AgroTIC

RÉALISÉ PAR
COLINE CHOTEAU
NAEVA DUDON
ANÈS NOBIGGH

DARK WEB

ARCHITECTURE SYSTÈME INFORMATISÉ

2025

Table des matières

Introduction

Le web, tel que nous le connaissons aujourd'hui, est composé de plusieurs niveaux d'accessibilité et d'indexation des informations. Ces niveaux sont généralement classifiés en trois grandes catégories : le web en surface (Surface web), le Deep web et le Dark web.

1. Le Surface web

Le web en surface est la partie du web accessible directement via des moteurs de recherche classiques comme Google, Bing ou Yahoo. Il correspond à environ 10% du contenu total du web. [2] Tous les sites visibles et indexés par ces moteurs font partie de cette couche. C'est la partie la plus connue et la plus utilisée du web par le grand public. (ex : les réseaux sociaux, les sites d'actualités, les sites de e-commerce, Wikipédia…)

2. Le Deep web

Le Deep web désigne toutes les pages web qui ne sont pas indexées par les moteurs de recherche. Il comprend une multitude d'informations protégées, accessibles uniquement avec une authentification spécifique ou des droits d'accès particuliers.

Le Deep web représenterait 400 à 550 fois la taille du web en surface. Contrairement aux idées reçues, la majeure partie du Deep web n'est pas utilisée pour des activités illégales. Il est essentiellement composé de bases de données, de services internes d'entreprises, d'accès restreints à des publications scientifiques et de documents protégés par des mots de passe. (ex : Les bases de données académique et scientifiques, les services bancaire en ligne, les espaces clients de sites marchands, les messageries privées)

3. Le Dark web

Le Dark web est une sous-partie du Deep web qui nécessite des logiciels spécifiques pour y accéder, comme TOR (The Onion Router) ou I2P (Invisible Internet Project) [6]. Contrairement au Deep web, il est intentionnellement caché et vise à assurer un anonymat total de ses utilisateurs et de ses contenus.

Il est souvent associé à des activités illégales en raison de son anonymat, mais il existe aussi des usages légitimes. Des journalistes et des militants des droits de l'homme l'utilisent pour contourner la censure et protéger leurs sources.

Aspect	Surface web	Deep web	Dark web
Description	Contenu qu'un outil de recherche peut trouver	Contenu qu'un outil de recherche ne peut pas trouver	Contenu qui est caché intentionnellement
Information trouvée	4%	96%	
Accessibilité	Publique	Privée ou restreinte	Restreinte et anonyme
Indexation	Indexé par moteurs de recherche	Non indexé	Non indexé
Exemples d'usage	Recherche d'informations, e-commerce	Bases de données, courriels	Liberté d'expression, marchés noirs
Outils nécessaires	Navigateur standard (Google chrome, Mozilla Firefox)	Authentification ou lien direct	Navigateurs spécialisés (TOR, I2P)

Figure 1 : tableau résumant la surface, le deep et le dark web

L'image souvent utilisée pour expliquer ces couches du web est celle d'un iceberg :

- Le web en surface correspond à la partie visible de l'iceberg, accessible à tous.
- Le Deep web représente la partie immergée de l'iceberg qui est accessible uniquement via des accès restreints.
- Le Dark web est la zone la plus profonde, difficilement accessible et volontairement cachée.

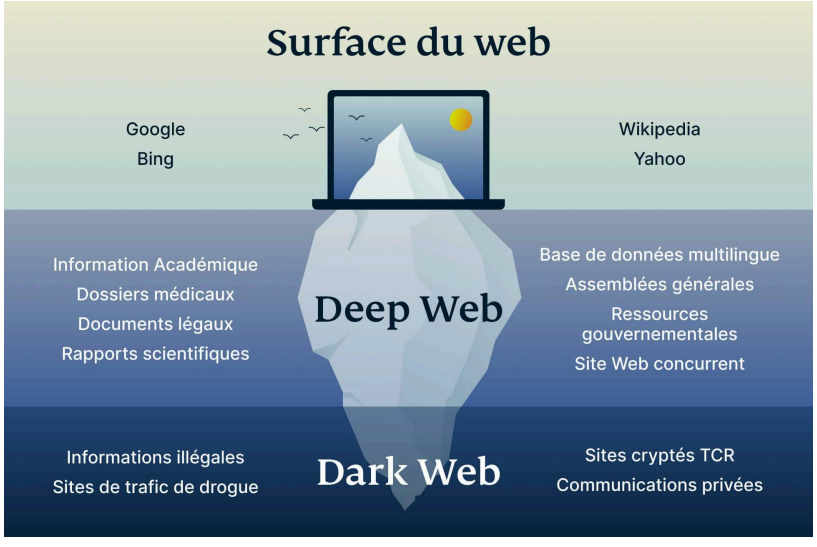

Figure 2 : Image illustrant la surface, le deep web et le dark web [1]

Le Dark web illustre la complexité des réseaux informatiques modernes. Il pointe également du doigt la sécurité et l'anonymat sur le web. L'étude de celui-ci permet de mieux comprendre les défis et innovations dans l'architecture des systèmes informatisés.

I. Architecture technique du Dark web

1. Les bases du fonctionnement

Le fonctionnement du Dark web repose sur des logiciels comme TOR, I2P ou encore Freenet. Ces technologies ressemblent à des moteurs de recherches, mais comparés à ceux bien connus de la population, ils sont décentralisés et permettent l'anonymat de l'utilisateur. L'adresse IP ainsi que la localisation ne peuvent pas être tracées correctement, signifiant que les sites visités sont dans l'incapacité de connaître l'identité des usagers. [1]

Que ce soit I2P, Freenet ou TOR, ces logiciels se distinguent par leur promotion de la liberté d'expression sur internet et la protection de la vie privée des utilisateurs. [7] Sur un navigateur classique, toutes les actions des utilisateurs sont accessibles et souvent utilisées ou vendues à des tiers. Ces données peuvent être exploitées à des fins de marketing ciblé, de profilage des utilisateurs, ou encore revendues à des entreprises pour améliorer leurs stratégies commerciales. De plus, toute parole postée sur le web est accessible à tous. La liberté d'expression n'est donc pas réellement garantie, car à tout moment, l'État ou toute autre administration puissante peut utiliser les propos de l'utilisateur contre lui. Ces logiciels prônent la "résistance à la censure" ainsi que le "respect de la vie privée". [7]

Pour cela, ces logiciels cachent le serveur à l'utilisateur et l'utilisateur au serveur. Le trafic à l'intérieur ne communique pas directement avec internet et utilise des tunnels unidirectionnels cryptés. [8] La cryptographie est une technique d'écriture qui permet d'écrire un message à l'aide de codes secrets ou de clés de chiffrement. Des algorithmes permettent de décrypter les messages, cependant certains cryptages sont considérés comme basiques (par exemple, la lettre de l'alphabet est décalée vers la droite ou la gauche avec un certain nombre de notes) et d'autres offrent un niveau de sécurité presque absolu. [9] Les logiciels utilisés pour accéder au Dark web, utilisent des techniques de cryptage avancées pour protéger la vie privée et l'anonymat des utilisateurs, offrant ainsi une sécurité et un anonymat renforcés.

2. Routage en oignon (Onion Routing)

2.1. Concept

La méthode la plus simple pour accéder au Dark web est d'avoir recours au navigateur TOR (The Onion Router). Celui-ci multiplie le nombre de serveurs intermédiaires entre l'utilisateur et le serveur web. Ainsi, chaque utilisateur est un proxy potentiel pour le logiciel. Lors d'une requête de l'utilisateur, celle-ci va passer par un certain nombre de proxy qui chacun à leur tour vont crypter le

message. Cela signifie que seul le premier proxy connaîtra le destinataire, tandis que le serveur de destination ne connaîtra que le dernier proxy qui lui a envoyé le message. Pour retracer la requête, il serait nécessaire de remonter tous les proxys et de décrypter leurs messages un par un. Cependant, chaque proxy est utilisé pour plusieurs requêtes et donc par plusieurs utilisateurs. Ainsi, si quelqu'un remonte jusqu'à un proxy, il se retrouvera face à plusieurs utilisateurs potentiels, rendant la traçabilité compliquée, voire impossible. [10]

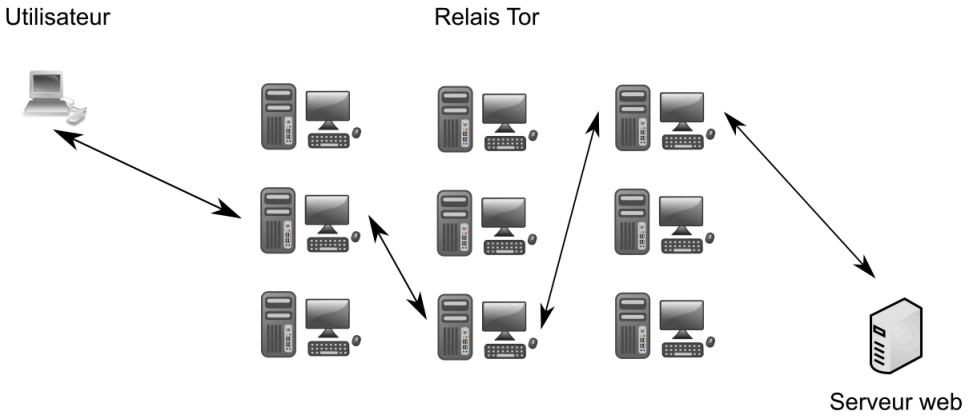

Figure 3 : Fonctionnement de TOR [3]

2.2. Limites

Bien que le routage en oignon ait l'avantage de fournir un anonymat à l'utilisateur, des limites restent tout de même d'actualité rendant son utilisation risquée et/ou contraignante.

Une première limite et mise en garde concernant l'accès au Dark web est que les logiciels tels que TOR ne garantissent pas à 100 % l'anonymat de l'utilisateur. En effet, personne n'est à l'abri de commettre une erreur ou d'être victime d'une défaillance technique qui permettrait de tracer son identité. Par conséquent, utiliser le Dark web pour des activités illégales comporte le risque de se retrouver en totale incompatibilité avec les lois du pays de résidence. En cas d'identification complète, cela peut entraîner des problèmes judiciaires majeurs. Ce point sera plus détaillé dans la suite de l'exposé.

Une deuxième limite que l'on peut citer est la lenteur du navigateur permettant de garder un anonymat. En effet, le passage du message par une multitude de proxy entraîne des ralentissements de navigation comparée à un navigateur traditionnel. Les pages mettront donc plus de temps à s'afficher, pouvant être une contrainte à l'utilisation de ces logiciels. [3]

3. Conseil pour l'accès au Dark web

Accéder au Dark web est donc assez simple, mais il est essentiel de prendre des précautions. Voici un guide pour vous aider :

3.1. Installer un navigateur crypté

Pour commencer, téléchargez et installez un navigateur crypté comme TOR en vous rendant sur le site officiel du projet. Le navigateur est disponible pour Windows, Mac, Linux et Android. Une fois lancé, créez un compte ou connectez-vous. [1]

3.2. Installer VPN

Pour renforcer la sécurité, nous vous conseillons d'utiliser un VPN (réseau privé virtuel). Un bon VPN peut faire transiter toutes vos données entrantes et sortantes via un tunnel sécurisé. Ce tunnel, qui connecte votre appareil à Internet, utilise un chiffrement fort (algorithme AES-256 bits) afin que vos activités en ligne ne puissent pas être interceptées et lues par d'autres. [1] Avant de commencer à naviguer, activez-le pour augmenter votre anonymat.

3.3. Accéder au Dark web

Une fois sur le navigateur crypté, comme TOR, commencez à naviguer vers les sites en .onion. Ces sites ne sont pas indexés par les navigateurs traditionnels. Certains annuaires sur le web peuvent vous aider à trouver des adresses .onion fiables. Restez prudent et évitez de télécharger des fichiers ou de cliquer sur des liens suspects si vous ne voulez pas que des logiciels malveillants ou des contenus illégaux envahissent votre ordinateur.

En suivant ces étapes, vous pourrez accéder au Dark web et reprendre possession de votre liberté d'expression ainsi que de votre anonymat sur le web. [12]

II. Usages du dark web

1. Usages légitimes

1.1. Protection de la vie privée & sécurisation des communications

Le Dark web est une couche supplémentaire d'internet, permettant une navigation anonyme, et une protection de la vie privée grâce à des protocoles de chiffrement avancés. Il peut être utilisé par les personnes souhaitant simplement protéger leur vie privée, dans une ère où la sécurité informatique n'est pas toujours garantie [5].

Parmi ces usages légitimes figure Facebook en version .onion. Il est utilisé par les personnes soucieuses quant à la transmission de données personnelles, mais aussi par des personnes issues de pays où le site Facebook originel peut-être censuré [11].

On peut également trouver des services de messagerie sur le Dark web : Elude, CTemplar, Riseup, Keybase… Ceux-ci permettent des échanges de mails, voire des chats, afin d'échanger en toute sécurité [11].

Cette inquiétude concernant la sécurité des données vient parfois en réponse d'une surveillance gouvernementale, comme PRISM : un programme secret de surveillance de masse mené par la NSA. Il permettait à la NSA de récupérer des données des utilisateurs de sites comme Facebook, Microsoft, Apple… [13].

1.2. Contournement de la censure

Selon les pays, les contenus disponibles sur le web peuvent être contrôlés à des fins politiques ou autres. Dans ce cadre, le Dark web permet d'échanger, de partager ou d'avoir accès de manière confidentielle à diverses informations, sans être contrôlé par les autorités gouvernementales, ou les fournisseurs d'accès internet [1] .

Le premier exemple qu'on peut citer est le cas du journalisme. Le Dark web devient un espace de liberté d'expression pour les personnes vivant dans des régimes oppressifs, où ce réseau est parfois le seul espace d'expression possible [5]. C'est aussi un moyen pour les grandes organisations de journalisme, et notamment de journalisme d'investigation, de se protéger et de protéger leurs sources. En conséquence, beaucoup d'informations peuvent être diffusées sans pour autant atteindre à la sécurité des personnes y contribuant [3]. À titre d'exemple concernant l'accès à l'information, nous pouvons mentionner le site de la BBC, censuré dans de multiples pays, qui existe en format .onion pour contourner cela [11].

Le second exemple concerne les lanceurs d'alerte et les dissidents. Au-delà d'un simple partage ou accès à de l'information, ces personnes se confrontent aux pratiques des puissants de notre monde. L'anonymat devient alors primordial pour leur permettre de pouvoir se battre pour leurs idées tout en évitant la surveillance de masse. En effet, ces comportements sont jugés déviants ou illégaux par endroit [3].

Voici 3 exemples de supports utilisés pour ces pratiques [11] :

- Propublica : destiné au journalisme d'investigation, lanceur d'alerte, média d'investigation accessible en web surfacique ou Dark web.
- SecureDrop : communication sécurisée entre les journalistes et les sources (lanceurs d'alertes).
- Wikileaks : publication de documents politiques ou historiques qui sont censurés ou cachés.

2. Usages illégaux

2.1. Développement des activités cybercriminelles

Le Dark web est un terrain de jeu pour les cybercriminels. C'est un lieu où les hackers peuvent se rencontrer et partager leurs connaissances, comme des astuces de hacking, des bouts de codes, ou encore des logiciels crackés, grâce à divers supports (wikis, forums, blogs) [3]. Cela peut être de manière bienveillante, avec en objectif le simple anonymat dans la navigation, mais dans beaucoup de cas, cet anonymat favorise au contraire le développement des activités cybercriminelles.

On va retrouver des sites permettant de faire appel à des services de hackers pour toute finalité souhaitée (ex : Hacker's Bay) [6]. On peut aussi retrouver de la vente de logiciels malveillants, accessibles à tous : virus, ransomwares, bots, chevaux de Troie, kits d'exploitation, des failles de sécurité… [6]. L'objectif avec cela peut être par exemple de réaliser des hacks de données sensibles, puis de revendre ces informations, ou de demander une rançon si la cible ne veut pas que ces données soient diffusées. Ce sont des événements qu'on voit souvent dans les actualités, avec des hacks de données d'utilisateurs de sites divers (Facebook, Linkedin…).

2.2. Marchés noirs

Les marchés noirs sont des sites où se vendent des biens et services dont la production et/ou la distribution sont illégales. Cela peut référer à de la vente de drogues, de la vente d'armes, de la traite d'humain, de la vente de contrefaçons, ou encore la vente de fausses identités et de carte de crédits volées… De manière générale, les achats se font via de la crypto-monnaie, comme le bitcoin [5]. Cela permet de ne pas avoir à renseigner d'informations de paiement et de garantir l'anonymat dans ces transactions. Le marketplace le plus célèbre est Silkroad, qui fut en opération entre 2011 et 2013. Aujourd'hui certains sites persistent comme Agora ou Silk Road 2.0 [6].

2.3. Diffusion de contenus interdits

Les contenus diffusés sur les sites publics sont très contrôlés, majoritairement pour préserver les auditeurs de scènes qui peuvent être parfois choquantes. Le Dark web est un espace de diffusion de ces contenus. Des sites comme Steakandcheese répertorient des vidéos très violentes [11].

D'autres contenus interdits, moins négatifs que ceux mentionnés ci-dessus, peuvent aussi être échangés, comme des documents scientifiques via Sci-Hub [6], ou des BD et livres via Comic Book

Library ou Imperial Library [11]. Ils sont interdits car cela viole les droits d'auteurs dans la majorité des cas.

III. Sécurité et défis associés

1. Risques pour les utilisateurs

1.1 Logiciels malveillants et arnaques

Les logiciels malveillants sont omniprésents sur le Dark web. On y trouve des malwares qui, par une simple visite sur un site douteux, exposent l'utilisateur à diverses infections : rançongiciel, enregistreurs de frappes, botnet [6] … L'objectif peut être d'accéder à des informations sensibles (données personnelles, mots de passe, numéro de carte bancaire…) que les cybercriminels pourront revendre ou utiliser comme levier de chantage [5]. Il faut donc être vigilant, même sur le Dark web, et ne pas hésiter à avoir un bon antivirus !

Les arnaques sont aussi monnaie courante, sans mauvais jeu de mot. La vente de divers services est parfois un leurre pour obtenir des données ou escroquer de l'argent : faux service de hacker, vente factice de fausses identités… Cette pratique frauduleuse compromet la sécurité financière et la vie privée des utilisateurs imprudents [5].

1.2 Surveillance et identification des utilisateurs

L'aspect légal sera détaillé dans la partie suivante, mais de manière générale, le Dark web n'est en soi pas illégal. Cependant, une simple utilisation de TOR peut attirer l'attention des autorités policières [6]. Ils ont la possibilité d'utiliser des logiciels pour suivre les activités des internautes [6].

De plus, comme brièvement mentionné précédemment, l'anonymat n'est pas garanti à 100% sur le Dark web [3]. Une erreur humaine ou un problème technique pourrait amener à une possible identification de l'utilisateur [3].

2. Défis techniques et juridiques

La lutte contre la cybercriminalité est confrontée à des défis techniques et juridiques. Dans un premier temps, la nature anonyme du Dark web rend difficile la traque des activités qui y ont lieu par les autorités [5]. De plus, la protection de la vie privée et la liberté d'expression sont des droits fondamentaux qui doivent être respectés. Il est donc nécessaire que les autorités trouvent un équilibre entre le respect de ces droits et la nécessité de lutter contre les activités criminelles [6].

Le cadre légal autour du Dark web est complexe et est en constante évolution [6]. De plus, il varie selon les pays. En effet, certains ont adopté des lois spécifiques pour lutter contre les activités criminelles, tandis que d'autres se concentrent sur la protection de la vie privée des utilisateurs [6]. De manière générale, les autorités policières et les organismes de réglementation traquent les activités illicites sur le Dark web. Mais la diversité de réglementation des pays opposée à la nature

mondiale d'internet soulève des défis en matière de coopération internationale quant à cette lutte [6].

Conclusions

1. Évolution du dark web

1.1 Tendance technologique et sociétale

Le Dark web évolue avec l'amélioration des technologies d'anonymisation (TOR, I2P) et l'essor des crypto-monnaies anonymes comme Monero. Les marketplaces décentralisées rendent plus difficile le démantèlement des réseaux criminels, tandis que l'intelligence artificielle et l'analyse de trafic sont de plus en plus utilisées pour tenter d'identifier les utilisateurs. D'un autre côté, le Dark web est devenu un outil de protection pour les journalistes et dissidents face à la censure (exemple : Chine).

1.2 Impacts potentiels de la régulation

Les gouvernements renforcent leur lutte contre la cybercriminalité en surveillant les flux financiers et en régulant les cryptomonnaies. Des collaborations internationales permettent la fermeture de certains sites (exemple : Silkroad (qui vient d'ailleurs d'être gracié par Trump)), mais les réseaux distribués compliquent ces efforts. L'interdiction de l'accès à TOR dans certains pays pose la question de la limite entre sécurité et liberté numérique. L'avenir du Dark web dépendra donc de cet équilibre entre régulation et protection de l'anonymat.

2. Ouverture

Le Dark web illustre la complexité des réseaux informatiques modernes et pose des défis majeurs en matière de sécurité, d'anonymat et de régulation. À travers notre analyse, nous avons mis en évidence son architecture technique unique, ses usages légitimes et illégaux, ainsi que les défis qu'il soulève pour les gouvernements et les chercheurs en cybersécurité.

D'un côté, il est un espace de liberté pour ceux qui souhaitent contourner la censure ou protéger leur vie privée. De l'autre, il abrite également des activités illicites, rendant la lutte contre la cybercriminalité particulièrement difficile. Les autorités tentent d'établir un équilibre entre protection des droits individuels et sécurité collective, mais les avancées technologiques rendent ce combat complexe. Ce qui en fait un sujet très controversé

Enfin, concernant notre module, l'étude du Dark web est essentielle pour comprendre l'évolution des infrastructures numériques et des technologies de chiffrement. Son existence pousse à repenser la gouvernance d'Internet et les moyens de garantir un Internet plus sûr et plus éthique, tout en respectant les libertés fondamentales.

3. Annexes

1. Bibliographie

[1] Journal du Geek. (2025). *C'est quoi le Dark web et comment y accéder ?* C'est quoi le Dark web et comment y accéder ? https://www.journaldugeek.com/vpn/faq/darknet/

[2] James Camilleri & Forensic Medicine. (2020). Surface web, Deep web and Dark web: three levels of exploitation. Write an essay discussing how each platform defers in terms of criminal opportunity, referring to difficulties related to criminal investigation and evidence gathering. https://www.researchgate.net/publication/347986866_Surface_web_Deep_web_and_Dark_web_three_levels_of_exploitation

[3] darknet-tor.com. (2025). *Le DARKNET : Définition & Explications Comment y accéder ?* https://darknet-tor.com//

[4] Guardia. (nd). Comment fonctionne le Dark web et quels sont les risques pour la sécurité en ligne. https://guardia.school/boite-a-outils/comment-fonctionne-le-dark-web-et-quels-sont-les-risques-pour-la-securite-en-ligne.html#tp-5

[5] Murielle Cahen. (2024). Le Dark Net est-il illégal ? https://www.murielle-cahen.fr/le-darknet-est-il-illegal/

[6] Masayuki Hatta. (2022) Deep web, Dark web, Dark net. https://www.academia.edu/109493469/Deep_web_dark_web_dark_net

[7] Freenet / Hyphanet build. (2025). Hyphanet. https://www.hyphanet.org/fr/index.html

[8] I2P. (2025). I2P Anonymous Network. https://geti2p.net/en/

[9] Oracle. (2025). Qu'est-ce que la cryptographie ? https://www.oracle.com/fr/security/qu-est-ce-que-la-cryptographie/#:~:text=En%20g%C3%A9n%C3%A9ral%2C%20la%20cryptographie%20est,un%20message%20consid%C3%A9r%C3%A9%20comme%20confidentiel.

[10] Vigicorp. (2025). Tor : le routage en oignon. https://www.vigicorp.fr/tor-le-routage-en-oignon/

[11] Géraldine Tomas. (2024). Les 20 meilleurs sites du dark web à jour en 2024. https://vpnoverview.com/fr/confidentialite/navigation-anonyme/sites-dark-web-qui-valent-la-peine/

[12] Cyberinstitut. (2025). Guide pour accéder au dark web en toute sécurité. https://cyberinstitut.fr/guide-acceder-dark-web-securite/

[13] Stéphane Fosse. (2024). L'affaire PRISM. https://fosse.fr/articles/affaire-prism.html

2. Glossaire des termes techniques.

TOR : The Onion Router

Rançongiciel : Logiciel malveillant qui chiffre les données d'un système informatique, bloquant ainsi l'accès aux fichiers. Pour déverrouiller les données, l'utilisateur doit verser une rançon

Malwares : logiciels conçus pour infecter, endommager ou accéder à des systèmes informatiques. Ils peuvent inclure des rançongiciels, chevaux de Troie, logiciels espions, etc.

NSA : National Security Agency (USA)