Epistémologie contemporaine autour de la Cybersécurité et des Données

Par Loïc Giraud

Table des matières

Executive Summary

In English :

In our time more than ever, it was high time to regulate all aspects related to the "Cyber". For a long time, we lived without thinking about the consequences that could result from a lack of rules on this subject. We did not anticipate what could happen and had to put in place, laws to regulate all kinds of drifts in cyberspace.
The ARPANET, whose the project was launched in 1966 has been divided into two distinct networks. The first still bearing the name of ARPANET and is dedicated to research.
The second is named MILNET, a military network protected from security policies such as encryption restricted access control.
With the accessibility of the Internet to the general public in the 1990's through the "Web", this interface is the best known by the layman and coded in an HTML language accessible via an HTTP protocol.
It will open access to information for millions of businesses and homes.
Data regulation also plays an important role in this equation, which remains a major issue to date.
The Datas, whether personal or strategic, can be of paramount importance in this economic war that has been going on for many years now.
Companies must not only protect themselves, it must go beyond them. It's called cyber-resiliency, an approach that not only addresses cybersecurity, but also business continuity and resilience within an organization.
A quarter of the companies organized the security so that it was attached to the executive committee. Business strategy is more about cybersecurity than ever before. Today, boards of directors are asking for a better vision, a better understanding of these issues. It is for this reason that these boards of directors seek to develop a more strategic approach that would take an efficient form by putting in place appropriate programs.
We are seeing that some measures are being put in place more and more over the years, which is a good thing for citizens and in generally the Web's users
Cyberspace is a new battleground where you have to arm yourself quickly and well, where you have to train and stay at the cutting edge of technology to be able to face new current and future threats.
Resilience must be at the heart of the concerns of every Information Systems Security Manager, in the measures to be taken to secure societies's information systems.
Are all these measures sufficient ? Should we innovate a little more to counter future threats ?
Perhaps it would be necessary to invest in Research and Development cells in order to anticipate these future threats such as there could be for IOTs (Internet Of Thing) for example or the Cloud.
Nearly half of all companies have cyber security programs in place to address cloud risks. We note that opinions are changing regarding this one, which has been feared for several years for its lack of control over data loss.
The Cloud has created a certain dependence among large companies, which see it as an opportunity to store their data in bulk, whether or not it is strategic for them, in a dematerialized way and without the need to store this data directly at home.

74% of companies still think they are enough prepared for security breaches, while half of them do not take the right steps to counter these threats.
Companies are trying to adopt an offensive stance, although the majority of them believe they are ready to face an attack.
Yet few have taken the initiative to set up crisis exercises, which is why companies rely mainly on technologies to counter ever more original and unusual improvements in attack techniques.

Introduction

Louis Pouzin disait : « *En réalité je déplore qu'on utilise le terme neutralité, parce que ce n'est pas vraiment le fond du problème. Le fond du problème c'est la transparence. C'est-à-dire que ce qu'on a besoin de savoir, c'est comment les opérateurs gèrent le trafic. Et si on s'embarque dans des grands mots comme "Neutralité", c'est-à-dire "Liberté, Égalité, Fraternité", on ne sait pas très bien de quoi on parle, et en fait, tout est faux. Le réseau n'a jamais été neutre.* »

Les gouvernements à travers le monde ont dû mettre en place des mesures afin de réglementer l'utilisation de l'internet et des données qui transitent au-delà des frontières. L'opacité qui régnait sur les données et leur utilisation ne pouvait plus durer, trop de scandales ont éclatés à cause de ceux-ci comme par exemple :

- Yahoo en 2013 – Plus de 3 Milliards de comptes compromis.
- Marriott international entre 2014 et 2018 – Plus de 500 Millions de clients dont leurs données personnelles ont été piratées.
- Uber en 2016 – Plus de 57 millions d'utilisateurs et 600 000 conducteurs dont les informations personnelles ont été exposées.
- Facebook en 2018 – Plus de 50 Millions d'utilisateurs ont vu leurs données personnelles exposées à cause d'une attaque informatique.
- Equifax en 2017 – Plus de 145 Millions d'utilisateurs américains ont vu leurs données personnelles fuiter dont 209 000 de ces utilisateurs, leurs données de carte de crédit également.

C'est pourquoi ce document traite de ce sujet épineux qu'est la réglementation en matière de cybersécurité et des données dans le monde. Ces réglementations qui n'auront de cesse d'évoluer et de s'abonnir avec les années pour faire face aux nouvelles menaces de plus en plus innovantes et donc par la même, de plus en plus dangereuses pour les systèmes d'information des grandes entreprises comme les plus petites. Les entreprises doivent être cyber-résilientes si elles veulent pouvoir tenir dans cette tourmente actuelle qui sévit sur Internet.

Partie 1 : Réglementations en Cybersécurité

Définition de « Réglementation »

C'est un ensemble de dispositions légales qui relèvent des pouvoirs publics, une réglementation est l'expression d'une loi et son application est imposée.
Un règlement sur la cybersécurité comprend des directives qui protègent les technologies de l'information et les systèmes informatiques dans le but de contraindre les entreprises et les organisations à protéger leurs systèmes et leurs informations des cyber-attaques venant de virus, de vers informatiques, de chevaux de Troie, d'attaques de type phishing, de dénis de service (DOS), de l'accès non autorisé et des attaques du système de contrôle.
Il existe de nombreuses mesures disponibles pour prévenir les cyber-attaques.

Les mesures qui s'imposent pour se protéger

Les mesures à prendre pour protéger un minimum un système d'information doit commencer par la mise en place de firewall, d'Anti-virus, de systèmes de détection et de prévention des intrusions, de chiffrement et de mots de passe de connexion.
C'est pour cela que des efforts ont été déployés pour améliorer la cybersécurité par le biais d'une réglementation et de collaborations entre le gouvernement et le secteur privé afin d'encourager les améliorations volontaires de la cybersécurité. Les régulations dans ce secteur, notamment les régulateurs du secteur bancaire, ont pris conscience du risque de la cybersécurité et ont commencé ou ont l'intention dans un avenir proche d'inclure la cybersécurité dans les examens réglementaires.

Réguler pour mieux fonctionner

La régulation ne date pas d'hier. L'idée de régulation n'est pas vraiment nouvelle. Ce grand peintre, scientifique, anatomiste, inventeur et plus encore, qu'est Leonard de Vinci qui était friand de poulets et qui les aimait bien cuits a imaginé un mécanisme qu'il installa dans sa cheminée.
Une simple hélice reliée à une broche sur laquelle était le poulet. Le procédé était que plus la chaleur du feu augmente, plus l'hélice et le poulet tournent rapidement. Sur l'internet, tout peut devenir "cyber", mais l'enjeu sociétal est immense. Dans le cyberespace on ne sait plus quelle est la cause ni quel est l'effet, on ne sait plus très bien qui gouverne et qui est gouverné. On ne cherche plus à savoir qui de l'œuf ou la poule est apparu le premier, car dans le cyberespace, on mange les deux.

L'ARPANET

L'ARPANET (**A**dvanced **R**esearch **P**rojects **A**gency **Net**work), est le réseau informatique expérimental précurseur de l'Internet.
Le DARPA (**D**efense of **A**dvanced **R**esearch **P**rojects **A**gency), qui est une branche du département américain de la Défense, a financé le développement de l'ARPANET dès la fin des années 1960. Celui-ci avait pour but de mettre en lien les ordinateurs des instituts de recherche entre eux, par le biais de lignes téléphoniques.
Dans les pires moments de la guerre froide, les chefs de guerre cherchaient un moyen d'obtenir un système de communication informatique sans noyau central et sans quartier général pouvant être attaqué et donc détruit par quelconque ennemi.

L'objectif initial d'ARPANET était purement académique avant d'être militaire, sauf qu'avec les installations académiques connectées de plus en plus nombreuses, le réseau commençait à prendre la forme de toile qu'avait été imaginée par les militaires.

Le projet « Cyclades » : La cyberguerre perdue

Dans les années 1970, l'internet tel que nous le connaissons aurait pu naitre en France, par l'intermédiaire des recherches du français Louis Pouzin.
Cyclades était l'équivalent en France de l'ARPANET aux Etats-Unis.
Le gouvernement français dont Valéry Giscard d'Estaing en était le président à cette époque, ayant refusé d'investir dans ce projet, nous a fait perdre un marché historique qui aurait pu être d'une importance capitale pour la France, mais sacrifier l'industrie informatique n'était certainement pas une bonne idée.
L'informatique n'était plus une priorité et c'est alors que le projet « Cyclades » mourut en 1978 faute de moyens financiers et de personnels.
Selon L. Pouzin, « *Plutôt que d'envoyer des données en séquence sur un canal préétabli, comme les wagons d'un train, ce qui a toujours été le dogme des télécoms, l'idée était d'envoyer des paquets comme des cartes postales. Les paquets ont une adresse de destination, et ils avancent dans le réseau en fonction de celle-ci.* »
Le minitel aurait pu fonctionner avec « Cyclades » a assuré L. Pouzin lors d'une interview. Gien et Zimmermann, deux anciens dans le projet « Cyclades » ont par la suite rejoint Sun Microsystems aux Etats-Unis et ont participé à la conception du système d'exploitation du nouveau moyen téléphonique d'Alcatel connecté sur l'internet, en somme un minitel évolué qui permettait de se connecter sur le net, il y a un peu de Cyclades là-dedans.

Un réseau enraciné

ARPANET est le produit final d'une décennie de développements en matière de communications informatiques, suscitée par les préoccupations militaires selon lesquelles
En ces temps de guerre froide, les Etats-Unis avaient certaines préoccupations quant aux Soviétiques qui pourraient utiliser leurs bombardiers à réaction pour lancer des attaques nucléaires surprises contre eux.
Dès les années 1960, le système SAGE (**S**emi-**A**utomatic **G**round **E**nvironment) avait déjà été mis au point et utilisait des ordinateurs pour suivre les aéronefs ennemis et coordonner toutes interventions militaires.
Ce système disposait de 23 centres de direction où chacun possédait un ordinateur central capable de suivre 400 avions. Ceux-ci pouvaient distinguer les avions alliés des bombardiers ennemis.
Un tel système a exigé six ans et plus de 60 milliards de dollars pour être mis en œuvre.

Un besoin d'interaction humaine

Joseph Carl Robnett Licklider sera le premier directeur du bureau de traitement de l'information, l'IPTO (**I**nformation **P**rocessing **T**echniques **O**ffice).
Le réseau SAGE ayant démontré l'énorme pouvoir de l'informatique interactive ou comme il l'a mentionné dans son papier « *Man-Computer Symbiosis* » en 1960, la « symbiose Homme-Ordinateur ».
Dans ses écrits, l'un des plus importants dans l'histoire de l'informatique, Licklider a émis l'idée selon laquelle la synergie entre l'humain et l'ordinateur pourrait mener à prendre de meilleures décisions.

Il est fort à parier que les craintes liées à la guerre froide aient mené à ce que les trois quarts des recherches en informatique financées aux Etats-Unis soient financées par l'ARPA.
L'ARPA est au cœur des réseaux informatiques et de l'internet mais également d'infographie ou de simulation de vol sur ordinateur et autres réalisations du genre.
En 1967, un plan pour le réseau a pour la première fois lors d'un symposium de l'ACM (**A**ssociation for **C**omputing **M**achinery) à Gatlinburg au Tennessee, été mis à disposition du grand public.
L'ancien directeur de l'ARPA Charles Herzfeld, racontait que Robert Taylor (L'un des pionniers d'Internet) et ses collègues cherchaient un moyen pour pouvoir connecter des chercheurs entre eux par le biais des ordinateurs.
Du point de vue militaire, le but de ce projet était beaucoup moins important. Charles Herzfeld faisant même remarquer que personne n'avait connaissance sur le fait qu'une telle expérience puisse être réalisable ou non.
Il était pourtant risqué de miser sur une expérience aussi innovante, en sachant que le financement d'un montant d'un million de dollars était à l'origine dédié au programme de défense missile antibalistique.

La cyber-origine du mot : « Cyber »
"Cyber" vient du grec « *Kubernêtikê* », qui signifie « Gouvernail », c'est un préfixe dérivé du mot "cybernétique" qui recouvre l'ensemble des activités liées à l'utilisation offensive du cyberespace. La cybernétique est la théorie de la communication et du contrôle de la régulation
Le « cyberespace », bien qu'il soit l'un des termes les plus omniprésents du vocabulaire de l'ère de l'information, est tout aussi flou que le reste du vocabulaire de l'ère de l'information. Ce terme a été créé par William Gibson dans son roman cyberpunk « Neuromancer » (« Neuromancien » pour la version française) et a été utilisé pour la première fois en tant que référence à l'internet en 1991. Le terme « Cyberespace », tel qu'on l'utilise aujourd'hui, évoque la fusion de tous les réseaux de communication, des bases de données et des sources d'information en un vaste ensemble d'échanges électroniques enchevêtrés et divers.
Ainsi, un « écosystème de réseau » est créé, un endroit ne faisant pas partie du monde physique normal. Un environnement « virtuel », « bioélectronique » littéralement « universel », qui existe partout où il y a des fils téléphoniques, des câbles coaxiaux, des lignes à fibres optiques ou des ondes électromagnétiques. Pratiquement tout élément du cyberespace peut être mis en péril et le degré d'interconnexion de ces éléments peut rendre difficile la détermination de l'étendue des mesures de sécurité nécessaires. On peut dire que le cyberespace est l'ensemble des ordinateurs connectés dans le monde.

Les divers aspects de la sécurité
La « sécurité » est un vaste sujet qui inclut entre autres la sécurité des pays contre les attaques militaires ou terroristes, la sécurité des ordinateurs contre les pirates, la sécurité à domicile contre des cambrioleurs et autres intrus, la sécurité financière contre des effondrements économiques et de nombreuses autres situations connexes. Dans notre contexte, nous devons nous préoccuper de deux concepts de sécurité différents : une technique et un qui englobe la sécurité de nations entières. Le mot « sécurité » en tant que terme technique, signifie non seulement que quelque chose est sécurisé, mais qu'il a été sécurisé.
Dans les télécommunications, le terme « sécurité » a la signification suivante :

« *Condition résultant de la mise en place et du maintien de mesures de protection garantissant l'état d'inviolabilité de systèmes malveillants* ».

D'autre part, la « sécurité nationale » peut être définie de manière objective comme l'absence de menace pour les valeurs fondamentales d'une société et de manière subjective comme l'absence de crainte que ces valeurs ne soient attaquées. Il décrit également les mesures prises par un État pour assurer sa survie et son bien-être général.

Deux notions qui diffèrent

Toutes deux impliquent une condition sans danger (Qu'il soit réel ou imaginaire).
Cependant leur portée et leur "Objet de référence" sont différents, de même que la chose à protéger le sera également.
La sécurité des systèmes d'information concerne dans sa forme la plus pure, des mesures techniques telles que des *firewall* pour garantir les mesures de sécurité nationale.
Ceci inclut le maintien des forces armées, le maintien des services de renseignements pour détecter les menaces, les mesures de défenses civiles et la préparation aux mesures d'urgence pour assurer la sécurité et la liberté. Avec l'avènement de la cybersécurité dans les politiques de sécurité, les deux notions se confondent. De nos jours, la sécurité nationale s'inquiète également des tentatives de création de résilience et de redondance des infrastructures nationales, par le biais de mesures de cybersécurité, ou par la protection des informations classifiées. Cela signifie que les mesures généralement considérées comme relevant de la sécurité de l'information peuvent également être incluses parmi les mesures visant à assurer la sécurité nationale.

La cybersécurité

Rassemblant les deux mots « Cyber » et « Sécurité », la cybersécurité vise à protéger le cyberespace des menaces, et donc des cybermenaces. La notion de « cybermenaces » reste relativement vague et implique la malveillance dans l'utilisation des Technologies de l'Information et de la Communication (TIC) comme cible ou comme outil par nombre d'acteurs malveillants.
Tel qu'il est couramment utilisé, le terme « Cybersécurité » fait référence à trois choses :

- Un ensemble d'activités techniques et non techniques, destinées à protéger les ordinateurs, les réseaux informatiques, le matériel informatique et les dispositifs logiciels associés, ainsi que les informations qu'ils contiennent et communiquent, y compris les données, ainsi que d'autres éléments du cyberespace, les menaces, y compris liées la sécurité nationale.
- Le degré de protection résultant de l'application de ces activités et mesures.
- Le domaine d'activité professionnelle associé, y compris la recherche et l'analyse, visant à mettre en œuvre ces activités et ainsi améliorer leur qualité.

La cybersécurité ne se limite donc pas à la sécurité de l'information ou à la sécurité des données, elle est étroitement liée à ces deux domaines.
En effet, la sécurité de l'information est aujourd'hui au cœur de la question, elle concerne tous les aspects de la protection de l'information.

Le plus souvent, ces aspects sont classés en quatre catégories :

Confidentialité, Intégrité, Disponibilité des informations et Responsabilité.

- La Confidentialité fait référence à la protection des informations contre la divulgation à des parties non autorisées.
- L'Intégrité fait référence à la protection des informations contre toute modification par des tiers non autorisés.
- La Disponibilité signifie que les informations doivent être mises à la disposition des parties autorisées sur simple demande.
- La Responsabilité ou l'exigence selon laquelle les actions d'une entité doivent être attribuées de manière unique à cette entité, est ajoutée à la liste.

Jusqu'au début des années 1990, la confidentialité était l'élément le plus important de la sécurité de l'information, suivi de près de l'intégrité et enfin de la disponibilité.

La cyber-évolution

Début 2000, l'évolution des modes d'utilisation combinée à l'augmentation des attaques externes ont placé la disponibilité en tête des points précités dans cette liste de priorités.
En réalité, le premier objectif de la sécurité de l'information moderne est de garantir la fiabilité prévisible des systèmes face à toutes sortes de malices, en particulier face aux attaques par déni de service. Cela nous montre encore une fois à quel point il est important de prendre en compte les perceptions de menaces liées aux contre-mesures.
Le sujet de la cybersécurité est entré dans l'agenda politique de la sécurité et discute des caractéristiques des cybermenaces.
Divers gouvernements abordent la question et mettent l'accent sur des problèmes communs qui mettent en lumière la comparaison de ces initiatives. En particulier les différences et les similitudes dans les approches nationales en appliquant la théorie des sciences politiques au sujet. La manière dont le sujet est abordé sur la scène internationale met en exergue deux paradigmes fondamentalement opposés qui pourraient poser des difficultés considérables au développement d'une culture mondiale de la cybersécurité.
Le débat sur la cybersécurité tel que nous le connaissons aujourd'hui a commencé aux États-Unis au milieu des années 1990, puis s'est étendu à d'autres pays développés et s'est manifesté sous diverses formes dans les programmes de politique de sécurité.

Le produit de deux développements récents

D'une part, il est inextricablement lié à la révolution dite de l'information, qui concerne l'évolution et la propagation dynamiques des technologies de l'information et de la communication dans tous les aspects de la vie et leur intégration. Certaines caractéristiques de ce développement technologique, notamment l'insécurité évidente et inhérente aux réseaux numériques, ont eu un impact décisif sur notre perception et notre réaction aux cybermenaces.

Des politiques pour contrer les menaces cyber

La montée des cybermenaces peut être considérée comme le fruit d'une profonde réorientation des politiques de sécurité survenue après la fin de la guerre froide.
C'est en choisissant de se tourner vers des spécialistes de l'analyse et des chercheurs, pour non seulement pour obtenir des conseils sur des alternatives politiques, mais aussi pour

arriver à identifier les nouvelles menaces, que tout ceci a conduit à l'ajout d'une multitude de nouveaux problèmes dans les programmes de sécurité.
Ce développement a été motivé par les préoccupations de la communauté de la défense américaine selon laquelle son énorme domination militaire conventionnelle forcerait tout type d'adversaire.
Certains États et groupes « sous-étatiques » utiliseraient des moyens asymétriques, tels que des armes de destruction massive, des opérations d'information ou des actes terroristes contre les États-Unis d'Amérique.
Avec la propagation rapide des TIC (**T**echnologies de l'**I**nformation et de la **C**ommunication) sur le marché mondial, le libre accès pour tous aux armes d'information et la dépendance croissante des sociétés modernes à l'égard des TIC, la peur des vulnérabilités asymétriques s'est accrue de façon exponentielle. On pourrait craindre qu'un ennemi qui ne pourrait jamais gagner une bataille contre la puissante machine de guerre américaine à haute technologie dans un conflit conventionnel ne frappe un point névralgique aux États-Unis, que ce soit sur un lieu physique ou dans le cyberespace.

Pour résumer, la perception des cybermenaces présente donc deux aspects principaux :

- Un nouveau type de vulnérabilité lié à la dépendance de la société moderne à l'égard de systèmes d'information intrinsèquement non sécurisés
- L'expansion du rapport aux menaces, en particulier en ce qui concerne les groupes malveillants et leurs capacités envers les autres.

Critères de sécurité et exemples d'impacts opérationnels

Confidentialité de l'information
Des informations sur un prototype de téléphone sont échangées entre le fabricant et son sous-traitant. L'interception de ces données par un concurrent peu compromettre l'avantage stratégique du fabricant.
Intégrité de l'information
Des informations sont stockées sur une base de données d'une entreprise et doivent servir à un fournisseur pour la fabrication d'un produit. La modification des données de fabrication (dimensions…) conduit à la fabrication de pièces non conformes.

Disponibilité de l'information
Des données sont utilisées pour le catalogue numérique d'un fournisseur, la suppression de ces données entraine l'indisponibilité du catalogue. L'indisponibilité de l'information empêche la vente des produits.

La révolution en réseaux
Certains prétendent que les débuts de la révolution de l'information remontent à l'invention du télégraphe. En fait, ce n'est qu'au début des années 1990 qu'une convergence d'événements a donné lieu à ce que l'on peut décrire comme une ascension crescendo des rêves de révolution de l'information. Les ordinateurs sont devenus populaires auprès du grand public et les chercheurs ont commencé à être plus nombreux que les travailleurs d'usine. Cet environnement technologique plus récent est à la tendance de « l'omni-connexion », qui créé de vastes réseaux ouverts de différentes tailles et formes.

Depuis leurs débuts il y a une vingtaine d'années, les réseaux informatiques sont devenus un élément central de la société moderne et dans un sens plus abstrait, le « réseau » est devenu une métaphore de nombreux aspects de la vie moderne. L'alliance des ordinateurs et des télécommunications ainsi que la mise en réseau mondiale de systèmes tels que des systèmes informatiques avancés, des bases de données et des réseaux de télécommunications qui rendent les informations électroniques disponibles et accessibles. Ce sont des infrastructures mondiales de l'information et sont en fait ce qui a rendu la révolution actuelle, un phénomène de masse ayant pris des proportions importantes.

L'infrastructure de l'information

Il n'est pas simple de comprendre en quoi consiste précisément l'infrastructure d'information, même à échelle réduite. Cela est dû au fait qu'elle n'a pas seulement une composante physique tels que les réseaux à haut débit, interactifs, à bande étroite et à large bande, les systèmes de communication par satellite, terrestres et sans fil ou encore les ordinateurs, téléviseurs, téléphones, radios et autres produits que les gens utilisent pour accéder à cette infrastructure.

Il y a aussi une composante immatérielle tout aussi importante et parfois très difficile à cerner, à savoir les informations et le contenu qui circulent dans l'infrastructure, les connaissances qui en sont créés, et les services fournis sur cette base. Les outils de la révolution de l'information évoluent rapidement. Avec l'éclatement de la bulle Internet, l'euphorie hyper-technologique des années 1990 a fortement diminuée. Les experts s'entendent sur le fait que dans le futur, les principales tendances technologiques seront à l'automatisation, à la mobilité, à la miniaturisation et à l'omniprésence croissante de l'informatique et des réseaux qui renforceront les tendances existantes et en créeront de nouvelles.

Dans ce contexte, les implications en termes de sécurité sont particulièrement intéressantes. Vu que les cybermenaces concernent en priorité l'utilisation malveillante d'un système d'informations, les caractéristiques (actuelles et futures) de l'environnement technologique auront un impact considérable sur la perception de la menace. Les incidents de plus en plus perturbants dans ce cyber-domaine et Microsoft avec ses systèmes d'exploitation présentant des failles de sécurité persistantes, ont pu donner l'impression que le monde informatique pourrait poser un grave problème de sécurité.

Comparaisons des réglementations proactives en matière de cybersécurité

Afin de placer le sujet de la cybersécurité dans un contexte mondial, il faut comparer le **C**omputer **F**raud and **A**buse Act (CFAA) avec les pays analogues du G8, à savoir les États-Unis, le Canada, la France, l'Allemagne, l'Italie, le Japon, la Russie et le Royaume-Uni.

Ces pays ont été sélectionnés parce qu'ils font partie des cyber-puissances les plus avancées. Même si le G8 est un symposium ayant connu des moments difficiles de par les actions de la Russie en Crimée et ailleurs, la stature de ce pays est un élément à prendre en compte dans cette analyse.

Tableau récapitulatif des comparaisons de lois entre les différents pays du G8

Pays	Articles de loi	Année de la loi	Textes de loi
Canada	• Code pénal du Canada § 342.1 • Code pénal du Canada § 430 (1.1)	• 1985 • 1985	• « Quiconque de manière frauduleuse, sans apparence de droit, accède, directement ou indirectement, un service informatique est coupable d'un acte criminel… » • « Tout individu commettant un méfait, qui volontairement A. Détruit ou modifie les données ; B. rend les données dénuées de sens, inutiles ou inefficaces ; C. bloque, interrompt ou interfère avec l'utilisation licite des données ; Ou D. entrave, interrompt ou interfère avec toute personne dans l'utilisation licite des données ou refuse l'accès aux données à toute personne ayant le droit d'y accéder. »
France	Code pénal, article 323-1	2000 (non en vigueur avant 2002)	« L'accès frauduleux à tout ou partie d'un système de traitement automatisé de données est puni d'une peine de prison maximale de deux ans et d'une amende de 30 000 euros ».
Allemagne	Code pénal, article 202(a) : Espionnage de données.	1998	« Toute personne qui obtient sans autorisation, que ce soit pour elle-même ou pour une tierce personne, des données qui ne lui sont pas destinées et spécialement protégées contre les accès non autorisés est passible d'une peine d'emprisonnement allant jusqu'à trois ans au plus ou d'une amende ».
Italie	Code pénal, article 615 Ter : Accès non autorisé dans un ordinateur ou un système de télécommunication.	2008	« Toute personne qui entre sans autorisation dans un ordinateur ou un système d'informations protégé par des mesures de sécurité, ou qui y reste malgré la volonté explicite ou implicite de celui qui a le droit de l'exclure, est passible d'une peine d'emprisonnement allant jusqu'à trois ans au plus ».
Japon	Loi n ° 128, article 3 : Ordinateur non autorisé. Loi d'accès.	1999 (A pris effet en 2000)	« Nul ne doit commettre d'acte d'accès non autorisé à un ordinateur… »
Russie	Code pénal, chapitre 28, Article 272 : Accès illégal aux informations de l'ordinateur.	1996	« L'accès illégal à des informations informatiques protégées par la loi […] est punissable par une amende d'un montant égal de 200 à 500 fois le salaire minimum, ou du montant du salaire ou traitement, ou de tout autre revenu de la personne condamnée pour une période de deux à cinq mois,

			soit par un travail correctif d'une durée de six à douze mois, ou par privation de liberté d'une durée maximale de deux ans. »
Royaume-Uni	Loi sur les abus informatiques.	1990 (Modifiée en 2006 - Loi sur la police et la justice, Article 35)	« Une personne est coupable d'une infraction si : A. il oblige un ordinateur à exécuter toute fonction dans l'intention de sécuriser l'accès à un programme ou à des données contenues dans un ordinateur [ou de permettre à un tel accès d'être sécurisé] B. l'accès qu'il a l'intention de sécuriser [ou de permettre de sécuriser,] n'est pas autorisé ; Et C. il sait au moment où il fait en sorte que l'ordinateur remplisse cette fonction. »
Etats-Unis	• USA Patriot Act • Fraude informatique et abus	• 18 États-Unis § 1030 (2001) • 8 États-Unis § 1030 (1984, dernière mise à jour 2008)	• « Cet amendement au Patriot Act concerne « les ordinateurs situés en dehors des États-Unis, dans la mesure où ils affectent le commerce ou les communications entre États ou à l'étranger des États-Unis ». • La loi sur les fraudes et abus informatiques régit les personnes qui accèdent « sciemment » ou « intentionnellement » à un ordinateur sans autorisation ou qui ont un accès supérieur…"18 U.S.C. § 1030 (a). (2) • Le ministère de la Justice a noté que le terme « sans autorisation » n'est pas défini par le **C**omputer **F**raud and **A**buse *Act*. Le terme « dépasser l'accès autorisé » signifie « accéder à un ordinateur avec autorisation et utiliser cet accès pour obtenir ou altérer des informations que l'individu n'a pas le droit d'en connaître ou de modifier ». 18 U.S.C. § 1030 (e) (6) »

Analyse comparative de ces réglementations

Il est important de noter que chaque pays du G8 a une loi qui régit « l'accès non autorisé » dans une mesure plus ou moins grande. Ces lois visent principalement à criminaliser le piratage purement informatique (plutôt que le « piratage »), ce qui peut être dû à l'influence de la Convention du Conseil de l'Europe sur la cybercriminalité (aussi connue sous le nom de « Convention de Budapest »).

Dans tous les cas, une telle congruence est importante à noter. Par exemple, le Canada a adopté les dispositions pertinentes de son code pénal en 1985, peu après l'introduction de la CFAA au Congrès des États-Unis.

D'autres membres du G8, notamment l'Allemagne, la Russie et le Royaume-Uni, ont adopté des lois pertinentes dans les années 1990, tandis que les autres, notamment la France, l'Italie et le Japon, n'ont réglementé ce comportement que dans les années 2000. Aucune loi active liée à la défense, créée par le G8, que nous pouvions localiser, y compris des amendements à des lois existantes telles que la CFAA ou le Code pénal italien, n'a été adoptée ou modifiée depuis 2008.
D'autres domaines de convergence au sein du G8 existent également. Chaque pays analysé mentionne l'imposition d'amendes et de peines d'emprisonnement, bien que les quantités de celles-ci varient considérablement selon les pays.
En France par exemple, le piratage informatique mène à une amende pouvant aller jusqu'à 30 000 euros, alors qu'en Russie, un présumé criminel pourrait faire face à une amende pouvant atteindre 500 fois le salaire minimum du pays.

Trois murs et des barreaux
La durée de la peine d'emprisonnement potentielle, est en revanche plus cohérente. Des peines de deux à trois ans étant courantes en France, en Allemagne, en Italie, en Russie et aux États-Unis (Petite exception pour ces derniers, les peines peuvent aller jusqu'à 20 ans), en fonction du type de violation commise en vertu de la CFAA.
De nombreuses lois sont également rédigées de manière assez large, les États-Unis et le Royaume-Uni poursuivent des approches similaires à la réglementation de « l'accès non autorisé », notamment en imposant une condition explicite d'état intentionnel.
De façon plus globale, le code criminel canadien réglemente de manière générale « *l'accès non autorisé » pour « quiconque [qui] commet un méfait* ».

Divergences de points de vue
Un domaine de divergence entre les pays du G8 est le degré de protection requis pour qu'une violation se produise. En Allemagne, une personne qui obtient des données sans autorisation d'accéder au système d'informations « spécialement protégé contre les accès non autorisés » est réputée avoir enfreint la loi. De même en Italie, seuls les ordinateurs « protégés par des mesures de sécurité » sont couverts par le code pénal. Les procureurs allemands et italiens pourraient par exemple avoir à se demander si le système qu'un présumé coupable est accusé d'avoir enfreint, était sécurisé ou « spécialement protégé ».
En revanche, le Canada, les États-Unis, la France, le Japon et le Royaume-Uni appliquent plus largement les lois en matière d'accès non autorisé, dans le fait qu'ils ne contiennent aucune disposition spécifique concernant la sécurité ou la protection requise pour le système informatique ou les données endommagées.
Des divergences politiques peuvent également se produire. En tant que groupe, le G8 s'emploie à lutter contre la cybercriminalité mondiale depuis 2006. En 2007, le G8 a convenu de « *travailler à l'incrimination, dans le cadre juridique national, de formes spécifiques d'utilisation abusive d'Internet à des fins terroristes* ». Les membres du G8 ayant approuvé ces déclarations faisant référence à la nécessité de prendre des mesures pour « *affaiblir la capacité des criminels transnationaux organisés, à opérer* ».
Cependant, les actions menées par la Russie en Crimée et ailleurs en 2014 ont beaucoup moins attiré l'attention sur le G8 en tant que moyen d'harmoniser les approches nationales en matière de cybersécurité, ce qui a eu pour effet de renforcer l'attention portée au G20. Des appels ont également été lancés pour que le G20 approfondisse ses partenariats avec des entreprises technologiques multinationales afin de mieux lutter contre la cybercriminalité,

une stratégie dite du « G20 plus 20 ». En outre, la cybercriminalité et les stratégies du secteur privé étant des problèmes mondiaux dans un monde de plus en plus multipolaire, il est particulièrement important de regarder au-delà du G8.

Vers un retour de la Russie dans le G8

Bien que le président des Etats-Unis Donald Trump, est favorable à un retour de la Russie dans le G7 qui reformerait donc le G8 comme c'était le cas avant 2014, le reste de l'Union Européenne voit elle d'un mauvais œil le fait de réintégrer la Russie après ce qu'elle a fait en Ukraine.

Emmanuel Macron, président de la république Française, ne parait pas totalement contre le retour de la Russie dans ce forum bien qu'il émette des réserves, notamment sur les conditions de celui-ci.

Il semble peu judicieux de garder la Russie en dehors du groupe, surtout quand bon nombre de sujets la concerne directement. C'est du moins les arguments qui ont été avancés par le président Trump.

Les Etats-Unis semblent avoir une connivence avec la Russie qu'il ne semble même pas cacher. Donald Trump aurait-il des intérêts dans ce conflit ?

En tous les cas, Paris juge que si que la Russie est toujours accusée d'agir en sous-main dans le conflit ukrainien, un potentiel retour de la Russie pour reformer le G8 serait inenvisageable.

Singapour, une nouvelle approche

Singapour, un grand centre financier mondial, a été victime d'une série d'attaques et de violations de plus en plus importantes au cours des dernières années, et son amendement de 2014 à sa loi sur les abus informatiques (**C**omputer **M**isuse and **C**ybersecurity Act (« CMCA »)) dans le cadre d'une tentative visant à remédier à la pénurie systémique de professionnels de la cybersécurité dans le pays. Cet amendement marque le début de son deuxième schéma directeur d'Infocomm Security, une période de développement de la cybersécurité qui s'étend jusqu'à 2018 (le premier schéma directeur d'Infocomm couvrant la période 2005-2007).

Les deux plans sont des stratégies nationales multiformes visant à promouvoir la cybersécurité à un niveau systémique et reflètent le besoin de Singapour de procéder à une réforme plus large de la cybersécurité. Compte tenu du profil de Singapour comme cible de grande valeur associée à une cybersécurité du secteur privé relativement médiocre, Singapour a décidé de poursuivre une politique nationale plus agressive en matière de cybersécurité que de nombreux pays occidentaux sous la forme du CMCA.

Le CMCA a la particularité de trouver un terrain d'entente dans le domaine de l'élaboration de politiques de défense active : s'il ne légalise pas complètement la défense active privée, il crée un mécanisme permettant à la défense active sanctionnée par l'État de protéger les infrastructures nationales essentielles.

Le secteur privé

Une nouvelle ère de cybersécurité proactive

Au début des années 2010, malgré l'incertitude juridique persistante aux États-Unis et au niveau mondial, les débats sur la cyberdéfense active ont commencé à évoluer.

Avec des cyber-attaques de plus en plus fréquentes et l'inquiétude croissante des entreprises, ont probablement contribué à un changement de perception.

Par exemple en 2010, plus de 40% des entreprises interrogées par Symantec ont signalées que les incidents liés à la cybersécurité étaient en tête de leurs préoccupations.

L'opération Aurora, une campagne sophistiquée faisant appel à des attaques par hameçonnage (Phishing) et au moins un exploit Zero-day exposé par Google début 2010, a certainement constitué un tournant décisif dans leur appréhension.
Les attaques étaient vraiment très élaborées pour au moins deux raisons :

- Le type de propriété intellectuelle volée (y compris le code source de Google, à savoir son bien le plus précieux)

- Des attaques commanditées par l'État ou d'autres attaquants hautement organisés et bien financés commençaient à viser des entreprises privées.

L'opération Aurora
Ce fut une attaque malveillante ciblée, dirigée contre une trentaine de grandes entreprises. Des compagnies comme Google et Adobe ont été concernées par cette attaque. Le mode opératoire a été d'exploiter une faille « Zero day » dans Internet Explorer.
L'exploit a permis aux logiciels malveillants de se charger sur les ordinateurs des utilisateurs. Une fois chargé, le logiciel malveillant pourrait prendre le contrôle de l'ordinateur pour voler la propriété intellectuelle de l'entreprise.
Le malware est originaire de Chine et Google est allé aussi loin en affirmant que l'attaque était parrainée par l'État. Cependant, il n'y a pas encore de preuve solide pour le confirmer.
Selon Dmitri Alperovitch, vice-président des recherches sur les menaces au sein de la société *McAfee*, l'opération « Aurora » représente le premier cas dans lequel des entreprises privées (en dehors de la défense) ont subi un niveau d'attaque aussi sophistiqué.
Par ailleurs, dans le cadre de l'enquête privée de Google, la société a eu accès à un ordinateur, alors situé à Taïwan, qu'elle soupçonnait d'être à l'origine des attaques (Aurora).
Lorsqu'elle a eu la preuve d'attaques impliquant d'autres sociétés américaines, Google a alerté et a collaboré avec les services de renseignement et d'application de la loi américaine pour retrouver le responsable des attaques en Chine. En faisant cela, Google a peut-être créé un précédent de ce qui est permis pour se défendre contre les APT (**A**dvanced **P**ersistent **T**hreat, soit les **M**enace **P**ersistante **A**vancée), même si on pouvait imaginer des scénarios similaires qui pourraient donner lieu à des poursuites au civil ou au pénal.
En 2011, *McAfee* a défini les APT comme « *des attaques sophistiquées et secrètes visant à voler subrepticement des données précieuses auprès d'entreprises ciblées et peu méfiantes* » et a ajouté que ce type d'attaques ciblées sont en augmentation.

Partie 2 : La réglementation des Données

Définitions des données stratégiques

Les données stratégiques représentent les données fondamentales et essentielles, qui sont sous la responsabilité d'acteurs clés et qui auront pour but de développer les axes stratégiques d'une société. Ces acteurs ont pour objectif de tirer pleinement parti de la valeur des données pour la mission, le service et le bien public, la collecte d'informations clés afin de créer des normes et des règles en guidant un gouvernement (Etat) dans la mise en œuvre d'une gouvernance éthique et d'une conception consciente et d'une culture d'apprentissage.
Les données stratégiques comprennent des informations qui mènent au développement et à l'évolution dans des sujets tels que l'économie, les statistiques sociales, les données politiques, les progrès technologiques.

La direction et la nature de l'économie dans laquelle la société évolue peuvent être rapportées dans des données économiques. Des informations sur les modes de vie, les croyances et les attitudes des personnes appartenant à l'environnement externe d'une entreprise peuvent être incluses dans les données sociales. Les données politiques incluent des informations légales et réglementaires, telles que la fiscalité et le droit du travail.

Qu'est-ce qu'une donnée personnelle ?

C'est une information à propos d'une personne physique identifiée de façon directe ou non. Ce peut être un nom, une adresse IP, un numéro de téléphone, une adresse postale, une adresse email, une empreinte (digitale, rétinienne…), un enregistrement vocal ou vidéo, un numéro de sécurité sociale etc.

Ces données sont dites sensibles car elles peuvent donner une ou des indications sur une personne pouvant donner lieu à de la discrimination ou des préjugés. Par exemple : Une opinion politique, une religion, un dossier médical etc.

Pour pouvoir être collectées, toutes ces données doivent avoir obtenu le consentement du propriétaire de celles-ci. Si l'utilisateur n'a pas donné son consentement écrit, de façon claire et précise, alors c'est interdit.

Droits de l'utilisateur

La loi de protection des données de 2018 stipule qu'un utilisateur a le droit de connaître les informations dont dispose le gouvernement et autres organisations à son encontre.

L'utilisateur a également le droit de :

- Être informé de la manière dont ses données sont utilisées.
- Accéder à des données personnelles.
- Avoir des données incorrectes mises à jour.
- Avoir des données effacées.
- Arrêter ou restreindre le traitement de ses données.
- La portabilité des données (permettant d'obtenir et de réutiliser ses données pour différents services).
- S'opposer à la façon dont ses données sont traitées dans certaines circonstances.

L'utilisation des données transforme le monde

Le moyen par lequel les acteurs fournissent et utilisent les données, tient une place unique dans la société. Le maintien de cette confiance dans les données est essentiel à un processus démocratique efficace. Les Etats ont besoin d'une approche coordonnée et intégrée d'utilisation des données pour mener à bien leur mission, servir le public et gérer les ressources tout en respectant la vie privée et la confidentialité.

Ces données stratégiques fournissent des indications sur la manière dont les agences devraient gérer et collaborer entre elles pour l'évolution des pratiques à mener pour s'améliorer.

La stratégie en matière de données se compose de principes et de pratiques visant à tirer parti de la valeur de l'ensemble du portefeuille de données tout en protégeant la sécurité, la confidentialité des données personnelles.

En règle générale, les données stratégiques impliquent des informations relatives au secteur dans lequel la société évolue. Les données industrielles peuvent inclure les barrières à l'entrée,

le pouvoir des fournisseurs et des acheteurs, la capacité des consommateurs à remplacer le produit et le nombre de concurrents dans l'industrie.
Les données collectées sur les concurrents directs aident les spécialistes du marketing à donner aux produits une apparence supérieure aux produits concurrents.
Les données sur les clients aident les spécialistes du marketing à créer des profils de consommateurs qui les aident dans tous les domaines, de la création de produits à la distribution, en passant par la publicité.
Les données relatives au travail et à la comptabilité aident au contrôle interne des finances et de la productivité.
Les données stratégiques aident également les spécialistes du marketing à rester en phase avec les tendances, ce qui permet de créer des produits en demande et des publicités attrayantes.

Le RGPD
C'est le Règlement Général sur la Protection des Données (ou GDPR en anglais, pour *General Data Protection Regulation*), dont le nom plus formel est le Règlement du Parlement Européen et du Conseil du 27 Avril 2016. Tous les résidents de l'Union européenne sont concernés par cette réglementation.
Avant celui-ci existait une directive sur la protection des données personnelles datant de 1995, celle-ci fût abrogée par le RGPD.
Son objectif est de servir de référence concernant le traitement des données personnelles au sein de l'Union européenne. Avec l'explosion de la bulle internet et les nouveaux usages de numériques toujours plus complexes et nombreux, il était nécessaire qu'une telle réforme voit le jour.
Il s'agissait également d'harmoniser le cadre juridique entre les pays de l'Union européenne et qu'il n'y ait plus qu'un seul texte de référence entre les états membres.

La protection des données au Royaume-Uni
En 1984, le Royaume-Uni a instauré la législation sur la protection des données à la demande des entreprises qui subissaient des pertes de données personnelles lors d'échanges commerciaux avec leurs voisins frontaliers.
Jusqu'à lors, le Royaume-Uni était considéré comme un « *Paradis des données* ».
La Directive 95/46/CE fut introduite à la suite de différends politiques et économiques, cette conséquence amena la demande de cette loi supranationale sur la protection des données visant à contrôler le flux des données transfrontalières.
Chacun des Etats membres a appliqué ces dispositions au travers de lois internes. En l'occurrence pour le Royaume-Uni, à travers le Data Protection Act 1998. Cependant, chaque état membre n'a transposé ces dispositions de manière identique, par conséquent, le résultat est une exécution fragmentée.
Cet échec des Etats membres à transposer cette directive de façon uniforme a été l'élément clé dans la décision pour la remplacer par un règlement. De plus, l'incertitude planait sur le fait qu'elle soit toujours adaptée à l'objectif initial quant aux avancées technologiques dans le traitement des données.
Le Règlement Général sur la Protection des Données est entré en vigueur le 25 Mai 2018 pour les pays membres de l'Union européenne, celui-ci remplace la Directive 95/46/CE et sera appliqué au Royaume-Uni sans qu'ils n'aient le besoin de le transposer en droit interne.

En revanche avec le Brexit qui subit de nombreux reports, ils ont été dans l'obligation d'abonnir le DPA 1998 pour s'accorder avec les exigences du RGPD 2016/679.
Avec sa future sortie de l'Union européenne, le Royaume-Uni sera soit dans l'obligation de s'accorder avec le RGPD, soit de mettre en œuvre de leur côté leur propre loi sur la protection des données personnelles.
Le Royaume-Uni pourrait vouloir à présent rejoindre l'Association Européenne de Libre-Echange (*European Free Trade Association*), dont les membres sont la Norvège, l'Islande et le Liechtenstein afin de réaliser des échanges commerciaux par le biais de l'Espace Economique Européen (EEE), mais ceci les obligerait à se soumettre au RGPD.
Mais il semblerait que la situation puisse basculer à leur avantage en négociant un nouveau partenariat stratégique avec l'Union européenne, selon un communiqué du gouvernement dans le « White Paper » : « *Ils n'essayeront pas de devenir membre du marché unique, ils poursuivront à la place un nouveau partenariat stratégique avec l'Union européenne, incluant un accord de libre-échange ambitieux et compréhensif et un nouvel accord douanier* ». Ainsi, ils n'auraient pas à se soumettre au RGPD.

Data Protection Act 2018

Avec le Data Protection Bill 2017, le gouvernement Britannique avait répliqué en incluant par exemple, l'exemption de contrôle de l'immigration, ce qui va à l'encontre de l'idée originelle du RGPD.
La situation semblait restée floue quant au traitement et la protection des données sur le sujet de l'immigration par le Home Office britannique. Cette situation rappelle bien sûr le fameux scandale du Windrush.
"Les dispositions du RGPD ne s'appliqueront pas au maintien d'un contrôle d'immigration efficace, ou à l'enquête ou la détection d'activités qui compromettrait le maintien d'un contrôle efficace de l'immigration"
Selon le Guardian, Joe Egan, le président de la Law Society of England and Wales est très critique vis-à-vis du Data Protection Bill 2017 : "Quiconque cherche à obtenir ses propres données personnelles auprès du Home Office pourrait se voir refuser l'accès sans justification et sans possibilité d'appel."
Cette loi de 2018 concerne la protection des données a été créée pour déterminer quelle façon les informations personnelles sont utilisées par des entreprises, organisations ou tout simplement le gouvernement.
Toute personne responsable de l'utilisation de données personnelles doit suivre des règles dites « Principes de protection des données » :

- Utilisées équitablement, légalement et de manière transparente.
- Utilisées à des fins spécifiées et explicites.
- Utilisées de manière adéquate, pertinente et limitée au strict nécessaire.
- Conservées plus que nécessaire.
- Traitées de manière à assurer une sécurité appropriée, y compris une protection contre le traitement illégal ou non autorisé, l'accès, la perte, la destruction ou les dommages.

Un renforcement juridique peut être nécessaire pour les informations plus sensibles telles que :

- L'origine ethnique.
- Opinions politiques.

- Croyances religieuses.
- Affiliation syndicale.
- La génétique.
- Biométrie (utilisée pour l'identification).
- Santé
- Vie sexuelle ou orientation.

Privacy shield

Le problème majeur à ce jour et qui concerne les utilisateurs d'Internet dans le monde entier reste celui de la confidentialité.

Avec l'essor du commerce en ligne et des données transitant toujours plus nombreuses par-delà les frontières internationales et en particulier entre les Etats-Unis et l'Europe a mené à se poser la question quant aux problèmes de confidentialité d'un point de vu gouvernemental. Il arrive parfois que ces fuites de données pourraient provenir d'une attaque cyber, mais sans compter sur la manière dont les entreprises, grandes et petites, gèrent leurs flux de données. C'est pourquoi, afin de mieux protéger les internautes européens dont leurs données transitent au-delà de la frontière Américaine, le ministère du commerce des Etats-Unis et la commission européenne ont développé ensemble ce « Bouclier » pour protéger la vie privée de ces internautes.

Grâce à ce *Privacy Shield*, les utilisateurs européens sont à priori protégés par un règlement établi pour leur garantir que leurs données qui entrent ou sortent des Etats-Unis disposent de mesures de protections adéquates en vertu des lois européennes.

La mise en place du Privacy Shield

C'est le 12 Juillet 2016 que la Commission européenne et le gouvernement des Etats-Unis ont adopté conjointement ce règlement.

L'union européenne a mis au point une loi particulière, à savoir la directive sur la protection des données. Celle-ci limite la façon dont les entreprises comme Facebook, Google ou encore des organismes d'état comme la NSA utilisent et collectent nos données.

Alors, le *Privacy Shield Framework* agit comme un ensemble de règles qui régissent les entreprises américaines qui ont des activités en Europe.

L'adhésion à ce cadre est sur la base du volontariat, il y a d'ailleurs déjà des centaines d'entreprises américaines qui se sont volontairement certifiées. Toutes les entreprises qui acceptent d'y participer sont tenues de respecter cette norme. Une infraction à celle-ci pourrait leur entrainer une amende de près de 22 millions de Dollars US ou 4% du revenu brut mondial de l'entreprise pour l'année en cours. Tout signalement de violation de données doit être effectué dans les 72 heures après constatation de celle-ci.

La *Federal Trade Commission* interdit les actes « déloyaux et trompeurs » et son application découle directement de ces règles.

Malgré le fait que la Commission européenne et les Etats-Unis se soient entendus sur le point qu'il faille clarifier plus en profondeur tout ce qui concerne la collecte de données en masse et qu'il faut absolument renforcer le rôle du médiateur. La situation reste relativement opaque quant à l'efficacité mise en œuvre pour protéger les droits des citoyens européens.

Nous constatons que des mesures sont mises en place de plus en plus avec les années, ce qui est une bonne chose pour les citoyens et plus généralement les utilisateurs sur le Web.
Le cyberespace est un nouveau terrain de bataille où il faut s'armer vite et bien, où il faut se former et rester à la pointe des technologies pour pouvoir faire face aux nouvelles menaces actuelles et futures.
La résilience doit être au cœur des préoccupations pour chaque Responsable de la Sécurité des Systèmes d'Information, dans les mesures à prendre pour sécuriser les systèmes d'information des entreprises.
Toutes ces mesures sont-elles suffisantes ? Faudrait-il innover un peu plus pour parer aux futures menaces ?
Peut-être faudrait-il investir dans des cellules de Recherches et Développements afin d'anticiper ces futures menaces telles qu'il pourrait y avoir comme pour les IOT (**I**nternet **O**f **T**hing) par exemple ou encore le Cloud.
Près de la moitié des entreprises mettent en place des programmes de cybersécurité pour contrer les risques liés au Cloud. Nous constatons que les opinions changent concernant celui-ci, qui pourtant a été craint pendant plusieurs années pour son manque de contrôle sur la perte des données.
Le Cloud a créé une certaine dépendance parmi les grosses entreprises, qui voient là une opportunité de stocker en masse leur données, qu'elles soient ou non stratégiques pour celle-ci, de façon dématérialisée et sans avoir besoin de stocker ces dites données en dur directement chez elles.
74% des entreprises pensent encore être suffisamment préparées face aux failles de sécurité, alors que la moitié d'entre elles ne prennent pas les bonnes dispositions pour contre ces menaces.
Les entreprises tentent d'adopter une posture offensive, bien que la majorité parmi celles-ci, estiment être prêtes à faire face en cas d'attaque.
Pourtant peu nombreuse à avoir pris l'initiative de mettre en place des exercices de crise, c'est pourquoi les entreprises se reposent principalement sur les technologies pour contrecarrer les améliorations des techniques d'attaque toujours plus originales et inhabituelles.

Annexes

Sources

- Savez-vous vraiment où sont stockées vos données stratégiques ? | Juriguide. (2013, 9 juillet). Récupéré le 5 août, 2019, de https://www.juriguide.com/monde-des-affaires/savez-vous-vraiment-ou-sont-stockees-vos-donnees-strategiques/
- Amal Sahli, A. S. (2018, 27 avril). La chasse aux données personnelles - Infoguerre. Récupéré le 5 août, 2019, de https://infoguerre.fr/2018/04/chasse-aux-donnees-personnelles/
- Christophe Ingrain et Xavier Philipps, C. I. E. T. X. P. (2018, 16 mars). Il est urgent de protéger les informations stratégiques des entreprises. Récupéré le 5 août, 2019, de https://www.dalloz-actualite.fr/chronique/il-est-urgent-de-proteger-informations-strategiques-des-entreprises
- Cybersécurité : la confiance numérique, un vrai défi stratégique pour les organisations. (2017, 9 août). Récupéré le 9 août, 2019, de https://lexpansion.lexpress.fr/high-tech/cybersecurite-la-confiance-numerique-un-vrai-defi-strategique-pour-les-organisations_1928043.html
- Didier FROCHOT, D. F. (2019, 6 juin). Données personnelles : la loi du 6 janvier 1978 restructurée et son nouveau décret d'application en vigueur - Les Infostratèges. Récupéré le 5 août, 2019, de https://www.les-infostrateges.com/actu/donnees-personnelles-la-loi-du-6-janvier-1978-restructuree-et-de-son-nouveau-decret-dapplication-en-vigueur
- Du G7 au G8, la Russie bientôt de retour ? (2019, 21 août). Récupéré le 21 août, 2019, de https://bfmbusiness.bfmtv.com/monde/du-g7-au-g8-la-russie-bientot-de-retour-1753148.html
- Elisa Braun, E. B. (2018, 25 mai). Protection des données personnelles : ce qui change avec la nouvelle loi européenne. Récupéré le 5 août, 2019, de http://www.lefigaro.fr/secteur/high-tech/2018/04/25/32001-20180425ARTFIG00001-le-rgpd-cette-loi-sur-les-donnees-personnelles-a-laquelle-il-faut-vous-interesser.php
- Gaëtan GORCE et François PILLET, G. G. E. T. F. P. (2014, 16 avril). La protection des données personnelles dans l'open data : une exigence et une opportunité. Récupéré le 5 mai, 2019, de http://www.senat.fr/rap/r13-469/r13-469_mono.html?fbclid=IwAR0YJrvKvh94DjSxpMoIchoowffhWwZv9I9rN7YjMFWYz5qKXCizgZCcZy4
- Hubert De LANGLE, H. D. L. (2018, 2 mars). PENSER LA GUERRE ECONOMIQUE. Récupéré le 5 août, 2019, de https://www.journaldeleconomie.fr/PENSER-LA-GUERRE-ECONOMIQUE_a5705.html
- Isaure Magnien, I. M. (2018, 17 mai). Cybersécurité : l'Union européenne contre-attaque. Récupéré le 5 août, 2019, de https://www.touteleurope.eu/actualite/cybersecurite-l-union-europeenne-contre-attaque.html
- Alain Gavriloff, A. G. (2019, 3 janvier). Légion d'honneur - Au Royaume-Uni, en France, aux États-Unis, les distinctions s'accumulent pour le Nivernais Louis Pouzin, un des pères d'internet. Récupéré le 5 août, 2019, de https://www.lejdc.fr/nevers-

58000/actualites/au-royaume-uni-en-france-aux-etats-unis-les-distinctions-s-accumulent-pour-le-nivernais-louis-pouzin-un-des-peres-d-internet_13098569/
- Laurent Mauriac et Emmanuèle Peyret, L. M. E. T. E. P. (1998, 27 mars). Et la France ne créa pas l'Internet... Cyclades est le projet français qui aurait pu avoir le même succès que les travaux américains qui ont abouti à l'invention du réseau mondial. Prometteur, il est pourtant mort-né. Récit d'un beau gâchis. Récupéré le 5 août, 2019, de https://www.liberation.fr/ecrans/1998/03/27/et-la-france-ne-crea-pas-l-internet-cyclades-est-le-projet-francais-qui-aurait-pu-avoir-le-meme-succ_231404
- Leonid Grustniy, L. G. (2018, 14 décembre). Top 5 largest data leaks of 2017 — so far. Récupéré le 5 août, 2019, de https://www.kaspersky.com/blog/data-leaks-2017/19723/
- What are the Privacy Shield Principles? (s.d.). Récupéré le 5 août, 2019, de https://www.bbb.org/EU-privacy-shield/privacy-shield-principles/
- Julien Lausson, J. L. (2019, 25 mai). RGPD : 15 questions pour comprendre le règlement sur la protection des données personnelles. Récupéré le 5 août, 2019, de https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-etes-un-internaute.html
- La cybersécurité : un pilier robuste pour l'Europe numérique - Sénat. (2018, 20 avril). Récupéré le 5 août, 2019, de https://www.senat.fr/notice-rapport/2017/r17-458-notice.html
- La protection des données dans le monde | CNIL. (s.d.). Récupéré le 5 août, 2019, de https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde
- La Russie prête à « examiner » un éventuel retour au G8. (2019, 21 août). Récupéré le 21 août, 2019, de http://www.lefigaro.fr/international/la-russie-prete-a-examiner-un-eventuel-retour-au-g8-20190821
- Le Privacy shield | CNIL. (2017, 24 mai). Récupéré le 5 août, 2019, de https://www.cnil.fr/fr/le-privacy-shield
- Patrice Touraine, P. T. (2019, 13 juin). Point de repère cognitif : l'échec de l'informatique française en termes de stratégie de puissance - Infoguerre. Récupéré le 5 août, 2019, de https://infoguerre.fr/2019/06/point-de-repere-cognitif-lechec-de-linformatique-francaise-termes-de-strategie-de-puissance/
- Patrick RENARD, P. R. (2018, 9 janvier). Cybersécurité : de nouvelles exigences pour les fabricants de DM connectés. Récupéré le 5 août, 2019, de https://www.devicemed.fr/dossiers/reglementation/cybersecurite-de-nouvelles-exigences-pour-les-fabricants-de-dm-connectes/14807
- Protection des données personnelles : que contient la loi du 20 juin 2018 ? - Dossier d'actualité - Vie-publique.fr. (2018, 21 juin). Récupéré le 5 août, 2019, de https://www.vie-publique.fr/actualite/dossier/securite-internet/protection-donnees-personnelles-que-contient-loi-du-20-juin-2018.html
- Queen's Printer of Acts of Parliament. (s.d.). Data Protection Act 2018. Récupéré le 5 août, 2019, de http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Rafaëlle Rivais, R. R. (2019, 30 janvier). Airbus a détecté un « incident de cybersécurité » dans sa division d'avions commerciaux. Récupéré le 5 août, 2019, de https://www.lemonde.fr/pixels/article/2019/01/30/airbus-a-detecte-un-incident-de-cybersecurite-dans-sa-division-d-avions-commerciaux_5416911_4408996.html
- RGPD nouvelle réglementation : obligations pour les entreprises pour 2018. (2017, 24 novembre). Récupéré le 5 août, 2019, de https://www.wooxo.fr/Wooxo-news/Le-

blog-Wooxo/Nouvelle-reglementation-RGPD-et-protection-des-donnees-ce-que-les-entreprises-doivent-savoir
- Utilisation stratégique des données dans les entreprises. (s.d.). Récupéré le 5 août, 2019, de https://www.pwc.fr/fr/vos-enjeux/liberer-potentiel-de-vos-donnees-et-accelerer-prise-de-decision/strategie-des-donnees-dans-les-entreprises.html
- Wikipedia contributors. (2018, 23 décembre). Discipline de gestion qui valorise les données en tant que ressources numériques. Récupéré le 5 août, 2019, de https://fr.wikipedia.org/w/index.php?title=Gestion_des_donn%C3%A9es
- SSI Gouv. (2017). Stratégie nationale pour la sécurité du numérique. Récupéré le 5 août 2019, de https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
- International Journal on Cybernetics & Informatics (IJCI). (2019, 02 Avril). A comparative analysis of the cyber security strategy of Bangladesh, Récupéré le 5 août 2019, de https://arxiv.org/ftp/arxiv/papers/1905/1905.00299.pdf
- Interdisciplinary Journal of Information, Knowledge, and Management. (2014). A Comparison of International Information Security Regulations, Récupéré le 5 août 2019, http://www.ijikm.org/Volume9/IJIKMv9p089-116Johnson0798.pdf
- International Telecommunication Union. (2015, 1er Juillet). A comparative analysis of cybersecurity initiatives worldwide, Récupéré le 5 août 2019, http://www.itu.int/osg/spu/cybersecurity/docs/background_paper_comparative_analysis_cybersecurity_initiatives_worldwide.pdf
- The Governance of Cybersecurity. (2015, Novembre). A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK, Récupéré le 5 août 2019, https://pdfs.semanticscholar.org/9f4c/b321bd2ca3a3c2f253066ccab7c4f39098ef.pdf

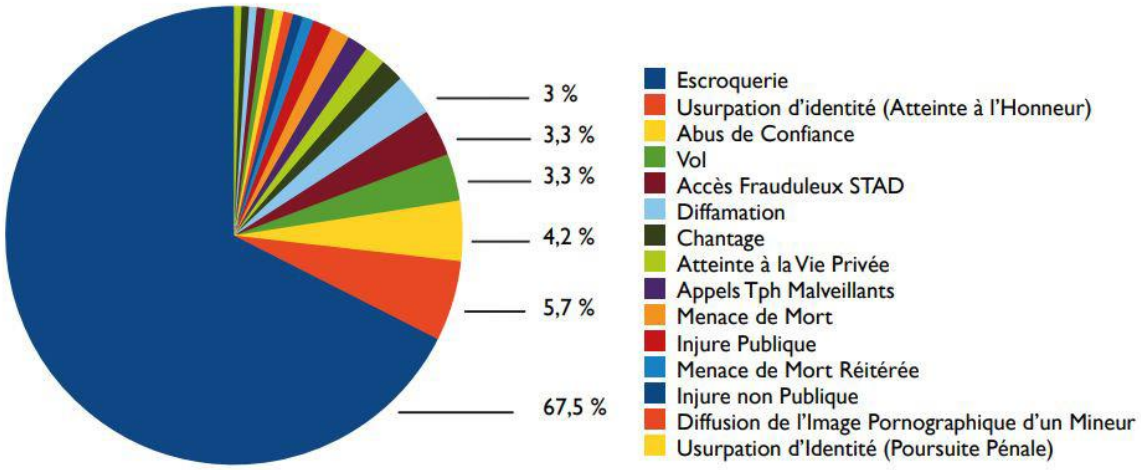
Bibliographie

- Planning, S. (2007). Assays for Determination of Protein. In *Current Protocols in Food Analytical Chemistry*.
- Brechbühl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development*. https://doi.org/10.1002/itdj.20096
- Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. In *IEEE Transactions on Systems, Man, and Cybernetics Part A : Systems and Humans*. https://doi.org/10.1109/TSMCA.2010.2048028
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*. https://doi.org/10.22215/timreview/835
- OECD. (2011). Reducing Systemic Cybersecurity Risk. *Sort*. https://doi.org/10.3163/1536-5050.98.2.021
- Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2016.07.002
- Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*. https://doi.org/10.1109/TPWRS.2008.2002298

- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*. https://doi.org/10.1016/j.jaccpubpol.2015.05.001
- Murphy, J. F. A. (2018). The General Data Protection Regulation (GDPR). *Irish Medical Journal*.
- Van Alsenoy, B. (2019). General Data Protection Regulation. In *Data Protection Law in the EU: Roles, Responsibilities and Liability*. https://doi.org/10.1017/9781780688459.021
- Stead, A. (2018). Data Protection Act 1998. In *Information Rights in Practice*. https://doi.org/10.29085/9781856049931.002
- Steel, B. S. (2014). Arpanet. In *Science and Politics: An A-to-Z Guide to Issues and Controversies*. https://doi.org/10.4135/9781483346328.n15
- Rosen, E. C. (2004). Vulnerabilities of network control protocols. *ACM SIGCOMM Computer Communication Review*. https://doi.org/10.1145/1015591.1015592
- Lukasik, S. J. (2011). Why the arpanet was built. *IEEE Annals of the History of Computing*. https://doi.org/10.1109/MAHC.2010.11
- Tronco, T. R. (2010). A brief history of the internet. *Studies in Computational Intelligence*. https://doi.org/10.1007/978-3-642-13247-6_1
- Roberts, L. (1986). The Arpanet and computer networks. https://doi.org/10.1145/12178.12182
- Ganguly, D., & Lahiri, S. (2012). Cryptography and Network Security. In *Network and Application Security*. https://doi.org/10.1201/b11517-4
- Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. In *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2015.04.12

Schémas

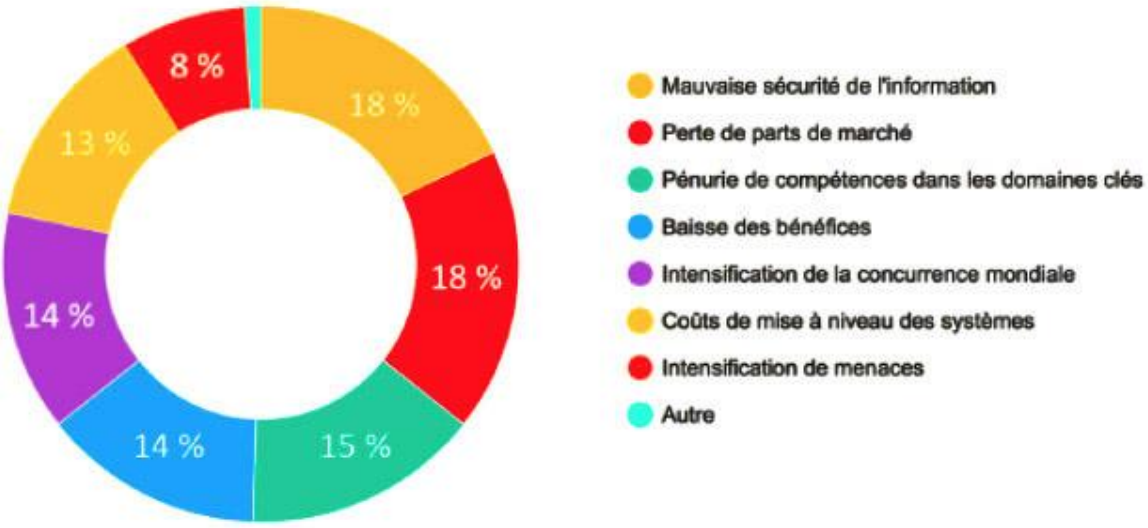
Répartition des infractions cyber les plus représentées par NATINF

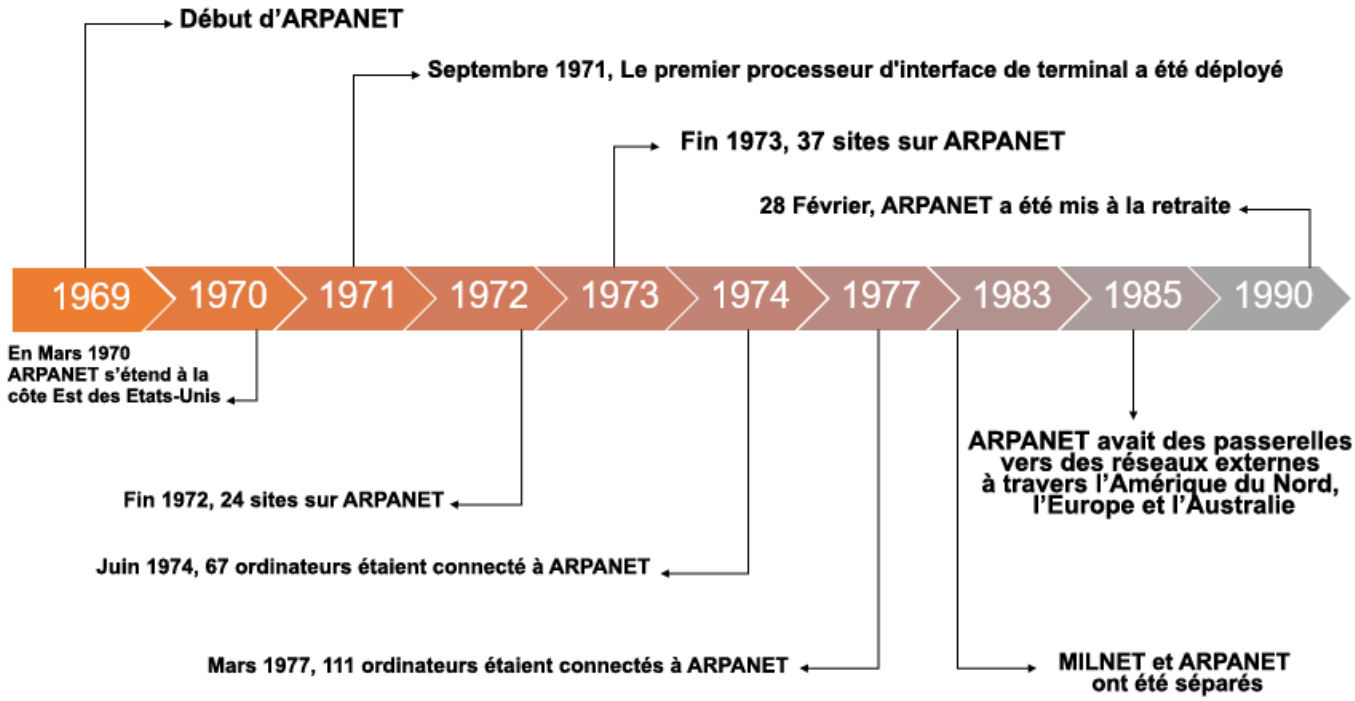


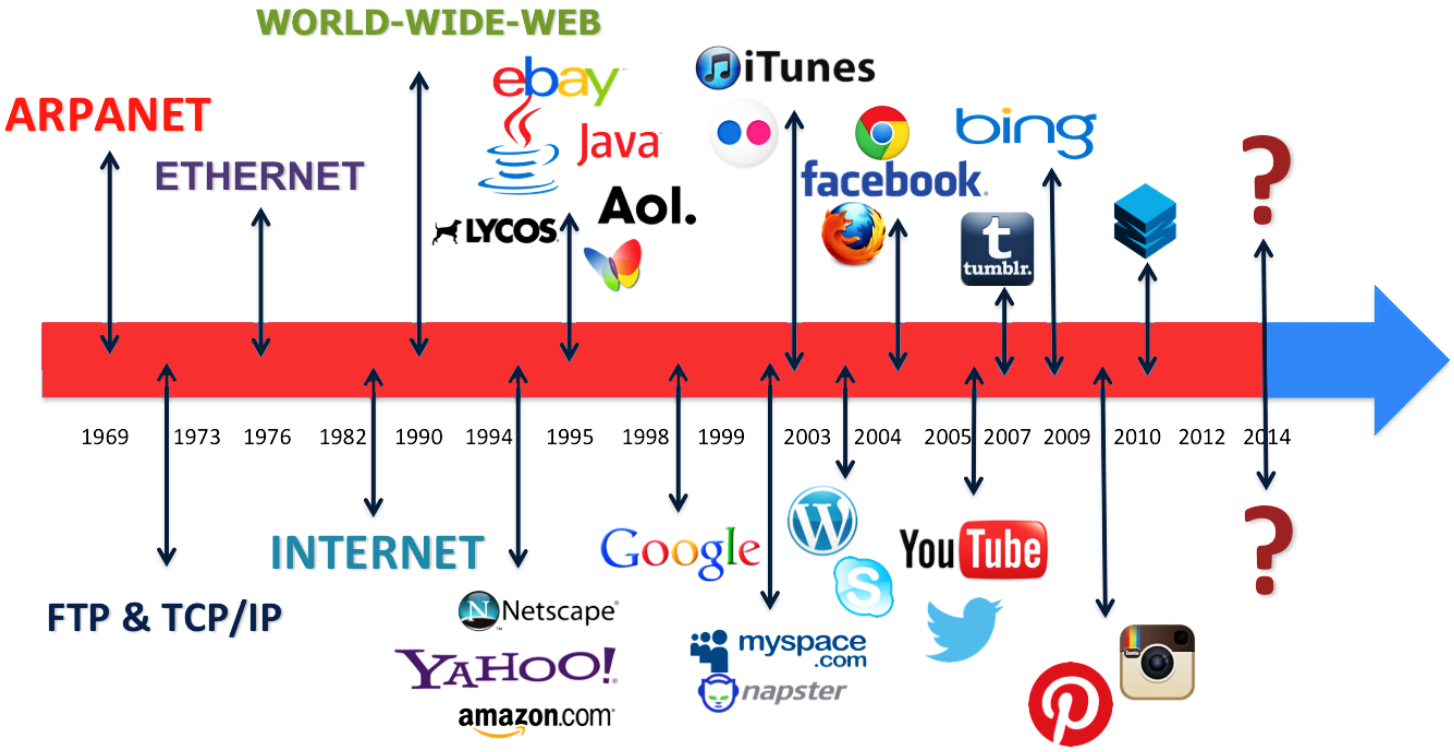
Etude CRPJ – Source : GN – C3N

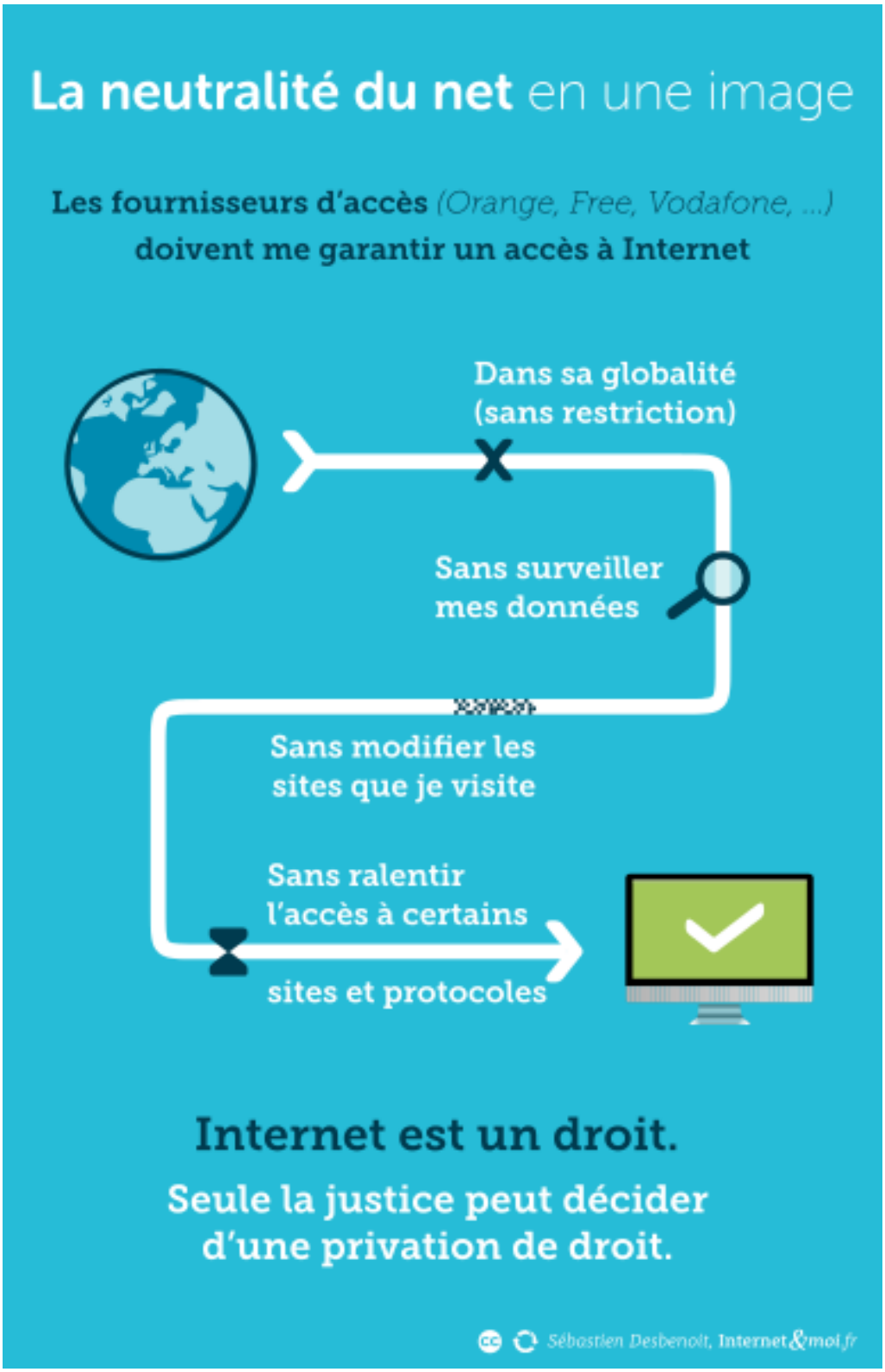
Quel est à vos yeux le risque n°1 pour votre entreprise ?

Question posée à la totalité de l'échantillon (1 000 sondés) - Étude réalisée par NTT Com Security

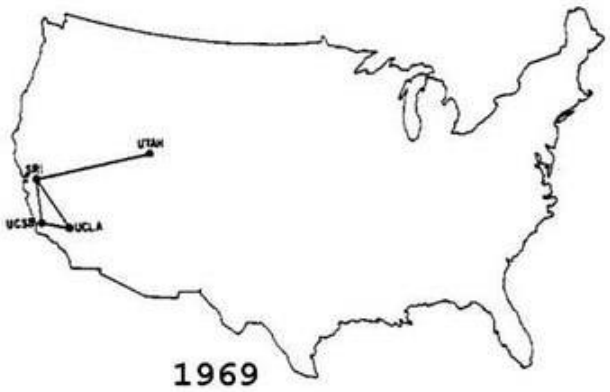



Début d'ARPANET
Septembre 1971, Le premier processeur d'interface de terminal a été déployé
Fin 1973, 37 sites sur ARPANET
28 Février, ARPANET a été mis à la retraite
1969
1970
1971
1972
1973
1974
1977
1983
1985
1990
En Mars 1970 ARPANET s'étend à la côte Est des Etats-Unis
Fin 1972, 24 sites sur ARPANET
Juin 1974, 67 ordinateurs étaient connecté à ARPANET
Mars 1977, 111 ordinateurs étaient connectés à ARPANET
ARPANET avait des passerelles vers des réseaux externes à travers l'Amérique du Nord, l'Europe et l'Australie
MILNET et ARPANET ont été séparés

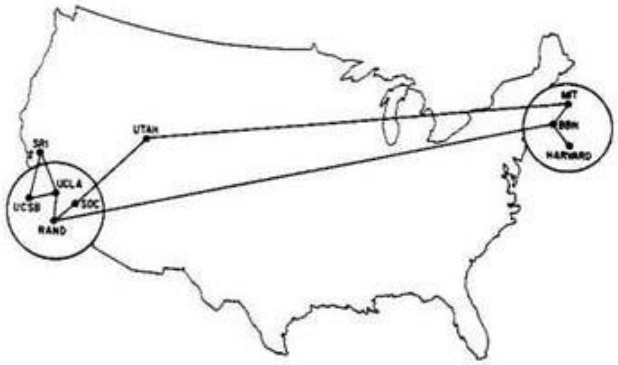

WORLD-WIDE-WEB
ARPANET
ETHERNET
ebay
Java
LYCOS
Aol.
iTunes
facebook
bing
tumblr.
?
1969
1973
1976
1982
1990
1994
1995
1998
1999
2003
2004
2005
2007
2009
2010
2012
2014
INTERNET
FTP & TCP/IP
Google
YouTube
?
Netscape
YAHOO!
amazon.com
myspace
.com
napster


La neutralité du net en une image
Les fournisseurs d'accès (Orange, Free, Vodafone, ...)
doivent me garantir un accès à Internet
Dans sa globalité
(sans restriction)
Sans surveiller
mes données
Sans modifier les
sites que je visite
Sans ralentir
l'accès à certains
sites et protocoles
Internet est un droit.
Seule la justice peut décider
d'une privation de droit.
Sébastien Desbenoit, Internet&moi.fr

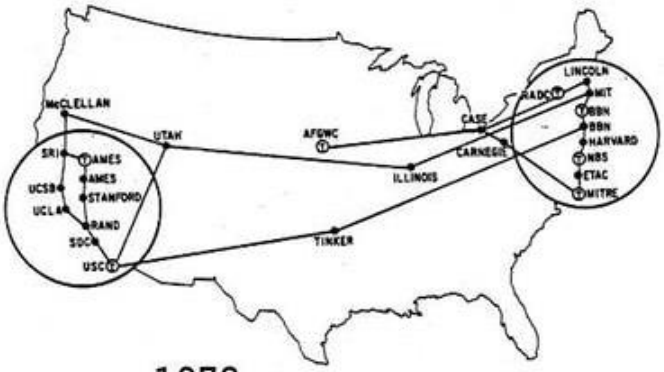
Progression d'ARPANET



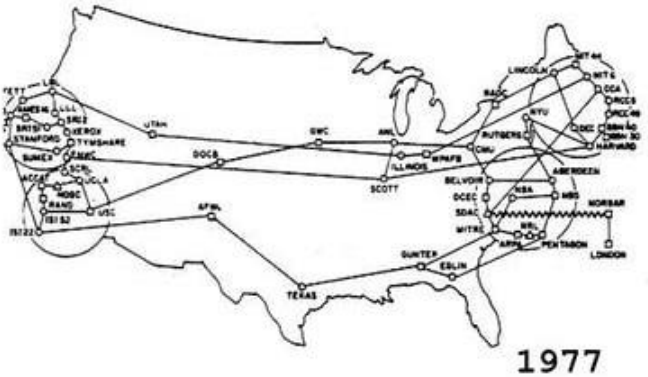
1969



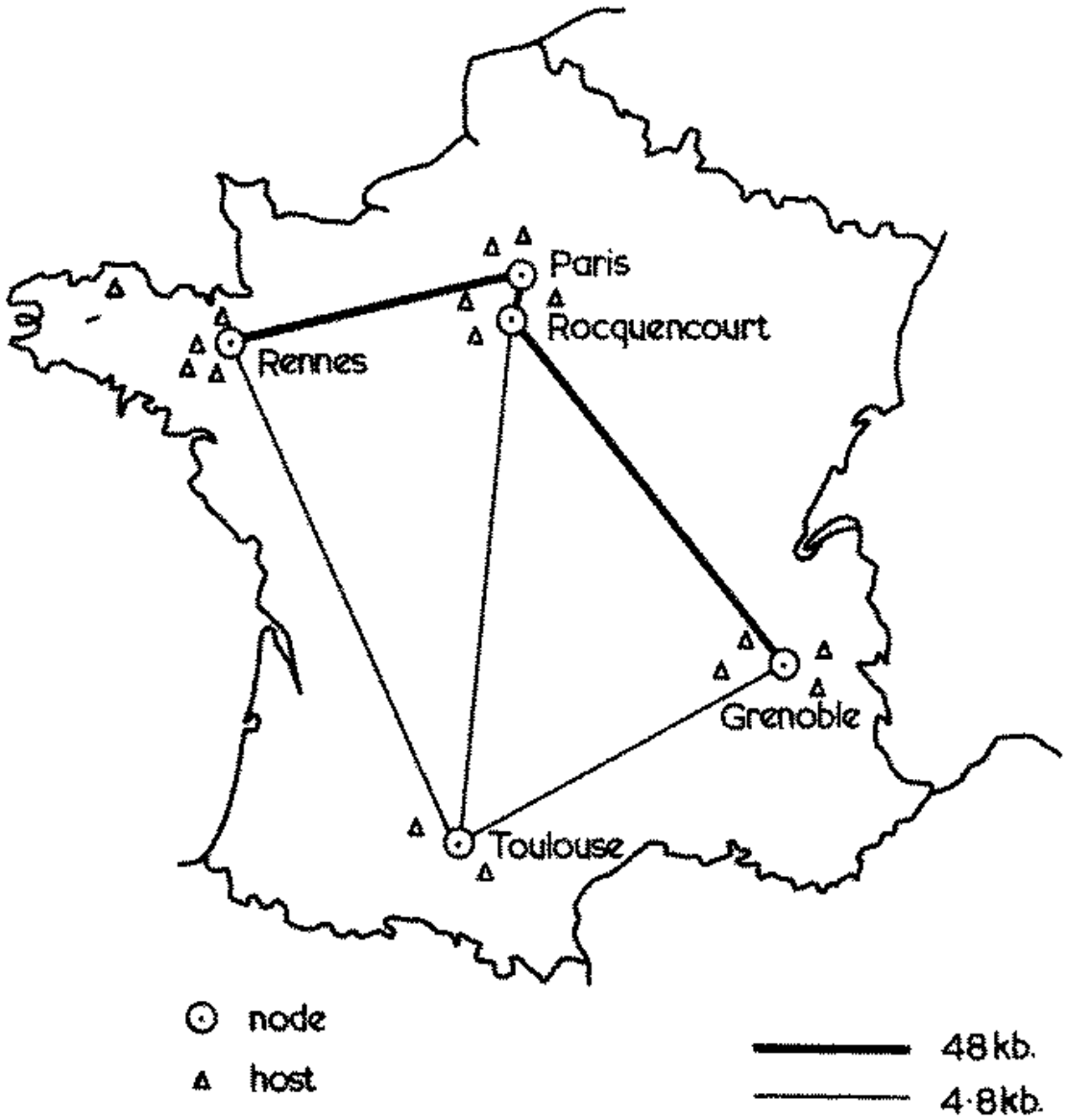
1970



1972

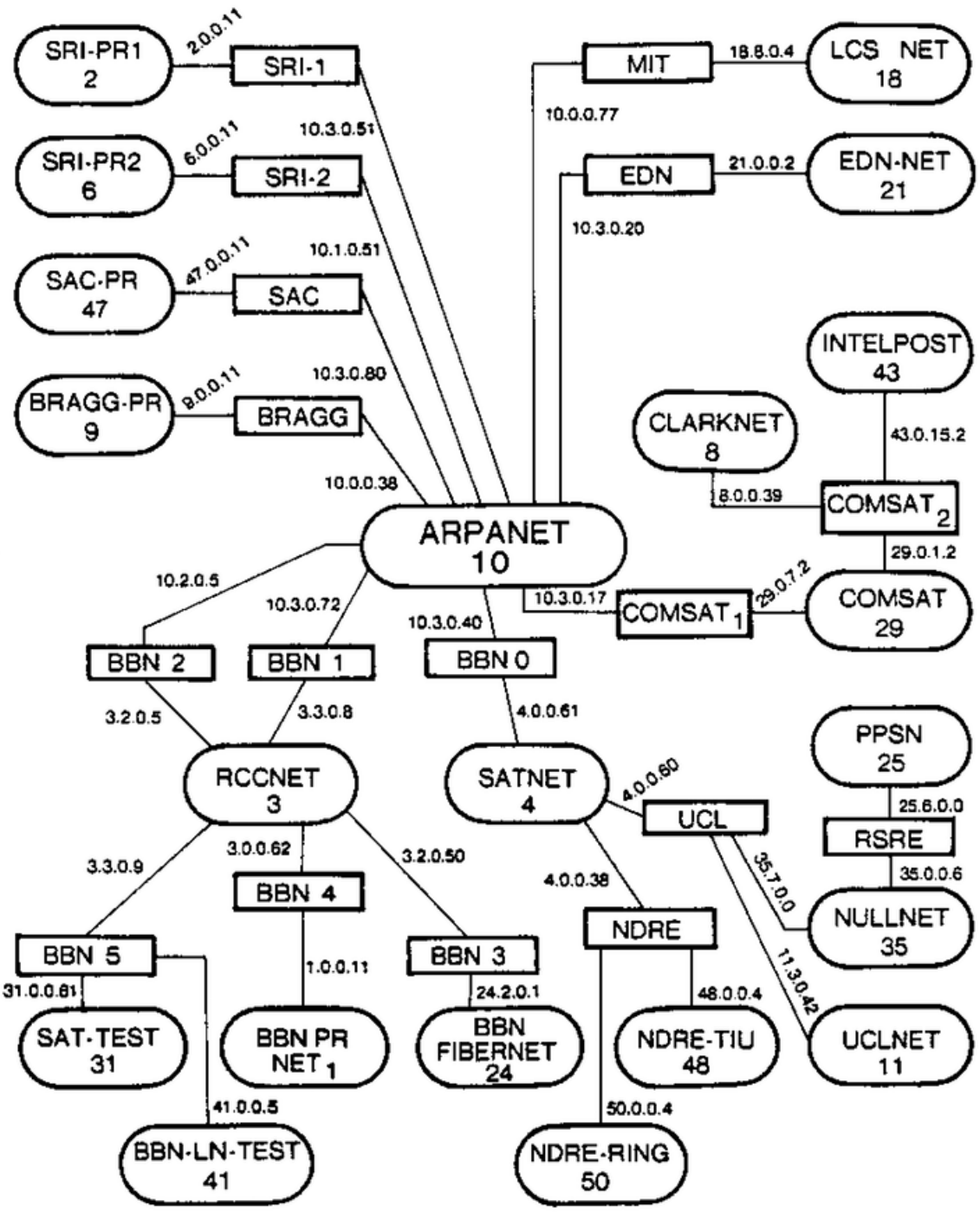


1977



16 Hosts - 6 types of computers - 8 operat. systems

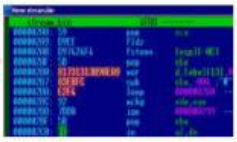
Fig. 1 CYCLADES NETWORK


SRI-PR1
2
2.0.0.11
SRI-1
SRI-PR2
6
6.0.0.11
SRI-2
SAC-PR
47
47.0.0.11
SAC
BRAGG-PR
9
8.0.0.11
BRAGG
10.3.0.51
10.1.0.51
10.3.0.80
10.0.0.38
ARPANET
10
MIT
18.6.0.4
LCS NET
18
10.0.0.77
EDN
21.0.0.2
EDN-NET
21
10.3.0.20
INTELPOST
43
CLARKNET
8
43.0.15.2
8.0.0.39
COMSAT 2
29.0.1.2
COMSAT
29
29.0.7.2
10.3.0.17
COMSAT 1
10.2.0.5
10.3.0.72
10.3.0.40
BBN 2
BBN 1
BBN 0
3.2.0.5
3.3.0.8
4.0.0.61
PPSN
25
25.6.0.0
RSRE
35.0.0.6
NULLNET
35
35.7.0.0
RCCNET
3
SATNET
4
4.0.0.60
UCL
11.3.0.42
UCLNET
11
3.3.0.9
3.0.0.62
3.2.0.50
4.0.0.38
BBN 4
NDRE
BBN 5
BBN 3
1.0.0.11
24.2.0.1
48.0.0.4
31.0.0.61
SAT-TEST
31
BBN PR
NET 1
BBN
FIBERNET
24
NDRE-TIU
48
41.0.0.5
50.0.0.4
BBN-LN-TEST
41
NDRE-RING
50

L’un des premiers ordinateurs du réseau Cyclades

Processus d'attaque (Aurora)

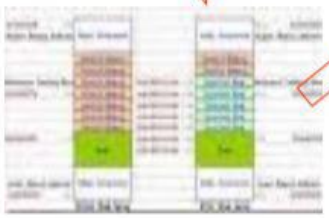
Etape 1 : Lien malveillant



Etape 4 : Script Shell

Etape 5 : Téléchargement

Etape 3 : Exploit d'Internet Explorer

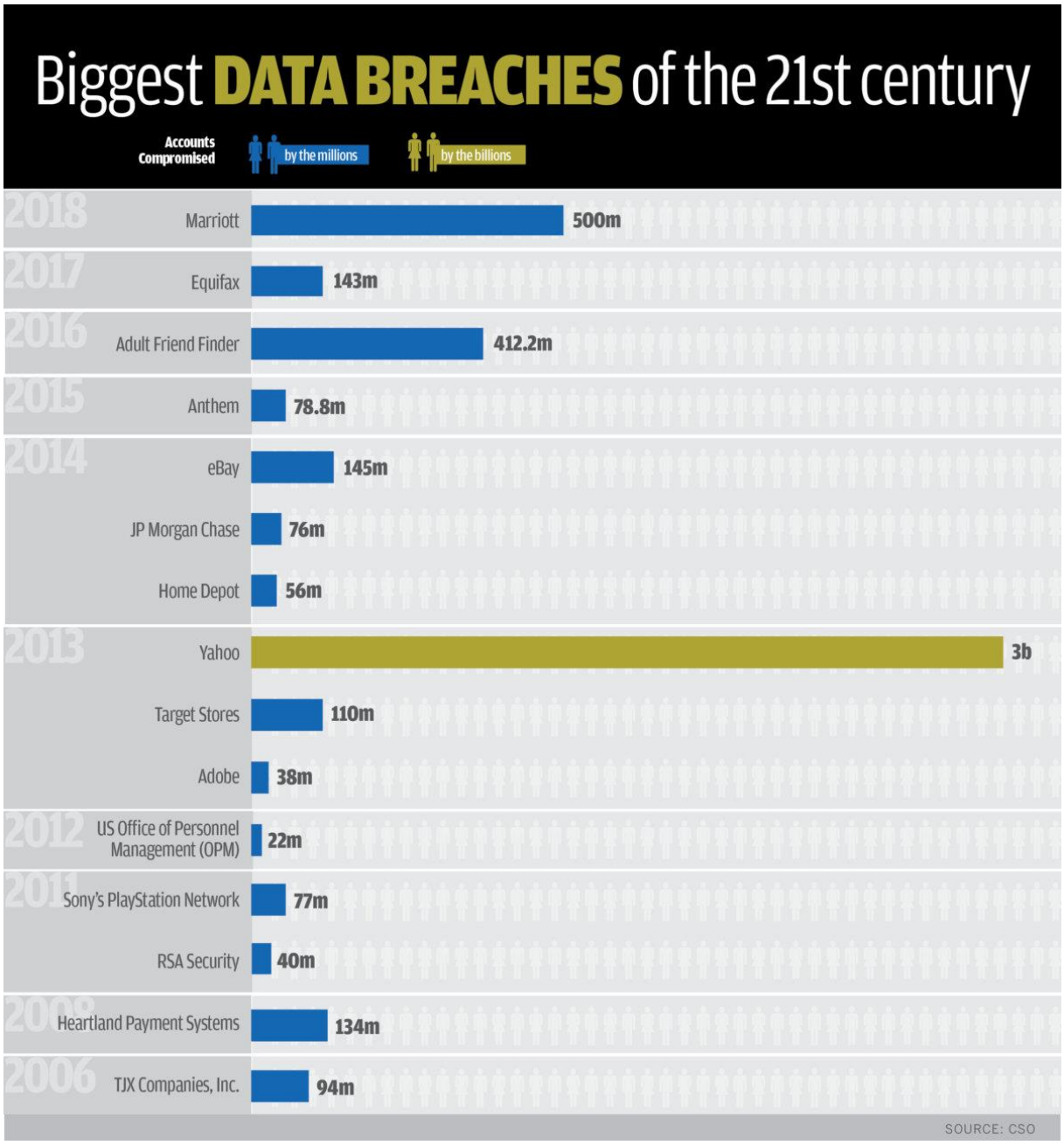


Etape 2 : «Heap spraying»
Exécution de code arbitraire

Etape 6 : Fichier malveillant

Etape 7 : Voler les informations

TREND MICRO


Biggest DATA BREACHES of the 21st century
Accounts Compromised
by the millions
by the billions
2018
Marriott
500m
2017
Equifax
143m
2016
Adult Friend Finder
412.2m
2015
Anthem
78.8m
2014
eBay
145m
JP Morgan Chase
76m
Home Depot
56m
2013
Yahoo
3b
Target Stores
110m
Adobe
38m
2012
US Office of Personnel Management (OPM)
22m
2011
Sony's PlayStation Network
77m
RSA Security
40m
2008
Heartland Payment Systems
134m
2006
TJX Companies, Inc.
94m
SOURCE: CSO