

# Géopolitique et Sécurité informatique

## Géographie

FÉV  
18  
2017

## En Bref

- (p. 2) Introduction ◀
- (p. 2) État contre État ◀
- (p. 3) Individu contre État ◀
- (p. 4) Conclusion ◀
- (p. 6) Types d'attaques informatiques ◀
- (p. 10) Red October ◀

### 1. Petit historique d'Internet

1934	Paul Otlet publie une vision prémonitoire de l'avènement d'Internet
1961	Premiers articles sur la communication par paquets
1965	Première communication longue distance entre ordinateurs
1969	ARPANET, le réseau développé par l'armée américaine et ancêtre d'Internet, acquiert 4 nœuds
1972	Création du système de message par Internet – les e-mails – et première démonstration publique du réseau
1989	Tim Berner Lee au CERN décrit les bases du web (page web, site web, etc.)
1992	Les ordinateurs sont devenus $10^9$ fois plus rapides qu'au début d'ARPANET, la bande passante est 20 millions de fois supérieure et Internet comporte un million d'hôtes
1998	Fondation de Google Inc.
2016	Internet compte 3,2 milliards d'internautes et c'est 205 milliards d'e-mails qui sont envoyés chaque jour

2. Cet article traitant de géopolitique, nous ne nous intéresserons qu'aux attaques contre des États dans ce document.

3. Voir l'annexe A

# 1 Introduction

« Internet »... Aujourd'hui, avec l'avènement des smartphones, le réseau électronique s'est infiltré partout. Son omniprésence semble faire penser à certains qu'Internet est un droit fondamental de l'Homme. Qui d'entre-nous ne s'est jamais senti bafoué par une mauvaise connectivité ?

L'expansion extrêmement rapide de ce moyen de communication dont les débuts remontent à il y a une cinquantaine d'années<sup>1</sup> pose cependant des questions parmi lesquelles celle de la sécurité. Initialement développé par l'armée américaine, ce réseau ne s'est jamais vraiment détaché des infrastructures vitales (armée, production et distribution d'énergie, gouvernements, etc.). Et si l'interconnexion d'ordinateurs de par le globe permet de mettre en commun les connaissances et d'augmenter la quantité d'informations échangées, elle expose aussi à tous des machines critiques pour la survie de nations entières.

Internet est un formidable moyen de communication qui a révolutionné notre mode de vie. Il a fait avancer la science et permis à l'humanité de se développer à un rythme jusqu'ici inégalé dans l'histoire. Mais c'est également un vecteur de fragilité ; sa création a exposé au monde beaucoup de systèmes essentiels et les rend ainsi susceptibles d'être la cible d'attaques.

Depuis la création du réseau, de multiples attaques visant des individus ou des États ont été constatées<sup>2</sup>. Nous nous proposons d'en détailler certaines dans la suite de ce texte, puis de discuter des modifications profondes qu'Internet a amené dans le cadre de la géopolitique.

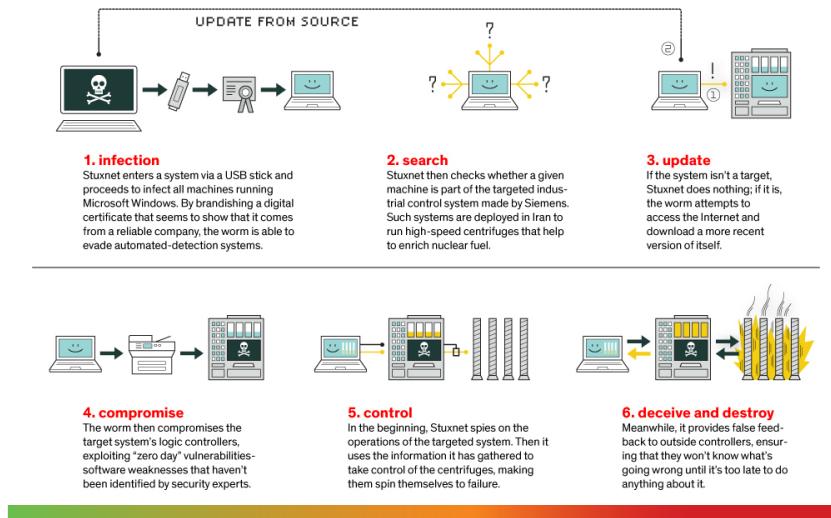
## 2 État contre État

L'histoire de l'humanité est entachée de guerres mêlant toutes les ethnies et tous les peuples. La taille des armées engagées dans de tels conflits a, au fil de l'histoire, continuellement augmenté pour atteindre, peut-être, son paroxysme lors de la Seconde Guerre Mondiale. Mais les guerres ont récemment changé d'apparence. Le facteur déterminant n'est plus le nombre de soldats allant se battre, mais la technologie et l'information dont chacun des partis dispose. Le conflit moderne, restant tout à fait meurtrier, ne se mène plus la baïonnette à la main mais plutôt le clavier sous les doigts et l'écran devant les yeux. Peu étonnant dès lors, qu'Internet devienne un facteur clé de la guerre du 21<sup>e</sup> siècle.

Un premier exemple d'un tel changement est celui du virus<sup>3</sup> Stuxnet, découvert en 2010 et probablement développé par les États-Unis et Israël. Il visait spécifiquement les ordinateurs des centrales nucléaires iraniennes et corrompait les programmes contrôlant les centrifugeuses d'enrichissement d'uranium, le tout résultant en de mystérieuses et inexplicables pannes. Le but d'une telle entreprise étant ici de ralentir le programme nucléaire iranien en empêchant la trop grande création d'uranium militaire. L'incidence d'un tel cas sur la géopolitique semble

évidente : une guerre larvée, dématérialisée, se déroule maintenant sur Internet entre les États pour des questions d'ordre politique.

## HOW STUXNET WORKED



**FIG. 1** Fonctionnement du virus Stuxnet

Autre coin du monde, autre conflit... Nous voilà maintenant dans l'ouest de l'Europe, à la frontière entre la Russie et l'Ukraine. Les tensions entre les deux nations induites par les conflits d'intérêts autour de la Crimée inquiètent. Et soudain, au soir du 23 décembre 2015, la région d'Ivano-Frankivsk sombre dans le noir total. La panne d'électricité touche près de 700'000 foyers durant plusieurs heures.

Pourquoi vous parler de cette panne ? Parce que la défaillance des services serait due à une attaque informatique lancée par des hackers pro-russe qui auraient utilisé une version modifiée du virus BlackEnergy<sup>4</sup> et que Kiev n'a pas manqué de pointer du doigt Moscou.

De fait, cette attaque marque un tournant dans l'histoire du hack. C'est la concrétisation d'un scénario catastrophe jusqu'ici resté hypothétique : les systèmes essentiels d'un pays sont touchés. La situation n'a causé aucun mort ni eu de conséquences trop sérieuses mais qu'en aurait-il été si les pirates avaient pris le contrôle des services de distribution d'eau, détruit le système de production/distribution d'énergie ou encore mis hors-service les réseaux de transport et de communication ?

4. Le crimeware (logiciel destiné à l'automatisation de tâches criminelles) BlackEnergy rassemble un certain nombre d'outils informatiques permettant de multiples actions néfastes : spam, création de réseaux de botnets, pénétration de toutes sortes de dispositifs (routers, ordinateurs, contrôleurs de machines industrielles, etc). Il est principalement utilisé par les réseaux de hackers russes et a déjà servi à attaquer de grandes organisations comme l'OTAN.

## 3 Individu contre État

Le conflit se déplace vers des éthers composés de zéros et de uns. Et il est évident que les États, disposant de moyens conséquents, peuvent développer des armes digitales puissantes. Cependant, Internet est un univers dont les règles ne correspondent en rien au monde matériel. Pour dupliquer un char d'assaut, il faut de l'argent, des hommes, des matières premières, beaucoup de connaissances scientifiques, etc. Pour dupliquer un virus, deux clics suffisent. Et ce changement de paradigme a opéré une véritable révolution. De nos jours, la participation au conflit digital n'est plus réservée aux seuls États mais est accessible à chaque

<sup>5</sup>. Des milliers d'ordinateurs particuliers de par le monde sont contaminés par des virus les utilisant, par exemple, comme des relais pour des attaques par déni de service (voir section A.1).



### <sup>6</sup>. Edward Snowden

Edward Snowden (né le 21 juin 1983), ancien agent de la CIA et de la NSA, est mondialement connu pour avoir copié des centaines de milliers de documents secrets de services comme la NSA, l'AIC (Australian Intelligence Community) ou encore le GCHQ (Government Communications Headquarters) et les avoir, par idéologie, rendus publics. Il est actuellement poursuivi par les États-Unis pour violation de l'*Espionage Act* de 1917 et vol de propriétés du gouvernement américain. Présentement en exil en Russie, il cherche asile quelque part dans le monde et risque des dizaines d'années de prison s'il est arrêté.

Documents publiés par Edward Snowden :  
<https://search.edwardsnowden.com>

*“Je ne peux, en bonne conscience, permettre au Gouvernement des États-Unis de détruire l'intimité, la liberté d'Internet et les priviléges élémentaires autour du monde, avec cette machine de surveillance massive qu'ils construisent secrètement.”*

— Edward Snowden



**240**

<sup>7</sup>. C'est le nombre de français qui seraient partis faire le Djihad en Syrie. Ce sont, en moyenne, des jeunes entre 18 et 25 ans qui partent, contactés directement par des vétérans djihadistes.

individu (que cela soit de manière volontaire ou non<sup>5</sup>).

Les dénonciations formulées par Edouard Snowden<sup>6</sup> sont un bon exemple de cette participation particulière. Dans ce cas, un seul individu a dévoilé les méfaits digitaux perpétrés par trois États — les États-Unis, l'Angleterre et le Canada. Ces derniers surveillaient et surveillent encore, à n'en pas douter, les communications passant par Internet. Le programme PRISM, un des logiciels développés dans le cadre de cette coopération, est chargé de collecter des données de toutes les grandes entreprises du net comme Google, Microsoft, Yahoo, Facebook ou Youtube et permet aux agents l'employant d'obtenir toutes sortes d'informations normalement privées (chat, commentaires, photos, e-mails, téléphonie par Internet, etc). L'annonce publique d'une telle surveillance le 5 juin 2013 avait eu un retentissement énorme dans les médias et pose la question des droits fondamentaux de l'individu face à l'État et celle de la vie privée.

Un autre cas où Internet joue un rôle prépondérant pour la géopolitique : le Djihad. Avec le printemps arabe le Moyen-Orient est devenu le théâtre de la montée en force de groupes islamistes radicaux. Et ces derniers font maintenant du recrutement en ligne par les réseaux sociaux, atteignant ainsi des populations plus éloignées que celles résidant au Moyen-Orient ; c'est l'Europe et plus généralement les pays développés comprenant des minorités musulmanes qui sont concernés<sup>7</sup>. Le groupe État islamique ne s'arrête pas seulement au recrutement, le défactionnement de site web est également devenu un outil. L'attentat de Charlie Hebdo fut d'ailleurs accompagné de centaines de sites web français piratés<sup>8</sup>. Internet est un instrument de propagande, mais aussi, et peut-être plus encore, de communication pour ces groupes. Il leur permet d'échanger informations et renseignements anonymement. Pour cette raison, les États-Unis ont lancé une véritable guerre informatique contre l'EIIL. 6000 soldats de l'US Army, spécialisés dans divers domaines digitaux, ont été placés sous la direction de l'amiral Michael Rogers (directeur de la NSA) avec pour but de surcharger les réseaux du groupe extrémiste, qui, ainsi, perdrait sa capacité à commander ses forces et son économie.

D'autres exemples de particuliers jouant un rôle important sur Internet viennent rapidement à l'esprit ; pour n'en citer qu'un : Anonymous. On assiste ici à un véritable changement d'échelle. L'individu a maintenant son mot à dire dans notre univers globalisé, il peut être entendu et ne saurait être ignoré des plus grands.

## 4 Conclusion

Soulignons-le encore, la création du réseau Internet est à marquer d'une pierre (blanche ou noire, chacun décidera) dans l'histoire de l'humanité. Ce nouveau moyen de communication a supprimé la notion de frontière en ligne et conduit à un bouleversement profond de notre mode et qualité de vie. Les conflits changent, les règles changent, les facteurs déterminants changent.

Toutes ces modifications apportent beaucoup de questions, auxquelles les lois peinent à répondre, car elles n'ont pas encore eu le temps de s'adapter (ce qui mène parfois à des procès partiaux<sup>9</sup>). Internet est un

lieu d'immense liberté, peu régulé. Il est facile d'y entrer dans l'illégalité et difficile de punir les coupables.

C'est un outil dont se servent les terroristes et les criminels pour faire du recrutement, de la vente et de l'achat d'armes et de drogues ; il est aussi un des derniers moyens de communication dont disposent les opprimés, il est une façon d'obtenir un peu d'anonymat, il est aussi la porte ouverte à la surveillance de masse. Ses multiples facettes sont innombrables.

Faut-il faire primer les États sur les individus ? Les États peuvent-ils se permettre de dépasser le cadre légal en ligne (surveillance, attaque d'autres États) ? La diffusion de logiciels de cryptographie puissants à tout un chacun est-elle à cautionner ?

Ces questions font couler beaucoup d'encre. Et il semble difficile de leur trouver une bonne solution. Mais une chose est sûre : l'informatique a une incidence importante sur la géopolitique. Elle va même très certainement augmenter. Ce qui est initialement une science va maintenant prendre une place de plus en plus grande dans la création, le déroulement et la résolution des conflits nationaux et internationaux. N'oublions donc jamais que...



Science sans conscience n'est que ruine de l'âme.

8. Quelques exemples de sites web défaillants :

- Site du Mémorial de Caen
- Site du Palais des Papes
- Site de la cathédrale de Nantes

9. Ross Ulbricht, fondateur du site web *The Silk Road* (site de vente de drogue sur le dark net, visant à démocratiser la vente et l'achat de drogue pour diminuer la criminalité associée à ce commerce), s'est vu condamné à perpétuité par la juge fédérale Katherine Forrest (États-Unis), alors que les preuves de l'accusation montraient de multiples incohérences et que certaines de ces preuves avaient probablement été obtenues illégalement.

## Quelques chiffres d'internet

### 205 mia

C'est le nombre d'emails envoyés chaque jour de part le monde. En tout, cela fait 74 trillions par année.

### 1\$ mia

C'est l'argent qu'un groupe de hacker d'Europe de l'Est nommé Carbanak a réussi à voler en deux ans grâce à des attaques de social engineering visant des centaines de banques.

### 38,5\$ mia

C'est le coût en dollar des dommages qu'aurait causé MyDoom dans les années 2004. Utilisant les pièces jointes des emails pour se propager, ce virus est connu pour être celui qui s'est disséminé le plus rapidement dans l'histoire de l'informatique.

### 1,6 mia

C'est le nombre d'utilisateurs Facebook en 2016.

### 10 mio

C'est le nombre d'attaques que subissait le département de la sécurité du gouvernement américain en 2012 par jour.

### 527 mio

C'est la quantité de tonnes de CO<sub>2</sub> émise par la production de l'énergie nécessaire à Internet. C'est équivalent à la pollution générée par la flotte aérienne mondiale. De fait, chaque recherche sur Google génère 0,2 gramme de CO<sub>2</sub> (un millier de recherches génère la même pollution qu'une voiture qui roule sur un kilomètre).

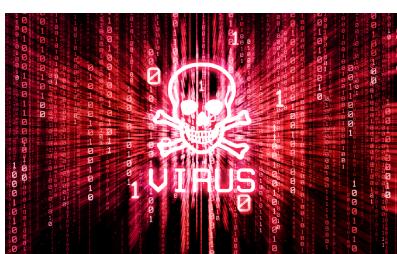
# A Attaques digitales et programmes malveillants

La sécurité informatique est un domaine extrêmement complexe et vaste. Il est par conséquent absolument impossible de dresser une liste complète de toutes les attaques possibles. En voici cependant une brève liste.

Les attaques digitales n'ont pas forcément ni le même but ni la même cible. On parlera d'attaques passives dans le cas où elles se contentent de récolter des informations. À l'inverse, l'attaque active tente de pénétrer un réseau, d'accéder à des ordinateurs puis de les pirater, d'obtenir plus de priviléges sur les machines compromises<sup>10</sup>, etc. Plus qu'écouter, elle agit.

Pour ce qui est des cibles, elles peuvent être de types très différents : réseaux, ordinateurs personnels, smartphones, routers, voitures connectées, compte email, site web, etc. De même, les buts recherchés peuvent varier immensément : défigurer un site web pour des raisons idéologiques, le mettre simplement hors-ligne, dériver les communications sortant d'une entreprise afin de pouvoir les écouter, usurper l'identité de quelqu'un en passant par son profil Facebook, gagner de l'argent en craquant des codes de cartes bancaires, etc. Internet est véritablement une jungle où le plus intelligent dicte sa loi.

10. Cette aspect du hack se nomme l'escalade de privilège et a pour but d'obtenir les droits administrateurs voire système (ce que normalement aucun utilisateur ne peut faire) sur un ordinateur.



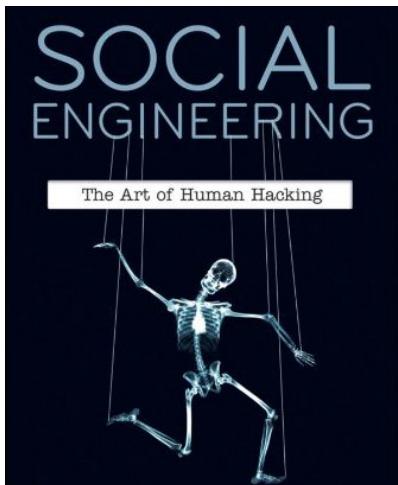
## A.1 Déni de service (distribué)

L'attaque par déni de service (distribué) nommée DoS (Denial of Service) ou DDos (Distributed Denial of Service) est une des attaques les plus courantes quand la cible est un site web. Elle consiste à demander des centaines de milliers de fois à un serveur web d'afficher une page du site qu'il héberge. La machine va tenter de faire cela au mieux et soutiendra, un moment du moins, la demande. Mais à terme la quantité de demandes trop importante fera surchauffer le serveur qui cessera de servir la page : le site web est alors mis hors-ligne. De telles attaques nécessitent d'être maintenues pour perdurer dans le temps. L'attaque distribuée implique non pas un seul attaquant mais des centaines voire des milliers de machines (souvent des réseaux de botnets). Elles sont beaucoup plus efficaces et difficiles à contrer.

## A.2 Virus, vers et chevaux de Troie

Sans rentrer dans trop de détails, ces trois catégories de programmes infectent les ordinateurs. Ils ont la capacité de se répliquer, soit à d'autres endroits sur une même machine, soit via le réseau, sur d'autres ordinateurs et donnent à l'attaquant de multiples possibilités : vol d'informations, accès secret à la machine, escalade de priviléges, transformer

l'ordinateur en « zombie » (il fera alors partie d'un réseau de botnet), etc.  
Pour compromettre la machine, ils utilisent des exploits (voir section  
[A.7](#)).



## A.3 Social Engineering

Peut-être l'attaque la plus dangereuse, elle vise le maillon le plus faible dans la chaîne de défense d'un système informatique : le facteur humain ! Elle consiste à manipuler des membres d'une entreprise ou d'un État par téléphone, via des emails ou tout autre moyen pour les pousser à donner mots-de-passe, adresses e-mail, adresses IP, etc. C'est très probablement aussi l'attaque dont on se méfie le moins car elle est moins connue et les entreprises, si elles investissent volontiers dans des anti-virus, ne pensent que trop rarement à former leurs membres.

## A.4 Pièces jointes corrompues

À l'inverse, cette attaque figure parmi les plus connues, elle consiste à envoyer une pièce jointe par e-mail contenant un fichier modifié de façon à pouvoir exploiter une faille dans le programme qui le lira (une faille dans le programme Word par exemple) pour pouvoir exécuter du code arbitraire sur la machine cible.

## A.5 Man in the middle

Dans cette attaque, l'attaquant dévie les communications entre deux personnes afin qu'elles passent par lui. Il peut ainsi « écouter » tout ce qui passe par le réseau entre ces deux individus. Il est même possible de modifier les données au vol afin que le contenu échangé corresponde à ce que l'attaquant veut qu'il soit. Certains protocoles de sécurité permettent d'éviter ce genre d'attaque mais elle reste très facile à exécuter sur certains dispositifs comme les Wifis.

## A.6 Faille XSS (Cross Site Scripting)

Aussi connue sous le nom d'injection SQL, cette attaque se décline en deux versions. Dans la première, nommée réfléchie (comme dans réfléchissant) ou non-persistante, des adresses web frauduleuses ou des formulaires remplis de façon particulière conduisent à l'exécution de code indésirable du côté client (par opposition au côté serveur). C'est la plus bénigne des deux dans le sens qu'elle ne change rien sur le serveur du site web et qu'elle ne peut causer que des dégâts limités chez le visiteur, car les langages clients sont généralement limités (vol de mots-de-passes, modification du contenu du site web du côté client uniquement). La deuxième, beaucoup plus dommageable, consiste à rentrer du code (SQL généralement) dans des formulaires mal protégés de sites web afin d'afficher ou de modifier des informations de la base de données normalement inaccessibles aux visiteurs. Cette dernière modifie le site web.



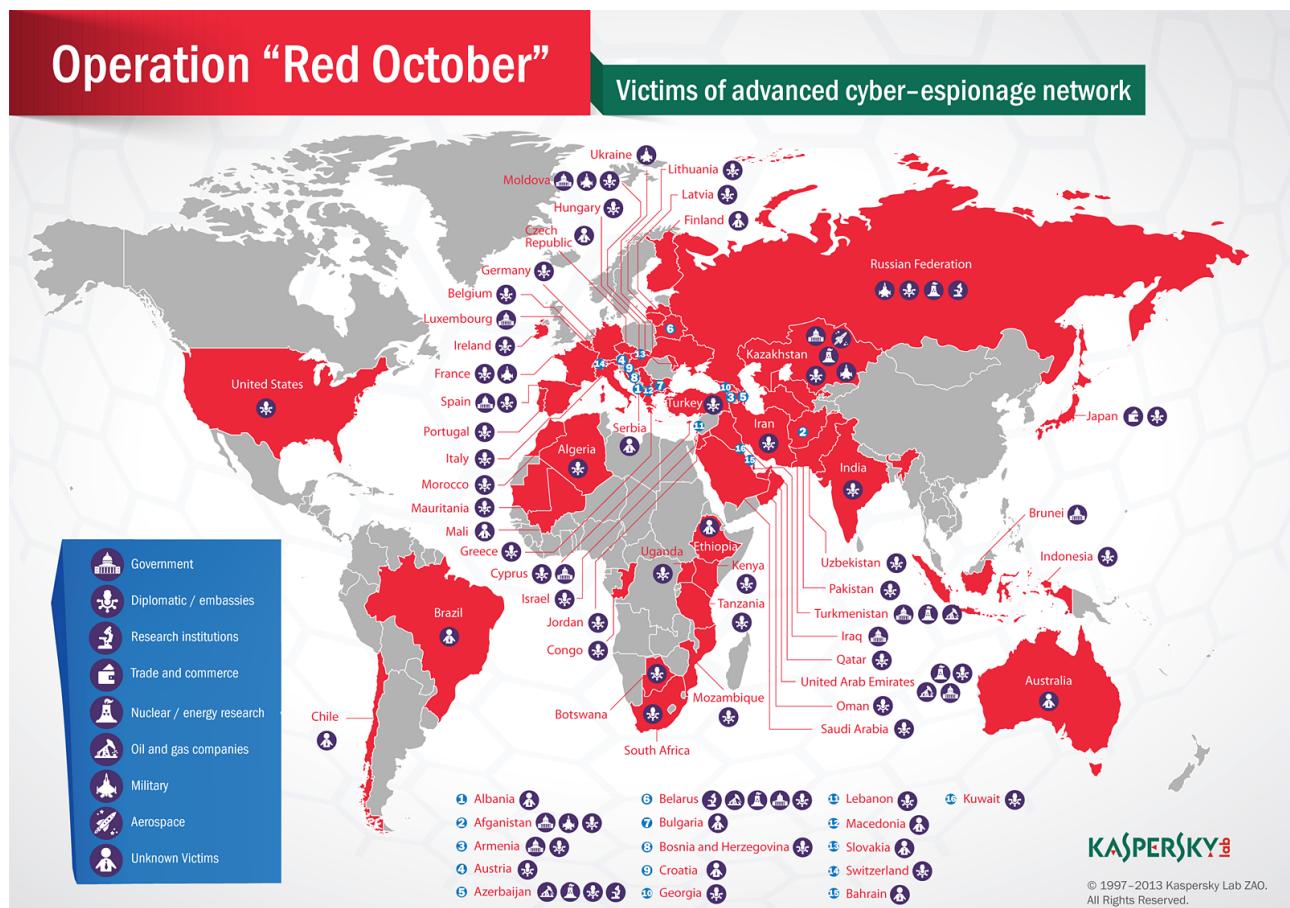
## A. Exploits et Zero-days

La plupart des attaques (pièce jointe malicieuse, virus, etc.) utilisent des exploits pour infecter les ordinateurs. Un exploit est une faille dans du code qui permet de détourner l'utilisation première à laquelle il était destiné. Elles peuvent être de types très variés. Les failles XSS, décrites plus haut, en sont un exemple. Elles fonctionnent car l'utilisateur peut entrer du code dans un champ texte (le programmeur ne vérifie pas suffisamment que l'entrée de l'utilisateur est celle attendue). Mais il en existe beaucoup d'autres. Une parmi les plus connues se nomme Buffer Overflow. Elle consiste à rentrer une chaîne de caractères beaucoup plus longue que celle attendue par l'ordinateur. L'attaquant dépasse la zone mémoire allouée pour la chaîne de caractères et écrit alors dans la mémoire temporaire de l'ordinateur (la RAM). Il peut ainsi lui faire exécuter du code arbitraire. Cette attaque figure parmi les plus répandues<sup>11</sup> et les plus dangereuses. Bien menée, elle peut conduire à la corruption totale d'un ordinateur (obtention des priviléges administrateur voire système).

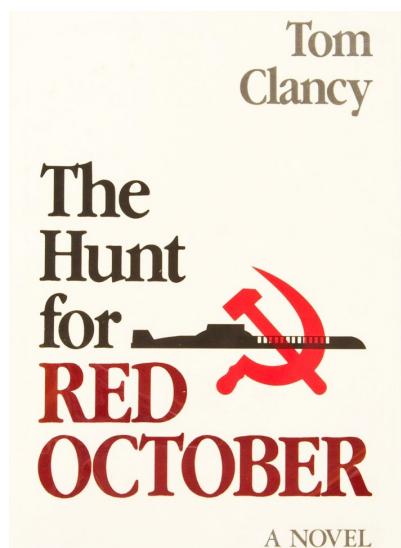
La plupart des exploits, une fois découverts, sont publiés et les responsables du code écrivent un correctif sous la forme d'une mise à jour. Cependant, les personnes qui cherchent ces exploits gardent parfois pour elles leurs découvertes, qui restent non-corrigées. C'est alors un exploit zero-day, une faille jusque-là inconnue du public dont il est quasiment impossible de se protéger. De telles faiblesses sont monnayées au prix fort sur le dark-net et parmi les acheteurs figurent parfois des gouvernements dont l'intention n'est pas de rendre leur achat public.

<sup>11</sup>. Le Buffer Overflow est une faille très répandue, car les langages C et C++, énormément utilisés depuis les années 80, ne vérifient pas que le contenu écrit dans la mémoire RAM ne dépasse pas la taille limite allouée.

# Red October



Petite anecdote intéressante, l'opération « Octobre Rouge » tire son nom de la nouvelle « The Hunt for Red October » par Tom Clancy. Red October est le nom d'un sous-marin russe dans la nouvelle.



L'opération « Red October » était une campagne de piratage lancée depuis au moins 5 ans avant d'être découverte, en janvier 2013, par le laboratoire de recherche Kaspersky. Cette attaque d'envergure visait principalement les ambassades et les gouvernements. Elle ne se limitait cependant pas à ces derniers : instituts de recherche scientifique, centrales nucléaires, bourses et services de l'aviation furent aussi touchés. En tout, c'est plus de 60 nations qui sont concernées, principalement dans l'Europe de l'Est et l'Asie, mais aussi certains pays « du nord » comme la Suisse ou les États-Unis.

Les victimes étaient infectées via une pièce jointe corrompue : un document Word ou Excel malicieux. Le virus ajouté à l'ordinateur relevait lui par contre d'une grande complexité. Propre au groupe pour l'instant inconnu de hackers menant cette opération, le programme Rocra (condensation de « Octobre Rouge » en russe) pouvait être augmenté de modules de cryptographie avancée, de modules pour les téléphones mobiles et même de code pour pouvoir réinfecter les machines qui auraient supprimé le virus principal.

Utilisant près de 60 serveurs de relai, Octobre Rouge a infecté des centaines d'ordinateurs clés (gouvernements, institutions diplomatiques, OTAN, etc.) de par le monde. L'attaque n'a pu être reliée à aucun pays

particulier mais l'exploit utilisé fut développé par des hackers chinois et le programme Rocra est écrit par des personnes russophones.

On estime que 7 terabytes<sup>12</sup> de données furent volés. Les types de fichiers concernés étaient divers : pdf, fichiers Excel, fichiers Word, etc. Cependant, beaucoup de fichiers portant l'extension .acid furent dérobés. Ces derniers étaient générés par le programme Acid Cryptofiler, un logiciel de cryptographie employé par l'armée française et l'OTAN.

12. 1 terabyte = 1000 gigabytes

L'influence d'une telle violation n'est pas à minimiser. Qui sait quels secrets furent volés ou déchiffrés. L'impact sur la géopolitique est ici plus évident encore que dans les exemples précédent, car l'attaque se concentrat sur la collecte d'informations touchant à ce domaine. Personne ne sait à quelles fins ces dernières furent utilisées. Elles ont probablement été vendues sur le dark-net ou utilisées directement.

