les personnes malveillantes usant de ces méthodes, d'exploiter le facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information.	Manipulation to obtain goods or information by exploiting the trust, ignorance or credulity of third parties. Note: Malicious individuals using these methods exploit the human factor, which can in some cases be considered a weak link in information system security.
Injection de code indirecte	Cross Site Scripting, CSS, XSS	Activité malveillante qui consiste à injecter des données arbitraires dans le code de pages HTML. Un utilisateur malveillant peut faire afficher à un site web vulnérable un contenu agressif ; ce contenu peut rediriger l'utilisateur vers d'autres sites, ou transmettre des informations (jetons de sessions, aussi appelés cookies, etc.) ou des droits.	Malicious activity involving the injection of arbitrary data into the code of HTML pages. A malicious user can cause a vulnerable website to display aggressive content; this content can redirect the user to other sites, or transmit information (session tokens, also known as cookies, etc.) or rights.
Intégrité	Integrity	Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.	Guarantee that the system and the information processed are only modified by a voluntary and legitimate action.
Intrusion	Intrusion	L'intrusion est le fait, pour une personne ou un objet, de pénétrer dans un espace (physique, logique, relationnel) défini où sa présence n'est pas souhaitée.	Intrusion is the act of a person or object entering a defined space (physical, logical, relational) where its presence is not desired.

K

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Keylogger	Enregistreur de frappes	Logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au clavier.	Software or hardware used by a malicious user to capture what a person types on the keyboard.

L

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Levée de doute	Removal of doubt	Ensemble d'actions de vérification effectué pour confirmer ou infirmer une alerte ou un signalement de sécurité informatique.	Set of verification actions carried out to confirm or invalidate a computer security alert or report.
Logiciel de contrôle parental ou de filtrage	Parental control software or filtering	Il s'agit de systèmes de protection qui s'installent sur un ordinateur et qui permettent notamment de bloquer l'accès aux sites inappropriés aux plus jeunes. Certains permettent également de paramétrer l'accès à l'internet (plages horaires, durée, applications…). Tout ordinateur personnel utilisé par un mineur devrait en être équipé (voir résultats du comparatif des principaux logiciels existants sur le marché).	These are protection systems that can be installed on a computer to block access to sites unsuitable for children. Some can also be used to configure Internet access (time slots, duration, applications, etc.). All personal computers used by minors should be equipped with such software (see the results of our comparison of the main software available on the market).
Loi de programmation militaire (LPM)	Critical Information Infrastructure Protection Law (LPM/ loi de protection militaire (Critical Information Infrastructure Protection law) Sigle anglais : CIIP law.	Nom français de la loi à utiliser *a minima* pour la première occurrence. Sans objet	Sans objet
Loi pour une République numérique	Loi pour une République numérique (Law for a Digital Republic)	Sans objet	Sans objet

M

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
MaaS (malware as a service)	Maliciel en tant que service	Sans objet	Sans objet
Malware	Maliciel	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau.	Program developed for the purpose of harming an IT system. Note: viruses or worms are two known types of malware.

Man in the cloud	Homme dans le nuage	Attaque donnant un accès distant au réseau via les espaces en nuage, permettant d'exfiltrer des données et d'exécuter des commandes arbitraires.	Attack giving remote access to the network nia cloud spaces, allowing data to be exfiltrated and arbitrary commands to be executed.
Man-in-the-middle	Homme-au-milieu-entre-deux	Catégorie d'attaque où une personne malveillante s'interpose dans un échange de manière transparente pour les utilisateurs ou les systèmes. Remarque : La connexion est maintenue, soit en substituant les éléments transférés, soit en les réinjectant. Une attaque connue dans cette catégorie repose sur une compromission des tables ARP (ARP Poisoning). Contrer les attaques par le milieu est aussi l'un des objectifs des infrastructures de gestion de clés.	A category of attack in which a malicious person interferes with an exchange in a way that is transparent to users or systems. Note: The connection is maintained, either by substituting the transferred elements, or by reinjecting them. A well-known attack in this category involves compromising ARP tables (ARP Poisoning). Countering attacks from the middle is also one of the objectives of key management infrastructures.
Marqueur de compromission	Indicator of Compromise (IOC)	Information technique, telle que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé, permettant de détecter et de caractériser une attaque. Le partage de ces éléments de connaissance permet notamment d'empêcher des compromissions futures. En revanche, de telles informations ne doivent parfois pas être communiquées si l'attaque a été judiciarisée.	Technical information, such as the IP address of a malicious server or the name of a spoofed website, allowing an attack to be detected and characterised. The sharing of these elements of knowledge is particularly helpful in preventing future compromises. Conversely, such information is sometimes not to be communicated if the attack is the subject of criminal proceedings.
Menace numérique	Digital threat	Terme générique utilisé pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l'objet de l'étude.	Generic term used to designate any hostile intention to do harm in cyberspace. A threat may or may not be targeted on the object of study.
Microblog	Microblogue	Blogue constitué de minimessages diffusés en temps réel, qui contiennent souvent des mots-dièse et dont l'enchaînement forme des fils de discussion.	A blog made up of short messages posted in real time, often containing keywords and linked together to form discussion threads.
Mode opératoire d'attaque, d'un attaquant (MOA) ou d'un groupe d'attaquants	The tactics, techniques and procedures (TTPS) of an attacker or group of attackers	Signature de l'attaquant, sa façon d'opérer pour cibler et attaquer ses victimes.	The attacker's signature, the way he targets and attacks his victims.
Modèle français de cybersécurité	French cyber security model	Le modèle français de cybersécurité et de cyberdéfense repose sur une séparation claire, au sein de l'État, entre les missions défensives et offensives.	The French model of cybersecurity and cyberdefense is based on a clear separation, within the State, between defensive and offensive missions.
Mois européen de la cybersécurité	European Cybersecurity Month (ECSM) Parfois, l'abréviation « ECSM » est utilisée en	Le Mois européen de la cybersécurité est une initiative conçue par l'Agence de l'Union européenne pour la cybersécurité	European Cybersecurity Month is an initiative of the European Union's Cybersecurity Agency (ENISA). It aims to promote the subject of

	français.	(ENISA). Elle vise à promouvoir le sujet de la cybersécurité à travers les pays de l'UE pour permettre de mieux comprendre les menaces et les appréhender.	cybersecurity across EU countries, to help people better understand and tackle threats.
Moisson de courriels	Mail harvesting	Action qui consiste à parcourir un grand nombre de ressources publiques (pages internet, groupes de discussion, etc.), afin d'y collecter les adresses électroniques avec des intentions malveillantes. **Remarque** : Les adresses récupérées sont utilisées, par exemple, pour envoyer des courriels contenant des virus, des canulars ou des pourriels. Une méthode pour s'en prémunir est de présenter sur ces ressources publiques une adresse électronique qui trompe les outils de recherche (comme prenom.nom_AT_domain.fr pour les outils cherchant '@', caractéristique d'une adresse) ; ceci est appelé address munging.	Action which consists of scanning a large number of public resources (Internet pages, newsgroups, etc.), in order to collect e-mail addresses with malicious intent. **Note:** The addresses collected are used, for example, to send e-mails containing viruses, hoaxes or spam. One way to prevent this is to present an e-mail address on these public resources that misleads search tools (such as prenom.nom_AT_domain.fr for tools looking for '@', the characteristic of an address); this is called address munging.
Mot de passe	Password	Un mot de passe est un élément de déverrouillage servant dans la vérification de l'identité annoncée d'une personne par un système d'information.	A password is an unlocking element used in the verification of a person's announced identity by an information system.
Mouchard internet	Web bug	Support graphique implanté dans une page internet ou un courriel, qui a pour objectif de surveiller la consultation de cette page ou de ce courriel, à l'insu des lecteurs. Remarque : ces supports sont souvent invisibles, car beaucoup sont paramétrés avec une taille très petite (1X1 pixel). Ils sont aussi fréquemment représentés par des balises HTML IMG.	Graphical support embedded in an Internet page or e-mail, whose purpose is to monitor the viewing of this page or e-mail, without the readers' knowledge. Note: these supports are often invisible, as many are set to a very small size (1X1 pixel). They are also frequently represented by HTML IMG tags.

N

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
National Center of Incident Readiness and Strategy for Cybersecurity	Centre national japonais pour la réponse à incident et de stratégie en matière de cybersécurité (NISC)	Sans objet	Sans objet
National Cybersecurity Center	Centre National pour la Cybersécurité (en spécifiant le pays auquel est attaché la structure) (NCSC)	Sans objet	Sans objet
National Security Agency	Agence Nationale de Sécurité (service de renseignement	Sans objet	Sans objet

	américain) (NSA)		
National Security Authority	Autorité norvégienne de sécurité nationale (NSM)	Sans objet	Sans objet
Nomadisme numérique	Digital mobility	Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.	Digital nomadism refers to any form of information technology use that enables a user to access the IS of the entity to which they belong or where they work, from remote locations that are not controlled by the entity.
Noyau (noyau de système d'exploitation)	Kernel	Une des parties fondamentales de certains systèmes d'exploitation. Il gère les ressources de l'ordinateur et permet aux différents composants (matériels et logiciels) de communiquer entre eux.	One of the fundamental parts of certain operating systems. It manages the computer's resources and enables the various components (hardware and software) to communicate with each other.
Numéroteur	Dialer	Logiciel qui compose automatiquement des numéros de téléphone. **Remarque :** les numéroteurs sont souvent proposés pour accéder à des sites à caractères pornographique (appels surtaxés). Par extension, un war dialer est une application composant une liste de numéros, et qui enregistre ceux retournant une tonalité spéciale, comme un modem ou un fax.	Software that automatically dials telephone numbers. **Note:** dialers are often used to access pornographic sites (premium rate calls). By extension, a war dialer is an application that composes a list of numbers, and records those returning a special tone, like a modem or fax.
Numérisation [1]	Digitalisation/ scanning	D'un document, de données analogiques.	From a document, analog data.

O

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Opérateur de service essentiel (OSE)	Operator of essential services (OES) Le sigle anglais est utilisé car il renvoie à une notion européenne.	Un OSE est un opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.	An OES is an operator dependent on networks or information systems, providing an essential service whose interruption would have a significant impact on the functioning of the economy or society.
Opérateur d'importance vitale (OIV)	Operator of critical national infrastructures (OIV), French operator. Le sigle français est conservé.	Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.	Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.
Opération de cyberdéfense	Cyber defence operation	Dans la taxonomie de l'ANSSI, une opération de cyberdéfense constitue le niveau maximal d'engagement de l'Agence dans le traitement d'un	In ANSSI's taxonomy, a cyber defense operation is the Agency's maximum level of commitment in dealing with a security event. This

		événement de sécurité. Cet engagement est réservé aux événements dont la gravité et la complexité sont significatives.	commitment is reserved for events whose of significant severity and complexity.

P

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Pare-feu	Firewall	Un pare-feu (ou garde barrière), est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.	A firewall is a tool used to protect a computer connected to a network or the Internet. It protects against external attacks (inbound filtering) and often against illegitimate connections to the outside world (outbound filtering) initiated by programs or people.
Password spraying	Arrosage de mot de passe	Fait de tenter l'ouverture de plusieurs comptes avec un seul mot de passe, souvent très utilisé.	Attempting to open several accounts with a single password, often widely used.
Peer-to-peer (P2P)	Poste-à-poste	Réseau où chaque entité est à la fois client et serveur. Réseau d'échange et de partage de fichiers de particulier à particulier.	Network where each entity is both client and server. Network for exchanging and sharing files between individuals.
Phishing	Hameçonnage, Filoutage	Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.	Fraudulent technique intended to deceive the Internet user by posing as a trusted third party (fake SMS, email, etc.) to prompt them to communicate personal data (access accounts, passwords, etc.) and/or bank details. This type of attack can be used for both an espionage attack and a ransomware attack.
Pirate informatique	Computer hacker	On appelle communément pirate l'auteur d'une attaque informatique.	The term "hacker" is commonly used to describe the perpetrator of a computer attack.
Plan de continuité d'activité (PCA)	Business continuity plan (BCP)	Ensemble de procédures documentées servant de guides aux entités pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation.	Set of documented procedures to guide entities in responding to, restoring, resuming and recovering a predefined predefined level of operation following a disturbance.
Plan de reprise d'activité (PRA)	Disaster recovery plan (DRP)	Procédures documentées permettant aux entités de rétablir et de reprendre leurs activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident.	Documented procedures enabling entities to restore and resume their activities based on temporary measures adopted to meet normal business requirements after an incident.
Plan de remédiation	Remedial plan	Plan visant à la reconstruction d'un SI à la suite d'une attaque.	Plan to rebuild an IS following an attack.

Point d'eau (Attaque par)	Watering hole	Ce type d'attaque est destiné à infecter les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée. La technique du « point d'eau » consiste à piéger un site Internet légitime afin d'infecter les machines des visiteurs du domaine d'intérêt pour l'attaquant. Les cas sont nombreux de sites d'associations professionnelles ou de groupements sectoriels insuffisamment sécurisés et dont les vulnérabilités sont exploitées pour contaminer leurs membres, et permettre ainsi d'accéder aux réseaux les plus sensibles de ceux-ci. Les secteurs les plus stratégiques sont évidemment les plus ciblés.	This type of attack is designed to infect the computers of personnel working in a targeted industry or organization. The "watering hole" technique involves tricking a legitimate website into infecting the machines of visitors in the attacker's area of interest. There are numerous cases of insufficiently secure sites belonging to professional associations or industry groups, whose vulnerabilities are exploited to infect their members, thereby enabling access to their most sensitive networks. The most strategic sectors are obviously the most targeted.
Polymorphe	Polymorphic	Se dit d'un ver ou d'un virus dont le code est chiffré, changeant le code de déchiffrement d'une infection à l'autre, et donc l'apparence et/ou la signature.	A worm or virus whose code is encrypted, changing the decryption code from one infection to the next, and thus its appearance and/or signature.
Port	Port	Code numérique utilisé dans les protocoles comme TCP ou UDP pour identifier à quel service appartient un paquet d'information du protocole IP. Par exemple, le service http est associé au port 80. La notion de port peut être assimilée à une porte donnant accès au système d'exploitation.	Numeric code used in protocols such as TCP or UDP to identify to which service an IP protocol information packet belongs. For example, the http service is associated with port 80. The notion of a port can be likened to a door giving access to the operating system.
Prestataire de sécurité (général)	MSSP (Managed Security Service Provider)	Entité proposant une offre de service de sécurité des systèmes d'information conforme au référentiel.	Entity offering an information systems security service that complies with the standard.
Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) – référentiel d'exigences	Cyber security support and consulting service provider (PACS) - requirements framework	Le référentiel PACS a pour objectif d'assister les responsables de la sécurité des systèmes d'information et leurs équipes dans leurs missions de protection des systèmes d'information, et notamment d'homologation de sécurité, de gestion des risques, de conception d'architectures sécurisées, et de préparation à la gestion de crises d'origine cyber.	The PACS standard is designed to support information systems security managers and their teams in their missions to protect information systems, including security certification, risk management, design of secure architectures, and preparation for the management of cyber-related crises.
Prestataires d'administration et de maintenance sécurisées (PAMS) – référentiel d'exigences	Secure administration and maintenance service provider (PAMS) - requirements framework	Le référentiel d'exigences relatif aux prestataires d'administration et de maintenance sécurisées est un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services dans ce domaine. Il couvre des exigences relatives aux prestataires d'administration et de maintenance	The requirements framework for secure administration and maintenance service providers is a set of rules for service providers wishing to qualify their services in this field. It covers requirements relating to secure administration and maintenance providers, their staff and the way in which services are

		sécurisées, à son personnel ainsi qu'au déroulement des prestations.	provided.
Prestataire d'audit de la sécurité des systèmes d'information (PASSI) – référentiel d'exigences	Cyber security audit service provider (PASSI) - requirements framework	Le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information est un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services dans ce domaine. Il couvre des exigences relatives au prestataire d'audit, à son personnel ainsi qu'au déroulement des audits. La qualification peut être délivrée aux prestataires d'audit pour les activités suivantes : audit d'architecture, audit de configuration, audit de code source, tests d'intrusion, audit organisationnel et physique.	The requirements framework for information systems security auditors is a set of rules for service providers wishing to qualify their services in this field. It covers requirements relating to the audit provider, its staff and the conduct of audits. Qualification can be awarded to audit providers for the following activities: architecture audit, configuration audit, source code audit, penetration testing, organizational and physical audit.
Prestataire de détection d'incidents de sécurité (PDIS) – référentiel d'exigences	Cyber security incident detection service provider (PDIS) - requirements framework	Le référentiel d'exigences relatif aux prestataires de détection des incidents de sécurité est un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services dans ce domaine. Il couvre des exigences relatives au prestataire de détection des incidents, à son personnel ainsi qu'au déroulement des prestations de détection des incidents. La qualification peut être délivrée aux prestataires de détection des incidents pour l'ensemble de l'activité de détection d'incidents de sécurité.	The requirements framework for security incident detection service providers is a set of rules for service providers wishing to qualify their services in this field. It covers requirements relating to the incident detection service provider, its staff and the way in which incident detection services are carried out. Qualification can be awarded to incident detection providers for their entire security incident detection activity.
Prestataire de réponse aux incidents de sécurité (PRIS) – référentiel d'exigences	Cyber security incident response service provider (PRIS) - requirements framework	Le référentiel d'exigences relatif aux prestataires de réponse aux incidents de sécurité est un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services dans ce domaine. Il couvre des exigences relatives au prestataire de réponse aux incidents, à son personnel ainsi qu'au déroulement des prestations de réponse aux incidents. La qualification peut être délivrée aux prestataires de réponse aux incidents pour les activités suivantes : pilotage technique, analyse système, analyse réseau et analyse de codes malveillants.	The requirements framework for security incident response providers is a set of rules for providers wishing to qualify their services in this field. It covers requirements relating to the incident response provider, its staff and the way in which incident response services are carried out. Qualification can be awarded to incident response providers for the following activities: technical control, system analysis, network analysis and malicious code analysis.
Prestataire de service informatique dans le nuage (SecNumCloud) –	Cloud computing service provider (SecNumCloud) - requirements framework	Le référentiel d'exigences relatif aux prestataires de service d'informatique en nuage est un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir	The requirements framework for cloud computing service providers is a set of rules for providers wishing to qualify their services in this field. It covers requirements relating to the

référentiel d'exigences		une qualification de leurs services dans ce domaine. Il couvre des exigences relatives au prestataire de service d'informatique en nuage, à son personnel ainsi qu'au déroulement des prestations. La qualification peut être délivrée aux prestataires de service d'informatique en nuage pour des services de type SaaS (Software as a service), PaaS (Platform as a service) et IaaS (Infrastructure as a service.	cloud computing service provider, its staff and the provision of services. Qualification can be issued to cloud computing service providers for SaaS (Software as a service), PaaS (Platform as a service) and IaaS (Infrastructure as a service) services.
Prestataire de service de confiance [qualifié] – référentiel d'exigences	[Qualified] Trust Service Provider (TSP) - requirements framework	Les référentiels d'exigences relatifs aux prestataires de services de confiance formalisent les règles applicables aux organismes désirant obtenir une qualification dans les domaines suivants : délivrance de certificats électroniques, horodatage électronique, validation des signatures et cachets électroniques, conservation des signatures et cachets électroniques, envoi recommandé électronique.	The repositories of requirements for trust service providers formalize the rules applicable to organizations wishing to obtain qualification in the following areas: issuance of electronic certificates, electronic time stamping, validation of electronic signatures and stamps, preservation of electronic signatures and stamps, electronic registered mail.
Produit de sécurité	Security product	Dispositif matériel ou logiciel conçu pour protéger la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que les systèmes d'information offrent ou qu'ils rendent accessibles.	A hardware or software device designed to protect the availability, integrity or confidentiality of stored, processed or transmitted data and related services that information systems offer or make accessible.
Protocole IP	Internet Protocol	La communication sur l'internet est fondée sur un protocole appelé IP pour Internet Protocol qui permet aux ordinateurs de communiquer entre eux.	Internet communication is based on a protocol called IP for Internet Protocol, which enables computers to communicate with each other.

Q

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Qualification	Qualification	Son objectif est de s'assurer qu'un produit de sécurité (matériel ou logiciel) ou qu'un prestataire de services de confiance répond aux besoins de l'administration.	Its aim is to ensure that a security product (hardware or software) or a trusted service provider meets the needs of the administration.

R

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Rançongiciel/ Logiciel rançonneur	Ransomware	Programme malveillant dont le but est d'obtenir de la victime le paiement	Malicious program designed to obtain payment of a ransom from the victim.

		d'une rançon. Les rançongiciels figurent au catalogue des outils auxquels ont recours les cybercriminels motivés par l'appât du gain. Lors d'une attaque par rançongiciel, l'attaquant met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible. L'attaquant adresse alors un message non chiffré à la victime où il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données. **Ressources** : https://cyber.gouv.fr/sites/default/files/2022-08/rancongiciel_infographie_anssi%5B1%5D.pdf Rançongiciel ou ransomware, que faire ? : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes	Ransomware is one of the tools used by profit-driven cybercriminals. In a ransomware attack, the attacker reversibly disables the victim's computer or information system. The attacker then sends an unencrypted message to the victim, offering to decrypt the victim's data in return for payment of a ransom. **Resources**: https://cyber.gouv.fr/sites/default/files/2022-08/rancongiciel_infographie_anssi%5B1%5D.pdf Rançongiciel ou ransomware, que faire ? : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
Reconstruction (SI)	Rebuilding	La reconstruction est une activité support à la remédiation ayant pour objectif de lui fournir les moyens informatiques nécessaires à la remise en fonction et en conditions de sécurité du système d'information.	Reconstruction is a support activity for remediation, the aim of which is to provide the IT resources needed to restore and security conditions of the information system.
Référentiel d'exigences [1]	Requirements rules set, Requirements baseline	Le référentiel d'exigences est un ensemble de règles qui s'imposent aux prestataires qui désirent obtenir une qualification de leurs services dans un domaine.	The requirements repository is a set of rules for service providers wishing to qualify their services in a given field.
Règle de détection	Detection rule	Une règle de détection est une combinaison de symptômes observables au niveau d'une source de données, dont la survenue est caractéristique d'une activité suspecte ou malveillante. Selon la méthode de détection et le niveau de sophistication de la règle de détection utilisée pour caractériser les événements malveillants, on parle également de marqueur, de signature d'attaque, ou de règle comportementale.	A detection rule is a combination of symptoms observable at a data source, the occurrence of which is characteristic of suspicious or malicious activity. Depending on the detection method and the level of sophistication of the detection rule used to characterize malicious events, it is also referred to as a marker, attack signature or behavioral rule.
Référentiel général de sécurité (RGS)	General Security Baseline	Ensemble des règles établies par l'ANSSI et prévues par l'ordonnance no 2005-1516 du 8 décembre 2005 « relative aux échanges électroniques	A set of rules established by ANSSI and set out in Order no. 2005-1516 of December 8, 2005 "relating to electronic exchanges between users

		entre les usagers et les autorités administratives et entre les autorités administratives » que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage.	and administrative authorities and between administrative authorities", which must be respected by certain functions contributing to information security, including electronic signature, authentication, confidentiality and time stamping.
Règlement général sur la protection des données à caractère personnel (RGPD)	General Data Protection Regulation (GDPR)	Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne. La CNIL est notamment en charge de traiter les plaintes et de développer de nouveaux outils de conformité pour garantir à tous la protection des données personnelles. **Ressource :** https://www.cnil.fr/fr	Regulates the processing of personal data within the territory of the European Union. The CNIL in particular is in charge of handling complaints and developing new compliance tools to guarantee the protection of personal data for all. **Resource:** https://www.cnil.fr/en
Remédiation	Remediation	La remédiation consiste en la reprise de contrôle d'un système d'information compromis et le rétablissement d'un état de fonctionnement suffisant du service. La remédiation est l'une des dimensions majeures de la réponse à incident suite à une attaque cyber, avec l'investigation et la gestion de crise. C'est un travail qui commence dès l'endiguement de l'action adverse et qui peut s'étendre sur plusieurs mois. (Site ANSSI)	Remediation consists in regaining control of a compromised information system and restoring the service to a sufficiently functional state. Remediation is one of the major aspects of incident response to a cyber attack, along with investigation and crisis management. It begins as soon as the hostile action is contained, and can extend over several months (ANSSI website).
Remédier	To mitigate	Cf définition de « Remédiation »	Cf définition of « Remediation »
Renifleur	Sniffer	Outil matériel ou logiciel dont l'objet est de capturer les trames transitant sur le réseau. **Remarque :** Si les trames contiennent des données non chiffrées, un utilisateur malveillant peut aisément récupérer des données confidentielles, comme des mots de passe, des courriers électroniques, des contenus de pages internet, etc. L'utilisateur malveillant peut aussi, à partir des trames, récupérer des informations sur les systèmes échangeant les trames, comme le système d'exploitation ou les services employés.	Hardware or software tool whose purpose is to capture frames transiting the network. **Note:** If the frames contain unencrypted data, a malicious user can easily retrieve confidential data, such as passwords, e-mails, web page content, etc. The malicious user can also use the frames to retrieve information about the systems exchanging the frames, such as the operating system or services used.

Réseau d'anonymisation	Anonymisation network	Réseau de machines compromises communiquant entre elles, utilisées par un groupe d'attaquants afin de rendre ses opérations plus furtives.	Network of compromised machines communicating with each other, used by a group of attackers to make their operations stealthier.
Résilience	Resilience	En informatique, capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident.	In IT, the ability of an information system to resist a breakdown or cyber-attack and return to its initial state after the incident.

Revue stratégique de cyberdéfense	Strategic review of cyber defence	Livre blanc de la cyberdéfense, il est un grand exercice de synthèse stratégique dans ce domaine.	The White Paper on Cyberdefense is a major exercise in strategic synthesis in this field.
Rootkit	Outil de dissimulation d'activité	Tout programme ou ensemble de programmes permettant à une personne de maintenir un contrôle illégitime du système d'information en y dissimulant ses activités. L'installation de ces programmes nécessite que le système soit préalablement compromis.	Any program or set of programs enabling a person to maintain illegitimate control of an information system by concealing his or her activities. Installation of such programs requires the system to have been compromised previously.

S

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Sabotage	Sabotage	Une opération de sabotage consiste, pour un individu ou un groupe d'individus, à conduire une attaque génératrice de dommages sur le système d'information de l'entité ciblée pouvant aller jusqu'à le rendre inopérant. Les conséquences d'une telle opération peuvent être désastreuses, en particulier si cette opération touche un secteur d'importance vitale comme la santé, le transport ou encore l'énergie.	A sabotage operation involves an individual or a group of individuals carrying out an attack that causes damage to the target entity's information system, or even renders it inoperative. The consequences of such an operation can be disastrous, particularly if it affects a vitally important sector such as health, transport or energy.
Scanning (ou "scan" utilisé en "français")	Balayage réseau	Technique servant à rechercher des appareils connectés spécifiques ainsi que des informations relatives à ceux-ci. Cette technique peut également servir à identifier la présence de vulnérabilités connues sur des systèmes exposés.	A technique used to search for specific connected devices and related information. This technique can also be used to identify the presence of known vulnerabilities on exposed systems.
Schéma d'attaque	Attack path	Sans objet	Sans objet
[Le] Secrétariat général de la défense et de la sécurité nationale (SGDSN)	[the] General Secretariat for Defence and National Security (SGDSN)	Placé au cœur de l'exécutif, le SGDSN, qui lui est rattaché, assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Il assure le secrétariat des conseils de défense et de sécurité nationale que préside le chef de l'Etat. Il agit ainsi en appui de la prise de décision politique. Son champ d'intervention couvre l'ensemble des questions stratégiques de défense et de sécurité, dans le domaine de la programmation militaire, de la politique de dissuasion, de la sécurité intérieure concourant à la sécurité nationale, de la sécurité économique et énergétique, de la lutte contre le terrorisme et de la planification des réponses aux crises.	Placed at the heart of the executive branch, the SGDSN, which reports to the Prime Minister, assists him in exercising his responsibilities in terms of national defense and security. It acts as secretary to the national defense and security councils chaired by the Head of State. It thus supports political decision-making. Its remit covers all strategic defense and security issues, including military programming, deterrence policy, internal security contributing to national security, economic and energy security, the fight against terrorism, and crisis response planning.

Secteur d'activité d'importance vitale	Critical sector	À la suite des attentats du 11 septembre 2001, la France a engagé une réflexion sur la notion d'infrastructure critique afin de moderniser la protection des points et des réseaux sensibles. Le décret du 23 février 2006↗ définit les activités d'importance vitale comme « un ensemble d'activités, essentielles et difficilement substituables ou remplaçables, concourant à un même objectif ou visant à produire et à distribuer des biens ou des services indispensables ». Douze secteurs d'activité d'importance vitale ont été définis dans un arrêté du 2 juin 2006, modifié par un arrêté du 3 juillet 2008, au sein desquels ont identifiés des Opérateurs d'importance vitale (OIV) chargés de la protection de leur Point d'importance vitale (PIV). Chaque secteur est rattaché à un ministère coordonnateur chargé du pilotage des travaux et des consultations.	In the aftermath of the September 11, 2001 attacks, France launched a review of the concept of critical infrastructure, with a view to modernizing the protection of sensitive points and networks. The decree of February 23, 2006 defines activities of vital importance as "a set of activities, essential and difficult to substitute or replace, working towards the same objective or aiming to produce and distribute essential goods or services". Twelve sectors of vital importance were defined in a decree of June 2, 2006, amended by a decree of July 3, 2008, within which Operators of Vital Importance (OIV) were identified, responsible for protecting their Point of Vital Importance (PIV). Each sector is attached to a coordinating ministry responsible for steering the work and consultations.
Sécurité des systèmes d'information (SSI) [1]	Cyber security, Information System Security (ISS)	Ensemble des moyens techniques et non-techniques de protection permettant à un système d'information d'assurer la disponibilité, l'intégrité et la confidentialité des données, traitées ou transmises, et des services connexes que ces systèmes offrent ou rendent accessibles.	All the technical and non-technical means of protection that enable an information system to ensure the availability, integrity and confidentiality of the data processed or transmitted, and of the related services that these systems offer or make accessible. accessible.
Security Service	Service de la sûreté britannique (MI5)	Sans objet	Sans objet
Sensibilisation, Campagne de sensibilisation	Awareness raising, awareness campaign.	Sans objet	Sans objet
Serveur racine ou serveur de noms de la racine	Root name server	La racine, en informatique, est le point de départ d'une arborescence. Il existe actuellement 13 serveurs de noms de la racine répartis dans le monde : ces serveurs hébergent les données permettant le bon fonctionnement du Système d'adressage par domaines (DNS) et des services qui utilisent ce système : internet, courrier électronique…	In computing, the root is the starting point of a tree structure. There are currently 13 root name servers around the world: these servers host the data required for the Domain Name System (DNS) to function properly, as well as the services that use this system: the Internet, e-mail...
Service européen pour l'action extérieure (SEAE)	European External Action Service (EEAS)	Sans objet	Sans objet
Services de confiance	Trust services	Cf « Prestataire de service de confiance »	CF "Trust Service Provider"
Shadow IT	Informatique de l'ombre/ informatique cachée	Désigne des SI réalisés et mis en œuvre au sein d'organisations sans	IS designed and implemented within organizations without the

		l'approbation de la DSI.	approval of the CIO department.
Signalement	Alert	Dans la taxonomie de l'ANSSI, un signalement est un événement de sécurité d'origine cyber avec un impact pour le SI de la victime bas (ex : hammeçonage), requérant une intervention minimum de l'Agence.	In the ANSSI taxonomy, an alert is a security event of cyber origin with a low impact on the victim's IS (e.g. hammoning), requiring minimum intervention by the Agency.
Signalement d'incident/ Signalement d'événement de sécurité numérique	Incident notification	On qualifie de signalement d'incident toute description détaillée des caractéristiques techniques d'un ou plusieurs événements de sécurité susceptibles de conduire à la découverte d'un incident de sécurité survenu sur le système d'information d'une organisation donnée.	An incident notification is any detailed description of the technical characteristics of one or more security events likely to lead to the discovery of a security incident on a given organization's information system.
Sous-direction expertise (SDE)	SDE (Expertise Department)	La sous-direction Expertise élabore et diffuse les bonnes pratiques et contribue à améliorer l'offre de produits et services cyber, pour accompagner la sécurisation des bénéficiaires de l'Agence.	The Expertise Deparment develops and disseminates best practices, and contributes to improving the range of cyber products and services, to support the security of the Agency's beneficiaries.
Sous-direction opérations (SDO)	SDO (Operations Department)	La sous-direction Opérations assure, au niveau opératif et tactique, la mise en œuvre de la fonction d'autorité de défense des systèmes numériques d'intérêt pour la nation dévolue à l'ANSSI. Elle constitue le centre opérationnel de la sécurité des systèmes d'information.	The Operations Department is responsible, at the operational and tactical levels, for implementing the ANSSI's role as defence authority for digital systems of national interest. It is the operational centre for information systems security.
Sous-direction stratégie (SDS)	SDS (Strategy Department)	La sous-direction Stratégie anime le processus de planification stratégique au sein de l'Agence, en assurant notamment le secrétariat du comité directeur de la stratégie. Elle développe et pilote la contribution de l'Agence à l'élaboration et à la mise en œuvre des politiques publiques en faveur de la sécurité du numérique ; communique vers l'ensemble des publics sur les enjeux de sécurité numérique, notamment à des fins de sensibilisation, et met à leur service les capacités de l'Agence, dans le respect des priorités nationales.	The Strategy Department leads the strategic planning process within the Agency, in particular by providing the secretariat for the Strategy Steering Committee. It develops and manages the Agency's contribution to the development and implementation of public policies in favour of digital security; communicates with all audiences on digital security issues, particularly for awareness-raising purposes, and makes the Agency's capabilities available to them, in line with national priorities.
Sous-direction ressources (SDR)	SDR (Resources Department)	A vocation transverse, la sous-direction Ressources (SDR) est responsable de la programmation et de l'exécution des activités de gestion et de pilotage des ressources financières, humaines, mobilières et immobilières, et de l'expertise et de l'accompagnement légal. A travers son activité la sous-direction Ressources soutient l'activité de l'Agence. Elle est l'interlocuteur privilégié du service de	The Resources Department has a cross-functional remit and is responsible for programming and carrying out activities relating to the management and steering of financial, human, movable and property resources, as well as expertise and legal support. Through its activities, the Resources Sub-Directorate supports the agency's activities. It is the main point of contact for the

		l'administration générale du SGDSN.	SGDSN's general administration department.
Spam	Pourriel, polluriel	Tout courrier électronique non sollicité par le destinataire. Le courrier est souvent envoyé simultanément à un très grand nombre d'adresses électroniques. Les produits les plus vantés sont les services pornographiques, la spéculation boursière, des médicaments, le crédit financier etc.	Any unsolicited e-mail. The mail is often sent simultaneously to a very large number of e-mail addresses. The most frequently advertised products are pornographic services, stock market speculation, medicines, financial credit, etc.
Supply chain attack	Attaque contre la chaîne logistique	Ce type d'attaque consiste à compromettre un tiers, comme un fournisseur de services logiciels ou un prestataire, afin de cibler la victime finale. Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et cybercriminels depuis au moins 2016. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible un fournisseur de logiciels largement répandus, une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier.	This type of attack involves compromising a third party, such as a software service provider or contractor, in order to target the end victim. This technique has been tried and tested and exploited by several state actors and cybercriminals since at least 2016. This method presents a risk of rapid propagation of an attack, which can sometimes affect an entire business sector or a precise geographical area, particularly when the attack targets a widely used software supplier, a local digital service company (ESN) or one specialized in a particular business sector.
Système de détection d'intrusion	Intrusion Detection System (IDS)	Un système de détection d'intrusion (Intrusion Detection System - IDS) est un dispositif logiciel ou matériel dont le rôle est de capter, puis d'analyser, l'activité d'un système numérique, dans le but de détecter les attaques ou les signes de compromission dont ce dernier est la cible. Un IDS se caractérise par la source de donnée utilisée pour capter l'activité d'un système (réseau, système, applicative) et par la méthode de détection employée pour distinguer les activités malveillantes des activités légitimes.	An Intrusion Detection System (IDS) is a software or hardware device whose role is to capture and analyze the activity of a digital system, with the aim of detecting attacks or signs of compromise. An IDS is characterized by the data source used to capture system activity (network, system, application) and by the detection method used to distinguish malicious from legitimate activity.
Système d'information (SI)	Information system (IS)	Ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l'information.	Organized set of resources (hardware, software, personnel, data and procedures) used to process and distribute information.
Système d'information d'administration	Administration information system	C'est l'ensemble des ressources matérielles et logicielles nécessaires pour réaliser les tâches d'administration. Il inclut le système d'exploitation du poste de travail utilisé pour les tâches d'administration qui peut être soit l'unique système d'exploitation d'un poste de travail physiquement dédié,	This is the set of hardware and software resources required to perform administration tasks. It includes the operating system of the workstation used for administration tasks, which can be either the sole operating system of a physically dedicated workstation, or the runtime environment in the

		soit l'environnement d'exécution dans le cas d'un poste de travail mettant en œuvre une virtualisation légère, soit le système d'exploitation de la machine virtuelle d'un poste de travail virtualisé.	case of a workstation implementing light virtualization, or the operating system of the virtual machine of a virtualized workstation.
Système d'information d'importance vitale (SIIV)	Critical information system (SIIV)	Ce sont les « systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ».	These are "systems whose security or operation, if compromised, could significantly decrease the war or economic potential, security or survivability of the Nation".
System on Chip ou SoC	Système sur une puce	Système complet embarqué sur une seule puce, pouvant comprendre, de la mémoire, un ou plusieurs microprocesseurs, des périphériques d'interface, etc…	Complete embedded system on a single chip, including memory, one or more microprocessors, interface peripherals, etc.

T

Terme couramment utilisé	**Traduction en français ou en anglais**	**Définition en français**	**Définition en anglais**
Tâche d'administration	Administration task	On appelle tâche d'administration d'un système d'information les opérations de configurations, maintenance, évolution du système d'infirmation administré, supervision ou gestion de la sécurité.	Information system administration tasks include configuration, maintenance, upgrading, supervision and security management.
Technologies de l'information	Information Technology (IT)	Sans objet	Sans objet
Technologies de l'information et de la communication (TIC)	Information and Communications Technology (ICT)	Sans objet	Sans objet
Test d'intrusion	Penetration Test	Action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs. Remarque : il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (agresser son propre système d'information).	Action that consists of trying out several operating codes on an information system, in order to determine which ones give positive results. Note: this is both a defensive action (to better protect oneself) and an offensive action (to attack one's own information system).
Typosquatting	Faute de frappe opportuniste, coquille	Action malveillante qui consiste à déposer un nom de domaine très proche d'un autre nom de domaine, dont seuls un ou deux caractères diffèrent.	The malicious act of registering a domain name that is very similar to another domain name, differing by only one or two characters.

U

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Usurpation d'adresse	Address spoofing	Action malveillante qui consiste à utiliser délibérément l'adresse d'un autre système en lieu et place de la sienne.	The malicious act of deliberately using another system's address instead of your own.
Usurpation de carte SIM	SIM swapping	Technique permettant à un attaquant de contourner la double authentification pour associer une carte SIM de la victime au numéro de téléphone d'un attaquant.	Technique enabling an attacker to bypass double authentication and associate a victim's SIM card with an attacker's phone number.
Utilisateur	User	Sans objet	Sans objet
Utilisateur final	End-user	Sans objet	Sans objet

V

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Vecteur d'attaque	Vector of attack	Moyen d'accès utilisé par un acteur malveillant pour exploiter les failles de sécurité et accéder à un serveur ou un équipement (pièces jointes, pages Internet, vulnérabilités non corrigées).	Means of access used by a malicious actor to exploit security flaws and gain access to a server or device (attachments, Internet pages, unpatched vulnerabilities).
Veille [1]	Monitoring	Supervision opérationnelle	Operational supervision
Veille [2]	Watch	Suivi de l'actualité, l'environnement	Keeping abreast of current events and the environment
Ver	Worm	Un ver est un logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.	A worm is an independent piece of malware that seeks to spread its code to as many targets as possible, then execute it on those same targets. It disrupts the operation of the systems concerned by running without the user's knowledge.
Virus	Virus	Programme dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, ...) et, souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Il s'implante au sein de programmes, se duplique à l'insu des utilisateurs, et peut nécessiter l'intervention explicite de ces derniers pour se propager (ouverture d'un courrier électronique, lancement d'un programme exécutable, etc.).	A virus is a malicious program or part of a program whose purpose is to survive on a computer system (computer, server, mobile device, etc.) and, quite often, to reach or parasitize its resources (data, memory, network). The means of survival can take many forms: replication, implantation within legitimate programs, persistence in memory, etc. To spread, a virus uses all available means: e-mail, file sharing, backdoors, fraudulent Internet pages, USB keys, etc.
Visa de sécurité	Security Visa	Les Visas de sécurité que délivre l'ANSSI permettent d'identifier facilement les plus fiables d'entre elles et reconnues comme telles à l'issue d'une évaluation réalisée par	The security visas issued by ANSSI make it easy to identify the most reliable of them, recognised as such following an assessment carried out by approved laboratories using a rigorous

		des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.	and proven methodology.
Voix sur réseau IP	Voice over Internet Protocol (VoIP)	Technologie qui permet de véhiculer la voix de l'Internet ou tout autre réseau acceptant le protocole TCP/IP. Cette technologie est notamment utilisée par le service téléphonie IP (ToIP-telephony over internet protocol) à travers des logiciels.	Technology used to transmit voice over the Internet or any other network supporting the TCP/IP protocol. This technology is used in particular by the IP telephony service (ToIP-telephony over internet protocol) through software.
VPN (Virtual Private Network)	RPV (réseau privé virtuel)	Interconnexion de réseaux locaux via une technique de tunnel sécurisé ou non, généralement à travers Internet.	Interconnection of local networks via a secure or non-secure tunnel, usually over the Internet.
Vulnérabilité	Vulnerability	Faille de sécurité pouvant affecter un logiciel, un système d'information ou encore un composant matériel. Elle peut servir de porte d'entrée pour des acteurs malveillants s'ils parviennent à l'exploiter. Les vulnérabilités sont généralement corrigées lors des mises à jour ou par des correctifs publiés par les éditeurs.	Security flaw that could affect a software product, an IT system or even a hardware component. It can serve as a gateway for malicious actors if they manage to exploit it. Vulnerabilities are generally corrected during updates or by patches published by software editors. Vulnerability in a computer system enabling an attacker to undermine its normal operation, or the confidentiality or integrity of the data it contains.
Vulnérabilité jour-zéro	Zero-day vulnerability	Vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif.	Vulnerability that has not been published or patched.

W

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Webcam	Cybercaméra	Caméra numérique, reliée à un ordinateur, qui permet de filmer et de diffuser en temps réel des vidéos sur un réseau.	Digital camera, connected to a computer, for filming and broadcasting video in real time over a network.
Webshell	Console web malveillante Code enquillé	Type de fichier malveillant, exécuté comme un code par un serveur web, qui permet un accès et un contrôle à distance à un serveur Web en permettant l'exécution de commandes arbitraires. Bien préciser que cela permet à l'attaquant d'obtenir un accès à distance à la machine compromise (ex : Un attaquant pourrait exploiter cette vulnérabilité pour obtenir un accès à distance au serveur de la victime via une console web malveillante).	A type of malicious file, executed as code by a web server, which allows remote access and control of a web server by enabling the execution of arbitrary commands. Clearly, this allows the attacker to gain remote access to the compromised machine (e.g. an attacker could exploit this vulnerability to gain remote access to the victim's server via a malicious web console).
WI-FI (Accès sans fil)	Wireless Fidelity	Technologie de réseau informatique sans fil pouvant	Wireless computer network technology that can be used to build

		fonctionner pour construire un réseau interne accédant à Internet à haut débit.	an internal network accessing high-speed Internet.

Z

Terme couramment utilisé	Traduction en français ou en anglais	Définition en français	Définition en anglais
Zero-day, 0-day	0 jour, jour zéro	Vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif.	Vulnerability that has not been published or patched.