Elhasnaoui Med-Ali

Guerres, Crimes et Politiques: bienvenue dans le Cyberespace

Guerres,Crime et Poliques:

Bienvenue dans le Cyberespace

Elhasnaoui Med-Ali ©L0rdD4rk 2013

Dédicaces

Pour ma mère qui m'a toujours soutenue et mes neveux, en espérant qu'ils grandissent dans un monde plus sur.

Pour mes amis Petit Kard , Kensouyaroba et Le_Phenix , pirates devant l'Eternel et a nos longues nuits passées devant les écrans.

Je dédie aussi ce livre à Abir et sa mèche ,Audrey et ses stock-options, Boutaina et les 10 centimètres qui lui manquent , Dounia et son business , Kaltoumette et son théme ,Lapinou et son café sans sucre , Khadija et son Linux , Meriem et ses meubles, Rasha et sa voix ,Sarah et ses amis louches, Salma et son poste chez PwC, Selma et son lisseur, Soukaina et son Iphone chinois disparu dans des conditions tragiques , Yasmine et la cellule de prison qu'elle veux co-louer et Yousra et son coté phoque .

L0rdD4rk

L’auteur :

Elhasnaoui Med-Ali ne se présentera pas.
Vous pouvez néanmoins le suivre sur Twitter : @L0rdD4rk

Prologue

Dans Die Hard 4 , John McClane doit sauver le monde d'une bande de hackers terroristes qui se sont attaqués a des infrastructures aux Etats-Unis et qui menacent l'Humanité d'un Apocalypse au format numérique.

En sortant du cinéma , vous devez surement avoir penser que de telles choses sont impossibles.

Hélas…..elles le sont !

Et hélas…..il n'y a pas de John McClane pour vous sauvez……

Sommaire

We Want War !

Russie Vs Estonie

« *L'Ours sort de sa tanière* »

Après la fin de la seconde guerre mondiale, plusieurs république baltes dont l'Estonie, furent contraintes de faire partie de l'Union Soviétique après que cette dernière les ai «libérées » du joug nazis.L'armée rouge, où plutôt le parti communiste dont elle dépend, ont eu pour habitude de dresser dans toutes ces républiques de l'Est des statues commémorant le sacrifice des soldats « rouges », histoire que personne n'oublie qu'ils sont tombés pour la libération de ces pays.
Parmi ces statues, ce trouve celle de Tallin, capitale de l'Estonie, qui sera le déclencheur de ce que les experts appelèrent plu tard, la « Première guerre du Web ».
Depuis la chute du Mur de Berlin et l'effondrement du bloc communiste, les tensions entre la communauté russophone (qui représente 35% de la population estonienne) et les Estoniens de souche n'ont cessées d'être exacerbé et elles atteindront leur point culminant en février 2007 ,lorsque les législateurs estoniens ont votés la « Loi des structures interdites »,loi qui stipule que tout les monuments et les symboles hérités de l'époque communiste devront êtres enlevés, et parmi eux ,la fameuse statut de Tallin.
Moscou protesta en arguant que déplacer cette statue représente un viol de la mémoire des héros soviétiques.
Voulant éviter un incident qui pourrait avoir de lourdes conséquences, le président Estonien opposa son veto à cette loi, mais la pression publique pour déplacer la statue fut si grande, que l'affrontement entre les russophones et les nationalistes estoniens ne pouvait être évité.
Le 27 avril 2007, plus connu sous le nom de la « Nuit de Bronze », un accrochage violent éclata entre les deux factions avec la police et la statue au milieu.
Les autorités sont intervenues rapidement pour déplacer la statue vers un lieu plus sur, dans le cimetière militaire, mais au lieu d'apaiser la tension, ce déplacement indigna fortement Moscou.
C'est la que le conflit bascula dans le cyberespace.
L'Estonie, pour sortir des marasmes du communisme, avait tout misée sur les nouvelles technologies et est devenu, avec la Corée du Sud, les deux pays les plus avant-gardistes en la matière.
Ainsi les citoyens estoniens peuvent créer des entreprises, payer leur impôts, élire leur députés, accéder a toute sorte de documents administratifs, payer leur parcmètre etc. en quelques clics seulement ce qui fait que leur pays est une cible parfaite pour une cyber attaque.

Le 1er mai, jour de la fête nationale russe, les serveurs hébergeant les sites web les plus utilisés en Estonie furent saturés de requêtes a tel point que certains d'entre eux se sont « crashés » et éteints.
D'autres furent inaccessible.
Les estoniens ne pouvaient plus accéder a leurs banques en lignes, ni aux sites d'informations, ni même aux services gouvernementaux, ce qui causa la panique parmi la population.
Dans les heures qui suivirent, la communauté russophone descendit dans la rue et provoqua de violents accrochages avec les forces de l'ordre. La distribution d'essence et de pain cessa et l'anarchie se répandit dans le pays. Sans ordinateurs, l'Etat cessa de fonctionner, ce qui augmenta la paranoïa de voir Moscou envoyer ses chars.
Ce qui paralysa l'Estonie était un DDOS, ou « attaque par déni de service distribué ».
En temps normal, un DDOS est considéré comme une nuisance mineure et non une arme majeure dans l'arsenal cybernétique.
Ce sont des requêtes préprogrammées chargé de saturer ou noyer des réseaux informatiques.
Il est distribué dans le sens ou des milliers, parfois même des centaines de milliers d'ordinateurs, sont engagés dans le processus de requêtes électroniques vers la cible désignée par les attaquants et cela a l'insu des propriétaires de ces ordinateurs.
Ces derniers sont appelés des « botnets », un réseau d'ordinateurs « zombies » qui sont télécommandés à distance. Ces derniers suivent les instructions qu'ils ont reçus de la part des serveurs « Control And Command » qui servent aux attaquants de centre de contrôle pour les ordinateurs qui sont sous leur domination.
Les seules indications qui permettent à une personne de savoir si son ordinateur est engagé dans une attaque DDOS sont que l'ordinateur devient un peu plus lent que d'habitude et que le temps de chargement des pages internet devient plus long. Votre ordinateur, maintenant, fait peut être parti d'un « botnet ».
Les moyens d'infections sont multiples, soit par une clé USB infectée, soit par la visite d'une page web qui semble a première vue parfaitement innocente mais qui installe secrètement des virus dans votre ordinateur ou en ouvrant un email contenant un fichier a télécharger et qui est infecté.
Un antivirus mis à jour peut détecter et bloquer le virus, mais les pirates découvrent sans cesse de nouveaux moyens de contourner les défenses.
Le DDOS qui frappa l'Estonie était le plus grand jamais vu. Plusieurs « botnets » différents, chacun composé de plusieurs milliers de machines infectées, se relayaient dans l'attaque. Au début, les autorités estonienne ont cru que ces attaques étaient le fait de certains russes outragés par la décision de déplacer la statue, mais quand les botnets ont commencés a cibler des adresses de serveurs inconnus du grand publique, tel que les serveurs régulant le réseau téléphonique, ceux des vérifications des transactions bancaires, ainsi que le directoire Internet,

ils ont enfin compris qu'ils avaient a faire a des gens qui ne pratiquaient pas le hacking que le dimanche.
Les autorités firent appelle aux experts de l'OTAN pour les aider à contrer les attaques, mais malgré cela, elles continuèrent de plus belle, enregistrant même un pic le 9 mai.
Utilisant les méthodes de traçage, les experts de l'OTAN ont réussi à intercepter les communications entre certains « zombies » et leur « maitres » et ils en ont conclu qu'elles convergeaient toutes vers la Russie. En parallèle, les programmeurs de l'OTAN disséquèrent le logiciel malveillant utilisé pour infecter certaines machines et ils découvrirent qu'il était écris en alphabet cyrillique.
Les autorités russes elles, se dont dédouanées et ont refusées la requête diplomatique de Tallin qui les invitaient a arrêter les attaquants, malgré une convention bilatérale entre les deux pays, en prétendant que ces attaques n'ont rien d'étatique et qu'elles ne sont que l'œuvre de hackers patriotiques avec lesquels elles n'ont aucun liens et qu'elles ne connaissent pas.
Mais tous les observateurs de la Russie savent bien que si les autorités russes le voulaient, elles auraient stoppés ces attaques, car la majorité des pirates russes, qui selon un sondage d'ABC, représentent 82% des meilleurs pirates du monde, sont tous au service du crime organisé, qui prospère en Russie grâce aux connections entre le Kremlin et la mafia russe.
Alors, est ce que le gouvernement russe a été derrière ces attaques ?
Peut être n'est ce pas la bonne question.
A-t-il suggéré, facilité, et refusé d'enquêté et punir les auteurs ?
Et finalement, qu'est ce que cela peux changer quand vous êtes un Estonien incapable de retirer votre argent d'un guichet bancaire ?

Russie Vs Géorgie

« *Aussi dur et tordu que le marteau et la faucille* »

La Géorgie avant 1917 faisait partie de l'Empire Russe.
Quand ce dernier commença a se désintégré sous les coups de la Révolution Russe, les géorgiens profitèrent du fait que les russes se battaient entre eux pour déclarer leur indépendance, mais elle fut de courte durée, car dès que les Soviets prirent le pouvoir, ils envoyèrent l'armée reprendre la Géorgie.
En 1991, l'Union Soviétique se désintégra et la Géorgie en profita a nouveau pour se déclarer indépendante, mais deux ans plu tard les populations russophone de l'Ossétie et de l'Abkhazie, soutenues par Moscou, défirent l'armée géorgienne et expulsèrent la majorité des géorgiens et se déclarèrent indépendantes a leur tour.
En juillet 2008, les rebelles ossétiens provoquèrent un conflit avec la Géorgie en lançant une série de raids sur des villages géorgien ce qui poussa l'armée géorgienne a riposté en bombardant la capitale de l'Ossétie et le 7 aout, elle envahi la région toute entière.
N'ayant pas été surpris par la réaction géorgienne, Moscou envoya le lendemain ses troupes a l'assaut des positions géorgiennes ce qui entraina une débâcle rapide de cette dernière.
Mais avant que les tanks russes ne fassent parler leur obus, les claviers, eux, avaient déjà commencés à faire parler les leurs.
Le 21 juillet 2008, le site web du président Mikhaïl Saakachvili fut frappé par une importante attaque DDOS, le rendant indisponible et quand il fut à nouveau en ligne, les pirates russes avaient remplacé ses photos par des effigies d'Adolf Hitler, ce qui obligea les autorités géorgienne à l'héberger sur la plateforme de blogs de Google.
Les pirates russes, pas découragés pour un sou, mirent en ligne plusieurs fausses répliques du site web et redirigèrent vers eux le trafic internet des gens voulant se connecter au site d'origine.
Mais les choses ne s'arrêtèrent pas la.
A l'inverse du précédent estonien, cette fois les pirates russes firent preuve de beaucoup plus d'organisation et de coordination.
Ainsi, le 9 aout, soit un jour après le début des frappes militaires, les hackers russes lancèrent le « StopGeorgia.ru », un forum ou une liste de 37 cibles géorgienne de valeur stratégique furent listé pour être prise d'assaut.

Et en plus de la liste des cibles, le forum fournissait également à ses membres les outils pour effectuer des attaques DDOS, et des tutoriaux pour apprendre à lancer des attaques plus sophistiquées telle que les injections SQL.
En parallèle, un canal IRC fut créer sur irc.dalnet.ru appelé #Stopgeorgia, pour coordonner les multiples « botnets » qui furent utilisés durant les attaques.
Sur ce forum, il y avait une hiérarchie très précise, dans laquelle les pirates les plus expérimentés se chargeaient de fournir le « matos »aux novices, mais aussi de chercher les vulnérabilités des sites web géorgiens à attaquer et prévenir les autres de leurs découvertes.
A ses débuts, le forum compté 70 membres, et a la date du 15 septembre 2008, ils étaient plus de 400 membres actifs.
Les administrateurs des forums XAKEP.ru (la Bible des hackers russophone) et StopGeorgia.ru surveillaient de très prés les visiteurs de leurs sites et gardaient un œil vigilant sur les publications postées dessus, ainsi des analystes du Projet Grey Goose, ont révélés des incidents qui démontrent bien que toutes les mesures furent a leurs summums, évitant ainsi de commettre les erreurs faites dans le cas estonien :
-un post sur Xakep.ru dirigé vers un sous-forum à accès protégé sur StopGeorgia.ru, appelé « Army ».Le lien fut directement supprimé par les administrateurs. Ensuite pendant une semaine, ces mêmes analystes parcoururent tous les sous-forums de xakep.ru a la recherche de posts semblables, et après ces tentatives infructueuses, toutes les adresses IP américaines furent bloqués et se virent refusé l'accès aux sites.
Du coté géorgien ,la réponse ne tarda pas non plus, les hackers géorgiens, aidés par des pirates du monde entier qui avaient une dent contre Moscou, s'organisèrent eux aussi dans des forums, et ils réussirent a prendre temporairement le contrôle de Stopgeorgia.ru,mais la dépendance infrastructures informatiques géorgienne a la Russie et la supériorité technique des pirates russes fit qu'ils ne résistèrent pas longtemps au assauts « rouges ».
La Géorgie est reliée a Internet a travers la Russie et la Turquie, et la majorité des routeurs qui dirigés le trafic vers la Géorgie furent assaillis par plusieurs attaques DDOS et les russes réussirent même à prendre le contrôle de plusieurs d'entre eux, rendant ainsi impossible aux géorgiens de pouvoir se connecter a n'importe qu'elle source d'informations étrangères (les sites de CNN et de la BBC furent bloqués), ni même pouvoir envoyer ou recevoir des emails en dehors du pays.
La Géorgie perdit le contrôle des noms de domaine finissant par .Ge et fut obligée de transférer plusieurs sites gouvernementaux sur des serveurs en dehors du pays.
Les russes se livrèrent aussi a une véritable guerre de l'information en envoyant une campagne de spam aux géorgiens, avec un email sois disant provenant de la BBC et qui affirmait que le président géorgien été un homosexuel avec une vidéo à télécharger et, en cliquant sur le lien, l'internaute géorgien se retrouvait a télécharger un virus « name.avi.exe » depuis l'adresse 79.135.167.49.

Ils mirent aussi en ligne plusieurs faux sites web d'informations, tel que http://www.os-inform.com pour induire en erreur la population.
Les géorgiens essayèrent de bloquer le trafic venant de Russie, mais les hackers à la solde de Moscou redirigèrent leurs attaques a partir de la Chine, du Canada, de la Turquie et, comble de l'ironie, de l'Estonie.
Les banques géorgiennes, marquées par le précédent estonien, décidèrent d'éteindre leurs serveurs, pensant qu'une perte temporaire de leurs services en ligne serait meilleur que de risquer des vols de données sensibles ou des dommages extrêmes de leur systèmes internes. Mais c'était choisir entre la peste et le choléra car les pirates russes, incapables d'attaquer directement le secteur bancaire géorgien, se tournèrent vers la communauté bancaire internationale, l'attaquant sous fausse bannière géorgienne, ce qui engendra la suspension des transactions bancaire entre la Géorgie et le reste du monde.
Les pirates russe enfoncèrent un clou de plus dans le cercueil géorgien en se prenant aussi aux réseaux de téléphonie mobile, et toutes ces attaques eurent un grand impact sur la Géorgie notamment sur le plan économique et social car l'économie géorgienne perdit plusieurs millions de dollars durant cette « CliczKrieg »(en référence la Blitzkrieg ou guerre éclaire lancé par Hitler contre l'Europe) ,et le montant des réparations et des nouveaux investissements pour renforcer le cyberespace se chiffrèrent aussi a plusieurs millions de dollars, mais le plus dangereux fut l'impact sur la société géorgienne ,qui fut pendant plusieurs jours déboussolée et plongée dans un état de panique permanent.
Malgré les fortes dénégations des officiels russes, il serait naïf de croire que des attaques de cette envergure, organisés de manière militaire et nécessitant de gros moyens financiers, puissent être l'œuvre de quelques hackers patriotique et isolés comme pour l'excuse avancée pour le cas estonien.
Les experts de l'Otan ont à nouveau réussi à tracer les communications entres les « zombies » et les « maitres » et les attaques DDOS émanaient de deux serveurs C&C (Control and Command), le premier, bizus-kohors.cc (207.10.234.244) et le deuxiéme, ns1.guagaga.net (79.135.167.22), des adresses appartenant au réseau turc systemnet.com.tr, classé au top 10 des pires spammeurs au monde. La Russian Business Network (que nous verrons dans un chapitre spécialement consacré à elle) est relié à ce réseau par des opérations de spam de produits pharmaceutique contrefaits et la RBN elle-même est relié à certains politiciens russes.
Toute activité cybernétique russe, quel soit gouvernementale, citoyenne, ou faites par des organisations criminelles, ne peut aboutir sans l'aval du FSB (ex KGB), tout puissant en Russie dont un ex-membre est actuellement le patron du Kremlin, Vladimir Poutine.
Les attaques russes contre l'Estonie et la Géorgie furent une « petite démonstration » de force, montrant une partie de ce que peuvent faire les agences de renseignement et l'appareil militaire russe en cas de conflits cybernétique.

Nul ne doute que les Russes ont gardés leurs meilleures armes pour d'autres jours, des jours ou ils seront en conflits directe avec les Etats-Unis et l'Otan.

Israël Vs Les hackers musulmans

« La version numérique du Djihad »

L'attaque de sites web israéliens est un sport populaire chez les hackers musulmans (et non arabo-musulmans car des pakistanais, des indonésiens, des malaisiens et des iraniens y participent).
Mais un autre tournant fut pris durant l'opération « Plomb Durci », menée par Tsahal (l'armée israélienne), pour forcer le Hamas à stopper les tirs de roquettes sur Israël.
Ainsi pour la première semaine de janvier 2009, le nombre de sites web israéliens ayant subit les foudres des hackers musulmans s'éleva a quelque 10000 sites web.
La plupart de ces attaques n'ont étés que simples « défacement », ou les pirates infiltrent le site web, et changent sa page principale en mettant a la place du contenu d'origine, des images contenant des messages de protestation contre Israël, mais aussi leurs pseudos et les noms de leurs groupes ainsi que leurs pays d'origine.
Si les médias se concentrèrent sur les cibles importantes ayant subit un piratage, cette cyber-guérilla visait aussi des milliers de sites web de TPE ainsi que des milliers de sites web personnels.
Cependant, compromettre des sites web de haute valeur stratégique tel que les partis politiques, les banques, les assurances, les compagnies de transports, les médias etc., n'attirent pas seulement l'attention du public, il force aussi ces même entreprises à dépenser plus d'argent pour sécuriser leur infrastructures informatiques, ce qui a un impact financiers important sur elles.
Parmi les cibles importantes frappées durant la cyber-offensive contre Israël, figurent entre autres, le site de Discount Bank, une des trois plus grande banques de l'Etat hébreu, la Israeli Cargo Airlines Ltd, une importante compagnie aérienne, le site de radio Tel-Aviv, le site du parti centriste Kadima, celui du ministre de la Défense, Ehud Barack et la banque Ha Poalim.
Nous allons prendre quelques instants pour faire connaissance avec les belligérants pour mieux assimiler le reste :

Team-Evil : ce groupe de pirates marocains s'est fait connaitre du grand publique en 2006,après avoir « défacés » plus de 800 sites web entre juin et novembre 2006 ,en guise de protestation contre l'offensive militaire israélienne au Sud-Liban. D'après les archives de Zone-H (un site

servant d'archiviste des exploits des pirates), Team-Evil serait derrière le « défacement » de 171 sites web de haute valeur.
Cette équipe c'est notamment fait remarquer par le degrés de technicité supérieur a celui des autres groupes de pirates impliqués dans ces attaques, a tel point que ,trois experts israéliens reconnu en matière de sécurité informatique,Kfir Damari ,Ami Chayun et Gadi Evron, ont dressé un rapport de 20 pages concernant la méthodologie de Team-Evil.
Ainsi, a titre d'exemple, lors de l'attaque de la Discount Bank, les hackers marocains ont infiltrés le bureau d'enregistrement de noms de domaines « DomainThenet », basé a New-York, ou est enregistré le nom de domaine de la banque, et ont orienté le trafic allant vers le site de la banque vers un autre site contenant des messages de protestation.

Cold Zero, Alias Rom Burner : jeune palestinien de 20 ans, arrêté par les autorités israélienne en janvier 2009 après avoir été piégé durant une opération mené par le Mossad. Il était membre de la Team Hell et avait gagné en notoriété après l'attaque du site web du Likoud, un grand parti politique israélien.

Team Hell : groupe de pirates saoudiens, dont les convictions sont quelque peu ambigües, car malgré l'attaque de plusieurs cibles israélienne, ils sont aussi derrière le « défacement » du site du groupe djihadiste palestinien « Al Nusra » (le même groupe qui s'active actuellement en Syrie contre le régime d'Al Assad) et sur certains sites, ils ont apportés leur soutien au parti de Mahmoud Abbas, le Fatah.

Agd-Scorp : groupe de pirates turcs, qui ont « défacés » des sites de l'Otan et du ministère de la Défense américain, en réponse a l'opération « Plomb Durci ».Ils se sont illustrés par une utilisation quasi-exclusive d'une seule forme d'attaque, l'injection SQL.
Ils sont aussi derrière le piratage des Nations-Unies, de l'université de Harvard, Microsoft, Shell et la NBA.

Jurm Team : groupe marocain, derrière les attaques des portails israéliens de KIA, Daihatsu, Fanta et Sprite.

Nous nous contenterons de ces groupes la, car la liste est encore longue, nous allons maintenant nous penchez sur les cyber-armes utilisées par ces différents groupes dans leurs attaques.
Tout d'abord, il y a l'incontournable DDOS. Pour cela ,les hackers musulmans ont utilisés la même méthodologie que leurs homologues russes, en créant plusieurs forums pour recruter des volontaires, et ils ont mis a leur disposition plusieurs outils d'attaques DDOS, dont l'un d'entre eux, Al-Durra (du nom de l'enfant palestinien tué par des tirs israélien), qui fut

développé en 2006 et dont la version amélioré disponible en téléchargement a été faite par Nimr Al Iraq, un hacker irakien tué en 2011 lors d'une explosion a Bagdad.
Les outils d'attaques DDOS, ne demandent pas de compétences spécifiques pour les utilisés, car il suffit a la recrue d'en télécharger un, de mettre le site web à attaquer et cliquer sur le bouton « Start », pour commencer un envoi continu de requêtes au serveur hébergeant la cible. Ainsi il suffit à une centaine de personnes disposant de bonnes connexions haut débit, d'utiliser tous en même temps l'outil pour venir à bout d'un serveur.
Viennent ensuite les « défacement » de sites web, qui eux, nécessite un degré supérieur de compétences, mais malgré cela, les « défacements » ne sont pas considérés comme des attaques sophistiquées. Dans ce type d'attaque, les hackers téléchargent des scanners de vulnérabilités (tel que SQL Poison ou Acunetix etc…..),disponible dans les forums spécialisés, mais aussi disponible nativement dans la « boites a outils » du pirate qu'est le système d'exploitation sous distribution Linux, Backtrack, largement utilisé par la communauté des hackers et des consultants en sécurité informatique.
Ainsi, ont met l'adresse du site visé et, le scanner se charge de détecter les vulnérabilités exploitables.
L'exploitation de ces dernières est relativement simple, il suffit de faire un tour sur des sites spécialisés tel que db-exploits.com pour télécharger « l'exploit » nécessaire, ou même utilisé un logiciel très connu dans la communauté des hackers, à savoir Havij, qui se charge automatiquement des injections SQL.
L'exploitation des vulnérabilités va de l'injection SQL au cross-scripting, plus connu sous le nom de XSS.
Par contre quand aux attaques utilisant des virus ou des trojans, une seule tentative a été enregistrée, grâce a une version modifiée du trojan Bifrost, qui a portée ses fruits en infectant une vingtaine d'ordinateurs israéliens.
Développer un trojan ou un virus capable de transpercer les multiples défenses israéliennes, nécessite une équipe de hackers de haut-vol, ainsi que beaucoup d'argent, c'est la raison pour laquelle ce type d'attaques ne fut pas utilisé par les équipes musulmanes impliquées dans ce conflit.
La réponse israélienne ne s'est pas fait longtemps attendre, car dès le début des attaques, le gouvernement israélien a mis en place un programme de recrutement d'activistes parlant d'autres langues que l'hébreu, avec la mission de « noyer » les forums de discussions et les blogs pro-palestiniens, de commentaires et d'opinions pro-israéliennes.
L'armée israélienne a aussi participée a ce cyber-conflit, en piratant les ondes de la chaine Al Aqsa, appartenant au Hamas, et aussi en piratant les pages de groupes Facebook pro-palestiniens, utilisant les méthodes de fausses pages de login, et le phishing (hameçonnage) par email, pour collecter les logins et mots de passe des membres de ces groupes.

Les activistes pro-israéliens ont aussi fait preuve d'ingéniosité, en développant un « botnet » volontaire.
Créer par un groupe de hackers connu sous le nom de « Help Israel Win », l'outil d'attaque DDOS lié a ce « botnet » fut baptisé « Patriot ».
Une fois installé et exécuté, « Patriot » ouvré une connexion avec le serveur C&C defenderhosting.com, mis à disposition par la société Virtacore, sise en Virginie au États-Unis.
Mais l'inverse des autres outils d'attaques DDOS, il ne disposait pas d'une interface utilisateur, permettant a ce dernier de choisir lui-même les sites à attaquer, mais le serveur C&C defenderhosting.com, le mettait a jour automatiquement avec les adresses IP des cibles visées.
Israël a aussi utilisé ses relais diplomatiques, pour forcer les compagnies hébergeuses des sites et forums de piratage pro-palestiniens à couper l'accès a ces derniers, ainsi par exemple, la Gaza Hackers Team a vu son site être mis hors-ligne suite aux pressions israéliennes.
Récemment aussi, nous avons assistez a des frictions entre les hackers musulmans et Israël dans le cyberespace, suite a la dernière offensive israélienne sur Gaza, provoqué par des tirs de missile Graad par le Hamas, qui conduisit Israël a coupé l'accès a Internet dans les territoires palestiniens et a mené contre eux des cyber-attaques massives.
Ainsi durant cette offensive, les hackers musulmans et d'autre sympathisants, groupés sous le label Anonymous, ont lancé l'opération #OpIsrael qui a aboutit a des perturbations majeurs dans les communications informatiques israéliennes, ainsi certains sites israéliens on été soumis a plus de 40 millions de requêtes par seconde.
La bataille durera longtemps entre les deux camps, et l'escalade de violence cybernétique ira crescendo, car les groupes de hackers iraniens, soutenus par leurs services secrets, ont lancés un véritable programme d'armements cybernétique pour contrer Israël.

USA+Israël Vs l'Iran

« *David et Zarathoustra se battent dans la 5eme dimension* »

Le cauchemar permanent des Etats-Unis et Israël et beaucoup d'autres pays de la région, est de voir l'Iran des ayatollahs possédé l'arme nucléaire. Non seulement cela bouleversera le rapport de forces dans la région la plus embrasées du monde, mais cela poussera aussi a une course effrénée a l'armement au Moyen-Orient et en Asie mineure.
Sans oublier que l'Iran a affirmé, a maintes reprises, son désir d'effacer Israël de la carte du monde, et qu'il a des vues belliqueuses sur plusieurs Etats de la région, alliés des Etats-Unis.
Mais depuis l'invasion de l'Afghanistan et de l'Irak par les troupes américaines et leur embourbement dans ces conflits, l'option militaire contre l'Iran, malgré le fait qu'elle soit toujours sur la table des dirigeants américains et israéliens, est pour le moment écartée, car même des frappes « chirurgicales » contre les installations nucléaires iraniennes risquent d'avoir des conséquences désastreuses ,car Tel-Aviv et plusieurs bases américaines dans la région, sont a portés des missiles iraniens, mais aussi un

conflit risquerait de déboucher sur une perturbation, voir même la fermeture du détroit de Hormuz, point de passage de 50 % du trafic pétrolier mondial ,ce qui aura des suites néfastes sur l'économie mondiale.
Alors pour contourner cela, dès 2006, l'administration Bush a mis en place, en collaboration avec le gouvernement israélien, une opération secrète, baptisée, « Olympic Games ».
Le but de cette opération, fut le développement d'un « beacon » (signal électronique), capable de tracer une carte des installations de la centrale nucléaire et collecter des informations sur la configuration des ordinateurs de cette dernière.
Sachant que les systèmes informatiques des sites nucléaires iraniens sont déconnectés d'Internet, l'introduction du « beacon », a du être faite par une clé USB infectée, introduite sur le site par un employé. Depuis longtemps, les scientifiques iraniens et autres responsables du programme nucléaire iranien, sont la cible d'attaques de « phishing » par emails, et l'infection de la clé USB a été le fruit de l'une de ces attaques.
Une fois les informations récupéré par le « beacon » , les équipes de la National Security Agency (NSA) , et celles de l'unité 8200, une unité de renseignement de Tsahal, responsable du renseignement électromagnétique et du déchiffrement de code, chapeauté a l'époque par le général Ravi Ashkenazi, ont commencés a développer un ver informatique spécialement adapté pour attaquer les systèmes d'exploitation Windows de Microsoft et SCADA (particulièrement Siemens Win CC) ,utilisé pour les commandes des processus industriels et qui est utilisé notamment par les centrales nucléaire.
Mis sur le terrain a la fin de l'année 2008, ce ver fut découvert par une société de sécurité informatique biélorusse, VirusBlockAda, en juin 2010 et c'est elle qui le baptisa « Stuxnet ».
Ce ver, est d'une grande complexité, car écrit dans plusieurs langages de programmation informatique différents, allant du C au PHP, chose inédite pour un virus.
Il a la particularité d'exploiter 4 failles dites « 0-Days », c'est-à-dire inconnu du public, et encore une fois, c'est du jamais vu pour un virus.
« Stuxnet » utilise aussi des certificats de sécurité numérique volés de Realtek et Jmicron, pour se faire passez pour un « agent » sur.
Rien que ces 3 détails nous font voir que ce virus ne peut être le fruit d'une bande de hackers sans soutien financier considérable, le coût de sa production est estimé, selon plusieurs experts qui se sont penchés sur son cas, à 50 millions de dollars.
Il a la capacité de se propager à grande vitesse a travers les ordinateurs du réseau, en utilisant d'autres failles et contourner les différents anti-virus et pare-feux et, il utilise les mots de passe par défaut pour faire des requêtes aux logiciels chargés de contrôler les centrifugeuses ,ce qui a pour effet, soit de ralentir, soit d'accélérer leurs vitesse ,dans le but ultime de les faire exploser a terme, sans que personne ne puisse s'en rendre compte, car sur les écrans de surveillances de la centrale, tous les voyants sont au vert.
Il communique aussi avec deux serveurs pour se mettre à jour et recevoir les ordres, le premier mypremierfutbol.com, basé au Danemark, le second, todaysfutbol.com, en Malaisie.
Il a aussi la capacité de se copier sur les disques amovible sans se faire détecter, mais c'est cette option qui lui fut fatale, car a force de se propager, il a fini par infecter plusieurs ordinateurs, dans plusieurs pays, n'ayant rien à voir avec le programme nucléaire iranien et, il a fini par être détecté.

Mais « Stuxnet » n'était que l'arbre qui cachait la foret, car en parallèle, deux autres vers informatique furent mis en selle, « Flame » et « Duqu », découverts respectivement en mai 2011 par KasperskyLab et en septembre 2011 par le Laboratoire de Cryptographie et de Sécurité (CrysysLab) de l'Université de Budapest.
Mais à l'inverse de « Stuxnet », ces deux programmes ont été conçus pour collecter des informations sensibles, mais aussi pour voler des certificats de confiance numérique, pour permettre le développement de futurs virus.
Ainsi « Flame » ne visait qu'un panel réduit d'ordinateurs, appartenant à des personnes impliquées dans le programme nucléaire iranien.
Il avait pour mission l'interception d'emails, l'enregistrement des conversations audio sur Skype et MSN et le vol de données PDF ou Office.
Il disposait aussi d'une connexion à un serveur pour être mise a jour et pour envoyer dessus les fichiers volés.
« Duqu » lui aussi est de la même essence que « Flame », mais a l'inverse de ce dernier, il se concentré surtout sur les informations liées aux systèmes de contrôle industriel et il fut programmé pour se désinstaller automatiquement après 36 jours, limitant ainsi les chances d'être détecté.
Après que la découverte de « Stuxnet » fut rendu publique et reprise par presque tous les médias, les autorités iraniennes ont d'abord niées, avant de se rétracter et d'avouer avoir détectées le ver et réussies à le contenir.
D'après différents rapports de plusieurs agences de renseignements, il semblerait que 1000 centrifugeuses, sur les 5000 en activités, dans la centrale nucléaire de Bouchehr aient été temporairement mises à l'arrêt grâce a l'action de « Stuxnet », ce qui est une réussite pour ses concepteurs.
Après que Kaspersky ait annoncé que « Flame » avait pénétré dans les ordinateurs de hauts officiels iraniens, une organisation de cyber défense iranienne le confirma le 28 mai 2012.
La dernière attaque connue contre des intérêts iraniens remonte au mois d'aout 2012,quand un virus du nom de « Wiper » ,20 fois plus grand que « Stuxnet », a copier puis effacer le contenu des disques dur du Ministère du Pétrole iranien et de la Compagnie Pétrolière iranienne ,ce qui les a forcés a débrancher leurs ordinateurs d'Internet.
Mais l'Iran est loin d'être un adversaire faible dans le cyberespace .
Le groupe de hackers iraniens Ashianeh Security Group, proche des services secret iranien ,est très actif dans l'espace numérique depuis 2006.
Ils ont attaqués a plusieurs reprises les sites du Ministère de la Défense israélien,ceux du Mossad et plusieurs autres sites stratégiques israéliens.
Par ailleurs les hackers iraniens ont réussi a prendre le contrôle d'un drone américain et l'ont fait atterir en Iran, et après une opération d'ingénieurie inverse ,les ingénieurs iraniens ont réussis a construire leurs propre drone ,qui a été utilisé par le Hezbollah pour espionner des installations israéliennes.
Mais les iraniens,au lieu de développer leurs propres armes cybernétique ,ce qui a un coût très elevé , et nécéssite des moyens humains considérable,non pas en nombre mais en degrés de compétence,font plutôt appel a l'ingénieurie inverse, en étudiant les codes sources des virus dont ils sont victimes et les modifient et améliorent ,pour les redirigés vers leurs créateurs d'origine ou vers d'autres ennemis de

l’Iran.Ainsi,une version sophistiquée de « Wiper » a été utilisée par eux pour causer les mêmes dégats dont ils furent victime , a l’Arabie Saoudite.
L’avenir nous réserve encore beaucoup de surprises,car les bélligérants impliqués dans ce conflit ne sont pas du genre a tendre la joue.

La Corée du Nord

« *Tous les Kim doivent mourir !*»

« Shot and talk after », est une vieille devise des cow-boys du Far-West, que les nord-coréens ont repris a leur depuis l'avènement de leurs régime en 1951.
Le 3 juillet 2009, veille de la fête de L'Indépendance américaine, un message fut envoyé par un agent nord-coréen à un « botnet » de 40000 ordinateurs, leur intimant l'ordre d'envoyer des requêtes continues à une liste de sites web des gouvernements américain et sud-coréen.
Un autre DDOS.
Ainsi, durant les heures qui suivirent, le gouvernement américain remarqua que les noms de domaine dhs.gov (Département de la Sécurité Intérieur), et state.gov sont devenus inaccessible.
Les sites web gouvernementaux furent frappés par une vague atteignant un pic d'un million de requêtes par seconde, rendant les serveurs complètement fous.
Durant la période s'étalant du 4 juillet au 9 juillet, les serveurs hébergeant les sites web du Trésor, du Secret Service, de la Commission Fédérale du Commerce et le Département des Transports furent tous submergés.
Suivirent ceux du Nasdaq, du NYSE (Bourse de New-York) et du Washington Post.
Par contre le site web de la Maison Blanche résista aux assauts car, en 1999, quand pour la première fois une attaque DDOS visa la Maison Blanche(les chinois en étaient les instigateurs, en réponse au bombardement américain de leurs ambassade a Belgrade durant la Guerre des Balkans),les experts avaient fait appel aux services de la société Akamai (société spécialisée dans la mise en cache de contenu web, qui permet de répartir les sites web sur plusieurs serveurs a travers le monde, permettant ainsi d'économiser le débit Internet , et utilisées par plusieurs sociétés informatiques tel que Facebook, Microsoft, Apple…) pour répartir le site web de la Maison Blanche sur 20000 serveurs a travers le monde, ce qui eut pour effet que seuls les « miroirs » du site web en Asie furent touchés.
La deuxième vague de DDOS utilisa plus de 60000 « zombies », visant cette fois, une vingtaine de sites gouvernementaux, de banques et de compagnies informatiques sud-coréennes car les américains réussirent à la bloquer.
La troisième et dernière vague fut encore plus violente, car cette fois ce sont plus de 160000 « zombies » de 74 pays qui submergèrent de requêtes les serveurs sud-coréens.
Les serveurs C&C utilisés pour contrôler cette armée de « zombies » furent au nombre de 8, situés en Corée du Sud, aux Etats-Unis, en Allemagne, en Autriche et, bizarrement, en Géorgie. Une société

vietnamienne spécialisée en sécurité informatique, la BKIS, conclue dans son rapport sur ses attaques, que ces 8 C&C étaient eux mêmes contrôlés par un autre serveur situé à Brighton en Grande-Bretagne.
Une guerre mondiale.
Mais le plus surprenant dans cette histoire est que ces attaques furent lancées par la Corée du Nord, un Etat réputé pour être un « Afghanistan numérique » tellement le manque d'infrastructures informatiques dans le pays est criant.
Seuls 20000 sur 23 millions de citoyens nord-coréens ont un téléphone portable, les radios et télévisions sont reliées physiquement aux canaux gouvernementaux et, les quelques sites web du gouvernement ne sont en place que pour communiquer la propagande du régime au reste du monde et, seuls quelques privilégiés du régime peuvent se connecter au réseau intranet, seulement pour accéder au site web du Leader Bien Aimé et nul par ailleurs.
Alors la question qui se pose maintenant est la suivante :
Comment un Etat aussi coupé du monde virtuel que du monde réel, peut-il enclencher des attaques d'une telle envergure ?
La réponse est simple.
Au lieu d'investir dans les infrastructures informatiques de son pays, Kim Jong-Il a choisit la solution inverse, investir pour développer des solutions nuisibles aux autres.

Ainsi ,l'Unité 110,suspectée d'être derrière ces attaques, fait partie des quatre branches formées pour doter la Corée du Nord de capacités cybernétique offensives car, défensivement parlant ,la Corée du Nord n'a rien a défendre étant donné l'absence de cyberespace dans le pays.
Les trois autres branches sont, l'Unité 121, regroupant plus de 600 hackers, l'Unité 204 avec plus de 100 et enfin l'Unité 35, ayant dans ses rangs une cinquantaine d'autres.
Toutes ces unités sont stationnées en Chine a cause du manque de débit Internet en Corée du Nord mais aussi car ils seraient facilement identifiables si elles menaient leurs opérations a partir de la et certains vont même jusqu'à dire que la Chine, alliée de longue date de Pyongyang et reconnue mondialement dans le domaine de la cyber guerre, forme ces hackers pour livrer des guerres par procuration.
Ces attaques, bien que non dévastatrices, furent très sophistiquées et leurs préparatifs durèrent plusieurs mois, allant de la recherche de failles exploitables et inconnues ,jusqu'à l'écriture du virus et sa propagation pour « recruter » l'armée de « zombies » , et les experts, en étudiant le code source du virus utilisé ,trouvèrent qu'une grande partie de ce dernier était écrite en utilisant un navigateur web en langue coréenne ,ce qui les intrigua fortement ,car comment quelqu'un qui peut produire une arme pareil ne se donne même pas la peine de « maquiller » le code et effacer les traces ?
Pour la simple raison que celui qui a écrit ce code voulait qu'elles soient découvertes.
Ainsi, la Corée du Nord, voulait montrer de manière claire et évidente qu'il faudra désormais avoir peur d'elle, non seulement nucléairement mais aussi cybernétiquement, et a l'heure ou sont écrite ces lignes, une nouvelle attaque nord-coréenne paralysa pendant deux jours les télévisions et banques sud-coréennes.
Kim est mort, mais il a laissé un héritier digne de lui.

Inde Vs Pakistan

« Shiva veut une robe en cachemire »

Le conflit opposant l'Inde au Pakistan est un conflit tumultueux, ancien et d'une grande complexité.
Lors de l'Indépendance, les Etats princiers placés sous mandat britannique ont eux le choix de rejoindre l'un des deux Etats nouvellement crées, ainsi ceux a majorité musulmane ont rejoints le Pakistan et ceux a majorité hindoue, l'Inde.
Mais parmi ces Etats, ce trouve le Cachemire, qui constitue un cas particulièrement ambigüe.
A majorité musulmane, il était gouverné par le maradjah Hari Singh, qui était de confession hindoue. Le prince hésita longtemps à rejoindre l'un des deux camps jusqu'à ce qu'il fut victime d'assauts de tribus pakistanaises et auxquelles se rallièrent une grande partie de la population locale.
Pour faire face à ces attaques, il demanda à ce que le Cachemire soit rattaché à l'Inde et dès lors, l'armée indienne intervint et s'est retrouvée en conflit directe avec l'armée pakistanaise venue au secours des populations musulmanes en 1948.
L'ONU s'interposa et négocia un cessez-le-feu qui entra en vigueur le 1er janvier 1949, mais en 1965, la question du Cachemire conduisit à nouveau les deux Etats à s'affronter, mais le Pakistan en sortit perdant.
Depuis, les armées des deux puissances nucléaires sont stationnées le long de la ligne de contrôle, divisant le Cachemire en deux et se regardent en chiens de faïence, avec a la clef, quelques échauffourées de temps a autre.
Mais depuis les années 2000, les claviers prirent la place des fusils d'assaut et les cyber-combattants celle des soldats et, se livrent une guerre sans merci dans la 5eme dimension.

Les belligérants :
La PAK Cyber Army (PCA)
La PCA est une organisation informelle a vocation ultranationaliste et djihadiste , dont les membres, divisés en plusieurs groupes, sont estimés a plus d'un millier.Parmis les plus connus, grâce a leurs faits d'armes, se trouvent : CyberRocker, XXX-Death-XXX, No Swear, M4STERMIND , Shak et la Team Poison.
Shak ,de son vrai nom , Bilal Yaqoob , est un jeune étudiant de l'Université du Penjab , originaire de Karachi, et dont le numéro de compte bancaire, celui de sa carte d'identité ainsi que celui de son téléphone mobile furent rendu publique après que , Lucky Leader et Indishell (tous deux indiens) , réussirent l'exploit de prendre le contrôle pendant quelques heures du site de la PCA

(www.cyberarmy.com.pk) .Bilal Yaqoob en était l'administrateur et il s'illustra auparavant en piratant avec succès plusieurs centaines de sites indiens , parmi lesquels ceux de plusieurs sociétés opérantes dans les nouvelles technologies tel HircoFirewall, TechLink et Cambridge Network.
Team Poison quant a eux, sont un groupe de 8 pirates âgés de 15 a 22 ans, et sont connus pour être parmi les plus actifs dans le collectif international de hackers, Anonymous. Ils ont à leurs actifs le piratage du blog de RIM Blackberry, le site de Tony Blair, celui de Sarah Palin mais aussi le vol d'une base de données contenant plusieurs milliers de logins et de mots de passe et appartenant au Nation-Unies.La Team Poison est aussi derrière la révélation d'une faille SQL sur les serveurs de la NASA.
Suite a des divergences avec les Anonymous et Lulzsec, mais aussi a cause des pressions de la CIA sur l'ISI (services secrets pakistanais qui protègent les hackers du pays), ils ont piratés et fait fuiter sur Internet plusieurs détails personnels de certains membres d'Anonymous et Lulzsec qui ont conduit a l'arrestation de ces derniers et parmi eux, Xavier Hector Montsegur, le ''cerveau '' de Lulzsec.
Deux de ses membres, non résidants au Pakistan, ont été arrêtés suite à une opération lancée par Scotland Yard, après avoir été victime d'un bombardement d'appels téléphoniques sur sa « hot-line ».

Durant les six dernières années, la PCA s'est illustrée par des attaques très sophistiquées, ce qui montre que certains de ses membres sont particulièrement doués et expérimentés.
Ils ont a leurs actifs plus de 28000 sites indiens « défacés » ou dont les bases de données furent volées, parmi lesquels, l'ambassade indienne de Suéde, des organismes gouvernementaux tel que le Central Bureau Of Investigation (l'équivalent indien du FBI), le parlement indien, celui du Police Research and Developpement, les sites de plusieurs ministères et aussi des médias tel que la chaine de télé Chanset et celui d'un des quotidiens les plus lus en Inde, le Hindu Times , ou ils firent une blague de très mauvais gout en annonçant la mort de Shah Rukh Khan.
Certains groupes de la PCA sont aussi très actifs dans le conflit israélo-palestinien, ainsi la Mujahideen Hacking Unit est derrière le « défacement » de plusieurs sites web d'entreprises israéliennes , mais leur fait d'arme le plus notoire est , la pénétration du site de l'English Defence League, un mouvement d'extrême-droite qui lutte contre l'islamisation de l'Angleterre et dont la base de données contenant les noms, adresses et numéros de téléphones de ses membres ,fut mise sur Internet après cet exploit.

L'Indian Cyber Army (ICA) :
L'ICA (www.cyberarmy.in), est l'alter-ego indien de la PCA, qui est aussi composée de plusieurs groupes indépendants les uns des autres, mais tous unis quand il s'agit de l'ennemi pakistanais.
Ne partageant pas le même degré d'ultranationalisme animant leurs homologues de la PCA, ils sont au total plus d'un millier eux aussi, coordonnés par Mohit Kumar, un jeune indien de New-Delhi, plus connu sous son pseudo TheEvilzHacker, et rédacteur en chef du web magasine Thehackernews.
Plusieurs membres et groupes de l'ICA sont impliqués dans des opérations menés par Anonymous, mais aussi contre le Bangladesh et la Chine, vieux ennemis de l'Inde.
Comme les pakistanais, les indiens ont a leurs actifs plus de 20000 exploits, parmi eux des sites gouvernementaux, des ministères, la Cour Suprême du Pakistan, la Marine Pakistanaise, le plus grand site d'informations pakistanais Dawn.com (qui fut piraté par Luckyleader, le même qui a révélé l'identité de Shak) ,celui de la défunte Benazir Bhutto mais aussi le fameux portail de téléchargements Songs.pk ,

qui fait perdre des millions de dollars a l'industrie cinématographique et musicale indienne, mais qui a été aussitôt remis sur pied, car la cyber guerre est aussi économique.
Mais cependant, et a l'inverse des pakistanais, les hackers indiens ont tendance à injecter des codes malicieux dans les pages des sites qu'ils attaquent, alimentant ainsi leurs réseaux de « botnets » avec des « zombies » pakistanais, qu'ils utilisent ensuite pour attaquer d'autres pays, faisant ainsi passer les attaques comme venant du Pakistan (False Flag Attack ou attaque sous fausse bannière).

A chaque fois qu'une attaque est révélée, les officiels pakistanais et indiens se renvoient les accusations, mais les deux pays ne s'arrêtent pas la, ainsi l'armée pakistanaise a décidée de créer une école spécialisée dans la cyber guerre, en partenariat avec la NUST School Of Electronical Engineering and Computer Science, en 2012.L'armée prendra en charge les frais de scolarité des étudiants, qui une fois diplômés au bout d'une cursus de 4 ans, deviendront des officiers de l'armée chargés de la défense du cyberespace pakistanais pour les 7 années suivantes. Cette école acceptera 30 élèves par ans, triés selon leurs notes au baccalauréat.
De son coté, le gouvernement indien à créer la « National Security Database », une base de données répertoriant tous les pirates et programmeurs qui peuvent protéger le cyberespace indien en cas d'attaque majeur. Cette base de données fut secrètement préparée après les attaques terroristes de Mumbay, et tous ces figurants furent soumis à des épreuves servant à valider leurs compétences. Par ailleurs, le gouvernement indien a aussi lancé un programme de formation de ses officiels, chapeauté par les hackers argentins Chris Russo et Fernando Vicarel, qui sont derrière le piratage du CERN.
L'Inde et le Pakistan ont encore de beaux jours devant eux pour montrer à la face du monde comment ils peuvent se déchirer entre eux par claviers interposés.

La Chine

« *Le souffle du Dragon* »

La Chine fascine, la Chine fait peur.
Pays le plus peuplé du monde -1.3 milliards d'habitants – superpuissance économique par excellence du 21eme siècle, la Chine c'est aussi 500 millions d'internautes dont plus de 400 millions de microblogeurs .Des chiffres a donnés le vertige a n'importe quel fournisseurs d'accès Internet.
Mais la Chine est aussi la puissance la plus dangereuse du cyberespace.
Du virus CodRed en 2001 , en passant par les attaques répétées contre Google ,jusqu'à la plus vaste opérations de cyber-espionnage jamais réalisée , la Chine a depuis 14 ans donnée des sueurs froides a tous les gouvernements et agences de renseignements de la planète.
La Chine a compris depuis la fin des années 90 que pour s'affirmer en tant que superpuissance, il lui fallait disposer d'une économie forte couplée à un appareil militaire dissuasif.
Ne se contentant pas d'être « l'atelier du Monde », elle a fait le choix de développer ses propres champions industriels nationaux et les envoyer a la conquête du monde.
Mais sachant qu'il y a un grand gap technologique entre ses entreprises et les mastodontes européens et américains, elle a pris le chemin le plus court pour le combler : le cyber-espionnage.
A partir de 2007, la Chine lança ses cyber-espions a la conquête des secrets industriels et des gouvernements de plus de 30 pays, ciblant surtout les Etats-Unis , pillant ainsi pendant plusieurs années les données sensibles de plusieurs acteurs industriels majeurs , tel que Lockheed Martin , Northrop Grumann ou L-3 Communication, des médias tel que le New-York Times et même le Nasdaq.
Mais si la Chine a réussie ces exploits, sans attirer l'attention, c'est surtout grâce a deux de ses constructeurs d'équipements de télécommunications, a savoir ZTE et Huawei.
Pratiquant un système commercial basé sur le low-cost, ces deux équipementiers ont connus une croissance fulgurante durant les dernières années et sont devenus les équipementiers de référence de nombre de gouvernements et de géants industriels.
Mais qui dit équipements, dit possibilité de laisser dans ces mêmes équipements des portes dérobées, permettant à leurs fabricants de « monitorer » ce qui passe par eux.
Et comme ZTE et Huawei sont très étroitement liés au complexe militaire chinois et qu'ils œuvrent dans une opacité total, le pas est vite franchi.
Mais la Chine n'en reste pas la.
Sentant le vent tourné des le début des années 2000 et comprenant que désormais les guerres seraient numériques, la Chine a beaucoup investis dans ses honkers (hackers rouge), pour développer des «cyber-armes » capable de changer a elles seules le cours d'une bataille.

Plusieurs agences de renseignements, grâce a un travail de longue haleine, ont réussi a localiser l'Unité 61398, cyber-cellule secrète de l'armée chinoise, ayant son quartier général dans un immeuble de 12 étages d'apparence anodine, dans le quartier de Pu Dông a Shanghai, mais ou s'activent chaque jour plus de 3000 cyber-combattants talentueux , développant chaque jour de nouveaux virus et bombardant toutes les entreprises visées par la Chine ,d'emails libérant des logiciels malveillants au moindre clic.
Le Dragon n'a pas encore fini de bruler tout sur son passage.

Les marchands de canons

« Le cri de détresse de la Kalachnikov »

Qui dit guerres dit armes, et dans les nouvelles guerres, le virus, la bombe logique et l'attaque DDOS vont prochainement reléguer la Kalachnikov, les F-18 et les Tomahawk au rang de simples figurants.
Le business des armes est un des seuls qui ne chôme jamais, car depuis que l'Homme est sur Terre, il n'a cessé de payer pour tuer ou éviter de l'être.
Mais depuis quelques années, la crise a débarquée et de nombreux Etats ont resserrés les cordons des bourses de leurs budgets d'armements.
Mais si les vieux marchands de poudre (Dassault, Boeing…) ont vus leur bénéfices s'effondrer, d'autres, nouveaux, voient les leurs progresser d'années en années et a l'inverse de leurs ainés ,les armes qu'ils vendent n'ont besoin ni de cartouches , ni de détonateurs , seulement d'un clavier et d'une souris et peuvent faire des ravages pire que ceux produit par les tanks ,et ,avantage majeur, elles sont beaucoup, beaucoup, moins chères.
Ce sont les marchands de canons « numériques ».
Beaucoup d'entre eux ont défrayés la chronique ces dernières années à cause des scandales provoqués par leurs produits.
Ainsi, Amesys, filiale du groupe français Bull, vendit son système Eagle, qui permet l'interception de toute sortes de communications Internet, pour la modique somme de 26 millions d'euros a un terroriste, Abdellah Senoussi,ex-premier flic de Libye, qui s'en servit pour rafler a tour de bras les opposants du régime. Amesys vendit ce système à plusieurs autres dictatures de la région aidant ainsi les tyrans à isoler et traquer les dissidents et les militants de la démocratie.
La société anglo-allemande , Gamma Technologie, elle , a fait mieux qu'Amesys en allant vendre a ces même tyrans un système répondant au doux nom de Finfisher (avec pour logo un requin) , qui permet de traquer tous les types de smartphones , en extraire les données, le géolocaliser ,contribuant ainsi a « monitorer » les populations des pays auxquels elle la vendue.
Plus grave encore , la société américaine Raytheon , commercialisera prochainement un moteur de recherche baptisé RIOT, permettant de trouver toutes sortes de renseignements disponibles sur Internet sur une personne (Facebook , Twitter, LinkedIn…)et allant même jusqu'à prédire les prochains faits et gestes de la personne en question, selon ce qu'elle a laissée comme traces sur Internet.
La société israélienne Applicure, elle, dama le pion au cybercriminelles, en permettant de louer en toute légalité des « botnets » pour lancer des attaques DDOS.

Et la liste est encore longue….
Le marché des « armes numériques » était quasiment inexistant au début des années 2000, et aujourd'hui il représente un chiffre d'affaires de 5 milliards de dollars et en 2018, ce marché avoisinera les 50 milliards de dollars.
A l'instar des marchands de poudre traditionnels, la majeure partie de ces sociétés sont situées en Europe ou aux Etats-Unis, ainsi sur 124 marchands de « canons a 0 et 1 » ,32 sont situés au USA, 17 en Angleterre, 15 en Allemagne, 8 en France, 7 en Italie et 10 en Israël.
Mais dans les pays occidentaux , la commercialisation interne et l'utilisation des systèmes de surveillances et d'interceptions des télécommunication est strictement encadré par tout un arsenal juridique ,mais ,cependant , rien n'interdit de les vendre a des pays beaucoup moins regardant sur les questions des Droits de L'Homme , car si selon les brochures commerciales ,ces « armes » sont destinées a combattre le terrorisme , traquer les pédophiles et les criminels il n'empêche qu'a plusieurs reprises ces armes ont été vendues a des pays soutenant le terrorisme ou opprimant leurs populations avec.
Entre un chasseur bombardier a 300 millions de dollars qui peux être abattu, un missile Cruise a 600000 dollars qui peux rater sa cible et un virus a 100000 dollars qui peux détruire toute l'infrastructure d'un pays, le choix est vite fait.
Le marché des « armes numériques » a encore de beaux jours devant lui.
Mikhaïl Kalachnikov regrette surement de ne pas être mort avant de voir son arme éponyme rangée au musée militaire.

Qu’est ce que le Cyberespace ?

Selon les scientifiques, le cyberespace est un « espace autre ».
Selon les militaires, il est, après la terre, la mer, l’air et l’espace, la cinquième dimension de combats.
Selon les acteurs économiques, il est le « marché de l’avenir ».
Pour les géographes, il est le « 9eme continent ».
Pour les politiques, c’est un terrain de chasse aux voix.
Pour l’internaute lambda, c’est sa « deuxième vie » qui parfois, prend le dessus sur la première.
Mais qu’est ce qu’il est vraiment ?
Le cyberespace est un ensemble hybride composé de plusieurs éléments sans lesquels il n’est rien.
Il repose sur un ensemble physique (ordinateurs, téléphones, câbles, routeurs…) et sur un autre virtuel (logiciels, sites, ondes, applications…).L’un ne saurait exister sans l’autre.
Mais pourquoi est-il si important ?
Son importance réside dans la rapidité, la disponibilité, l’absence de frontières et le coût financier qu’il représente.
Le cyberespace ne saurait être cantonné à Internet, qui est le réseau permettant l’accès aux autres réseaux ouverts.
Il est aussi composé de plusieurs autres réseaux, qui eux, ne sont pas « ouverts » sur Internet, comme ceux sur lesquels transitent les transactions bancaires et financières, les réseaux de communications militaires, ceux servant a la communication interne des entreprises. Il est aussi composé des réseaux de télésurveillance et acquisition de données (SCADA) qui permettent aux machines de se « parler » entre elles comme les pompes, les réacteurs, les trains, les avions etc.
En somme, le cyberespace est composé actuellement de plus de 2 milliards d’ordinateurs plus une quantité astronomique de serveurs, routeurs, switches et autres composants électroniques.
Mais la principale caractéristique du cyberespace est qu’à l’inverse des océans, de la terre, de l’air et de l’espace, il a besoin de l’Homme pour exister.
L’Homme fabrique ces composants, il les programme et l’Homme leur permet de « vivre ou mourir ».

La Cyber-force :

Depuis la nuit des temps, les humains se sont combattus entre eux, que ce soit pour le feu, pour le bétail, l’or, la terre, et ils se sont d’abord affrontés sur la terre ferme.
Du poignard a la lance, du bouclier à la catapulte, les humains n’ont cessez d’inventer de nouveaux moyens pour verser le sang et s’accaparer les richesses des autres.
Vint ensuite le temps des Empires, ou la mer est devenue leurs deuxième champs de bataille pour la domination.
Ainsi depuis la victoire des Hittites sur les Chypriotes en 1210 AV J-C jusqu'à la guerre en Ossétie du Sud, ils ont pensés, inventés, et modifiés de nouveaux navires dotés d’armes toujours plus puissantes pour leurs permettre de maintenir leurs supériorité et de conquérir de nouveaux territoires.

Quand les frères Wright ont réussis leurs premier vol en avion, les militaires n'hésitèrent pas à voir en cela de la futur de la guerre et ainsi depuis que l'Aviatike du lieutenant allemand Von Zangen fut abattu par le Voisin III du sergent Frantz et qui constitua le premier combat aérien, jusqu'aux chasseurs supersoniques et furtifs de nos jours, l'air est devenu leurs troisième champs de bataille.
Vint ensuite le temps de la « guerre des Etoiles » et sont lot de fusées, de missiles intercontinentaux et de satellites espions et l'espace fut a son tour dompté pour servir les desseins impérialistes de la nature humaine.
Aujourd'hui, plus que jamais auparavant, les Etats et tous leurs composants, qu'ils soient politiques, économiques, sociaux ou militaires se sont vu intégrés dans le cyberespace, un espace inventé par les hommes, pour les hommes, où les armes sont « silencieuses » et les guerres « tranquilles » mais ou les victimes peuvent désormais se compter en millions et cela grâce a un simple « clic ».
La course à la cyber-force est lancée !

Le Cyber-pouvoir :

Francis Bacon disait que « en effet, le savoir lui-même est un pouvoir », et le pouvoir basé sur l'information et ses multiples sources n'est pas nouveau. Dans le cyberespace cela a pour nom la « cyber-force ».
Alors que le cyberespace est la « plateforme » ou les cyber-opérations se déroulent, la « cyber-force » est le résultat des effets stratégiques générés par les cyber-opérations dans et a partir du cyberespace.
Son objectif stratégique s'articule autour de la capacité , en temps de paix ou de guerre, de pouvoir manipuler les perceptions de cet environnement (le cyberespace) a son avantage et en même temps ,dégrader la capacité d'assimiler ce même environnement chez l'adversaire.
La cyber-force est essentiellement l'habilité à contrôler les systèmes et réseaux informatiques à l'intérieur et a travers le cyberespace.
Elle est le résultat de l'utilisation, ou de la menace d'utilisation des capacités destructives des cyber-attaques par un Etat.
Le pouvoir dépend de plusieurs facteurs et instruments, et le cyber-pouvoir est la pour créer des synergies entre ces multiples éléments et les relier de manière a amélioré leurs assemblage.
Le cyber-pouvoir, lui aussi, est façonné par plusieurs facteurs, parmi eux, la technologie, car c'est son utilisation qui permet de pénétrer le cyberespace, par conséquent, elle sert de mesure de la capacité d'un Etat à utiliser cet environnement (le cyberespace).
Plus un Etat est avancé technologiquement, plus cette capacité est grande, mais paradoxalement, plus il est avancé et plus il est vulnérable.
Le cyberespace et le cyber-pouvoir sont des dimensions ou s'exerce a la perfection l'instrument que procure le pouvoir de l'information et ils existent une multitude de liens et de manières dont le cyber-pouvoir permet l'exercice des autres instruments de pouvoir.
L'information est ainsi le nerf du cyber-pouvoir.
Le cyberespace a transformé la façon dont l'information est créée : il est devenu le carburant alimentant les économies et les sociétés humaines.

De nouvelles formes de contenu –images, sons, informations et données sous des formes multiples – et les connectivités utilisées pour transmettre et échanger ces contenus, ont métamorphosés la manière dont les influences peuvent être exercées.
Le cyber-pouvoir a exercé des impacts significatifs et de plus en plus répandus sur toutes les sociétés au cours de ces deux dernières décennies et les Etats sont maintenant dans l'obligation de s'adapter à ces impacts par de nouveaux moyens car leur survie en dépend.
Les impacts les plus importants et transformateurs que le cyberespace et le cyber-pouvoir ont eux sur les sociétés sont dans les nouveaux moyens qu'ils ont crées pour relier les peuples et les organisations, façonnant ainsi un monde de plus en plus branché ou les frontières traditionnelles sont sans cesse rognées, permettant ainsi de nouvelles interactions entre les gens et les gouvernements a travers la planète.

La Cyber-guerre :

Militairement parlant, la cyber-guerre a été l'instrument le plus influent de ces 20 dernières années. Le cyberespace et le cyber-pouvoir sont devenus le noyau dur des nouvelles doctrines de la guerre.
Le cyber-pouvoir est devenu un élément incontournable des technologies militaires modernes.
Comme le cyberespace, la cyber-guerre n'a pas de définition acceptée à l'unanimité. Selon l'une d'entre elles, la « cyber-guerre se réfère généralement a un assaut numérique, massif et coordonné, fait par un gouvernement contre un autre. C'est l'action résultante de la pénétration par un Etat, des ordinateurs et réseaux d'un autre Etat, dans le but de causer des dommages ou des perturbations ».
Mais la cyber-guerre peut être aussi utilisée pour décrire les attaques livrées par des entreprises entre elles, par des organisations terroristes ou simplement des attaques lancées par des pirates contre d'autres pirates.
Le succès d'une cyber-guerre dépend de deux choses : les moyens et la vulnérabilité.
Les « moyens », sont les personnes, les outils et les armes cybernétique de l'attaquant.
La vulnérabilité, est la mesure dans laquelle l'économie et les infrastructures civiles et militaires, sont dépendantes d'Internet et des réseaux informatiques en général.
Un nombre croissant d'Etats ont organisés des unités de cyber-guerre et les ont dotés de moyens humains et financiers considérable, ainsi à l'heure actuelle, plus de 30 pays (USA, Chine, France, Israël…) ont organisés de véritables stratégies d'attaques et de défenses cybernétiques et d'autres sont appelés a les rejoindre.

La Cyber-Stratégie :

Le cyber-pouvoir est tactiquement, techniquement et fonctionnellement différent de tout autre instrument de l'arsenal militaire, mais il n'est pas non plus au-delà des stratégies militaires et il ne tend pas à renverser le caractère durable de la guerre, qui lui est immuable.
Par contre, l'attribut stratégique de première envergure du cyber-pouvoir est sa capacité à manipuler l'environnement adverse pour prendre un ascendant sur l'ennemi, sans même avoir à recourir aux armes conventionnelles.

Cela en menaçant directement tous les domaines stratégiques de l'ennemi, étant donné leur dépendance croissante au cyberespace.
Le cyber-pouvoir est soumis aux besoins de la politique des Etats et la cyber-stratégie est le processus qui permet de traduire ces besoins la dans le cyberespace.
Les cyber-opérations se déroulent dans le cyberespace et génèrent du cyber-pouvoir, mais ils ne servent en aucun cas leurs propres desseins : ils servent des fins politiques.
La cyber-stratégie est le pont reliant la politique et le cyber-pouvoir.
Elle s'appuie sur une combinaison systématique et structurée entre les fins (buts et objectifs), les moyens (ressources et compétences) et les manières
(comment utiliser les moyens pour parvenir aux fins), tempérée par des analyses régulières des risques et des coûts.
Afin d'élaborer une stratégie nationale pour le cyberespace, les Etats doivent créer simultanément des ressources cybernétiques et des procédures qui peuvent contribuer à atteindre les objectifs qu'ils se sont fixés pour leur sécurité nationale.

I need money !

Les carders

« *Je veux une carte de crédit pour Noël* »

Les organisations cybercriminelles commencèrent à fleurir a la fin des années 90 dans les pays de L'Europe de l'Est, devenues orphelins après la chute du Mur de Berlin.
Dans ces pays, toutes les conditions nécessaires à ce genre d'activités étaient réunies : faiblesses de l'Etat, corruption a grande échelle, absence de cadre juridique, chômage, mais surtout une frange de la population ayant de grandes connaissances technologiques.
Cette frange la, confiante dans son impunité et se drapant sous le voile du nationalisme, se lança sans aucune retenue dans les activités cybercriminelles.
L'histoire commence avec un certain Roman Stepanenko, alias BOA, un jeune ukrainien doté de deux diplômes universitaires en électronique et qui fut le premier à avoir émis un signal radio amateur depuis la Corée du Nord.
Partageant sa vie entre Malte et l'Ukraine, BOA avait lancé a la fin des années 90 une entreprise, basée à Malte, spécialisée dans la vente de matériels de surveillance et de technologies anti-terroristes à des politiciens et des businessmen de plus de 60 pays a travers le globe.
Mais la cupidité le poussa à lancer en 1999, le site boafactory.com, spécialisé dans la vente de faux-papiers en tout genre.
A l'époque, les cartes de crédits, connaissaient une croissante fulgurante et rien qu'aux USA, en Angleterre, au Japon et au Canada leur nombre total dépassé les 2 milliards de cartes en circulation.
Mais en parallèle, Visa et Mastercard bloquaient les transactions sur les sites russes et ceux enregistrés dans les pays de l'Ex-URSS.
Mais cela ne découragea pas pour autant nos amis de l'Est, car si les sites américains ne livraient pas en Ex-URSS , ils livraient volontiers aux Emirats, a Chypre , Malte ou en Turquie , lieux de villégiature par excellence de la nouvelle élite ex-communiste.
C'était l'époque des balbutiements du cyber-crime globalisé, l'argent été volée par un russe résidant en Ukraine, la marchandise achetée sur un site américain et livrée a Dubaï et de la, remontée jusqu'en Russie, et la transaction ne nécessité qu'une dizaine de minutes.
Avec l'accroissement des sites de e-commerce, Dimitry Golubov, alias Script, pensa a développer un site spécialisé dans la vente de numéros de cartes de crédits, de comptes bancaires et autres données sensibles, car sa base de données personnelle en contenait tellement ,qu'il n'avait plus ni le temps, ni la force pour pouvoir les exploiter.
La rencontre de Script et de BOA fut décisive. Tous deux décidèrent de lancer en mai 2001 la première plate-forme du cyber-crime, le défunt cardersplanet.com, enregistré sous la fausse identité d'une personne habitant Ho-Chi Minh City au Vietnam.

Carderplanet proposé à ses membres de vendre de toutes sortes de données confidentielles et de faux papiers et, BOA, fort de son expérience d'entrepreneur, apporta même la solution au manque de confiance entre les membres, en instaurant la règle du « tiers de confiance » : l'acheteur pour être sur de ne pas être dupé, confiant l'argent de la transaction a BOA ou a Script, et le vendeur devait attendre que l'acheteur soit sur de la qualité de la marchandise avant d'être payé.
Ainsi, Cardersplanet prospéra à tel point que, d'abord fait pour les russophones, le site se dota d'une partie en anglais, permettant ainsi à tous les cybercriminels en herbe de rejoindre le festin.
Fort de leurs succès, BOA et Script organisèrent en 2002 a Odessa la FWCC (First WorldWide Carders Conference), ou furent invités les meilleurs pirates d'Ukraine et de certains pays de l'ex-Union Soviétique tel que le groupe de hackers The Family, Auditor, Rayden ou encore Bigbuyer.
Les discussions de cette conférence s'axées autour de thèmes tel que l'exploitation des cartes bancaires JCB et Dinner ,qui étaient rares sur le site , a l'inverse des Visa et Mastercard , mais aussi autour du développement d'un réseau de « mules » en Amérique du Sud , en Océanie et en Afrique, ainsi que la création d'une franchise CardersPlanet ,en vue de la création de relais régionaux.
Le KGB, lui, avait déjà infiltré le site, mais se contenté seulement d'observer et de stocker les informations, en vue de dresser le Who's Who du site.
Mais, d'une manière imprévue, celle qui allait signer l'acte de décès du site, fut Autodesk, une société américaine de développement de logiciels pour les architectes.
Ayant remarquée qu'un vendeur sur eBay vendait certains de ses logiciels pour une bouchée de pain, Autodesk averti le FBI et la Piracy Protection Unit se lança dans la traque de ce fameux vendeur, qui n'était d'autre que BOA.
Roman Stepanenko fut arrêté en juin 2004 a Chypre et extradé aux USA ou il fut inculpé de 40 chefs d'accusations.
D'autres figures importantes du site furent arrêtées en parallèle, ce qui poussa Script à « éteindre » le site en aout 2004.
Ce dernier eu plus de chance que son partenaire car , malgré une enquête de l'Inspection des Services Postaux américains, les autorités ukrainiennes rechignèrent a l'arrêté ,arguant ne pas connaitre son adresse et durent attendre jusqu'au mois de juillet 2005 avant de procéder a son arrestation, mais avertit a temps , il procéda a la destruction des données présentent sur ses disques durs grâce a un générateur d'ondes électromagnétiques.
Quelques mois plu tard, il fut remis en liberté grâce a l'intervention de certains parlementaires ukrainiens qui témoignèrent en sa faveur, mais aussi étant donné l'absence de preuves suite a la destruction des disques durs.
Dimitry Golubov se lança dans la politique en créant le Parti Internet Ukrainien, avec plus ou moins de succès.
Son cas illustre parfaitement la connivence entre le crime organisé et le pouvoir politique dans certains pays de l'ex-Union Soviétique.
BOA, lui , purge sa peine sous le matricule 59-198-004 au centre de détention de Brooklyn Metropolitan.
Tous deux furent derrière l'émergence d'une nouvelle méthodologie d'engagement dans des activités criminelles majeurs : des fraudes perpétrées sur une large échelle , avec peu de ressources et un risque minimal.

Les site imitant CardersPlanet pullulèrent sur la Toile entre 2002 et 2008, mais très peu réussirent a s'affirmer comme des acteurs de premier plan et pour la suite , nous ne retiendrons que CardersMarket et DarkMarket , étant donnés que leurs histoires respectives illustrent bien les liens troubles entre les agences gouvernementales et les pirates.

Max Butler ,alias Iceman , un hacker de talent reconvertis en consultant en sécurité ,après avoir fait un tour en prison ,géré le site whitehats.com , tout en servant d'informateur au FBI pour couvrir ses activités cybercriminelles.
Surfant sur la vague du « carding » , Iceman lança le site CardersMarket.
Pour s'assurer une place de choix parmi la concurrence ,il décida que le meilleur moyen d'y parvenir serait en lançant un assaut sur les autres sites.
Ainsi, il s'attaqua a plusieurs d'entre eux, vola leurs bases de données, les intégra sur son site avant d'effacer les données des serveurs de ses concurrents. Il fit preuve aussi d'ingéniosité en créant pour son site un « false digital trail », qui donné l'impression a ceux qui voulaient le tracer que les serveurs hébergeant son site étaient localisés en Iran, alors qu'ils étaient en Californie.
CardersMarket prospéra pendant quelques années avant que le FBI ne décide de se retourner contre son informateur. Il fut arrêté en 2007 et accusé d'avoir volé les numéros de plus de 2 millions de cartes de crédits et dépensé plus de 86 millions de dollars en achats frauduleux. Il fut condamné à 13 ans de prison, la plus lourde peine jamais prononcée contre un hacker.
Iceman enfonça lui même les clous de son cercueil en allant exposé sur les sites adverses la liste des policiers et informateurs les surveillant, grâce au rootkit (outil de dissimulation d'activités) qu'il avait réussi a dissimulés sur les serveurs de plusieurs agences fédérales, ayant grâce a sa l'accès aux bases de données répertoriant les policiers, les informateurs et leurs missions.
Iceman réussi a « tuer » presque tous les sites anglophone de « carding » concurrents sauf un, DarkMarket, fondé en mai 2005 par Recka , le « roi des cardres suédois » .
Recka, pris de panique en voyant les arrestations pleuvoir, « éteignit » son site.

C'est la qu'un sri-lankais résidant en Angleterre, Renu Subramaniam, alias Jilsi , sorti de l'ombre a son tour et profita de la mise hors ligne de DarkMarket , pour enregistrer son site sous le nom de domaine Darkmarket.ws (Western Samoa).Il fit d'une pierre deux coups en surfant sur la popularité de DarkMarket et de sa réputation pour attirer sur le nouveau site tous les membres du site d'origine.
Le noyau de l'équipe était formé par Jilsi , Keith Mularski , de son vrai nom Pavel Kaminsky ,alias Master Splynter , et Cagatay Evyapan , alias Cha0s.
Un trio de choc.
Jilsi, a 11 ans, avait fui le Sri-Lanka suite aux persécutions dont son ethnie était victime et après un parcours scolaire chaotique et un rejet de la par de ses camarades, quitta l'école et entama une longue descente aux enfers.
Alcoolique et toxicomane, il passait le plus clair de son temps à jouer aux jeux vidéo et a des activités cybercriminelles.

Pavel Kaminsky, lui était un spammeur chevronné au grand carnet d'adresses criminelles ,ayant été retourné par le FBI en 2004 pour infiltré qui faisaient perdre des millions de dollars aux américains.
Identifié comme tel très tôt par Iceman , Kaminsky réussi néanmoins a gardé du crédit parmi ses pairs.
Cagatay Evyapan , un turc , était spécialisé dans la fabrication maison de « skimmers » , des instruments qu'on place dans les guichets bancaires et qui se chargent de copier toutes les données de la carte bancaire insérée par une victime et , une fois les données récupérées, ont peut reproduire des cartes bancaires « sœurs » qui seront utilisées pour dérober de l'argent.
Il fut arrêté durant un raid des forces spéciales turques après qu'il a identifié un de leurs informateurs et kidnappé et torturé, en publiant ses photos sur Internet.
Suite a l'opération Sting du FBI, qui abouti a l'arrestation de 60 pirates a travers le monde, Darkmarket fut déclaré mort.
Jilsi fut arrêté en Angleterre et inculpé pour plusieurs chefs d'accusation.
Kaminsky , lui court toujours.
Ce trio résume à lui tout seul l'adage circulant entre les pirates qui dit : « Un pirate sur trois est un proxénète des fédéraux ».
Kaminsky l'était.

La RBN

« *Quand les russkofs font du business »*

La Russian Business Network est considérée comme le département des nouvelles technologies de la mafia russe.
Apparue sur le Net en 2006, cette « société » d'hébergement basé a Saint-Pétersbourg, mais ayant des « filiales » disséminées un peu partout dans le monde, au Panama , en République Tchèque , en Chine, aux Seychelles, en Turquie , en Angleterre, mais surtout aux Etats-Unis a cause de la grande offre de data-centers disponible là-bas.
Mais, a l'inverse des sociétés d'hébergements classiques, la RBN n'offre pas de solutions d'hébergements grand public, seulement de l'hébergement pour activités cybercriminelles ultra-lucratives, d'ailleurs elle ne figure sur aucun registre de commerce.
Fondée par Alexandre Boykov ,alias Flyman, un jeune russe de 24 ans , lié a la mafia et a certains politiciens a la réputation sulfureuse , ce réseau d'hébergement dit «Bulletproof » ou a l'épreuve des balles, étant donné la difficulté rencontrée pour dresser une cartographie des tenants et aboutissants ,c'est fait une réputation de « pire hébergeur » de la Toile.
Réputation pour le moins méritée , car ce réseau va de la pornographie sous toutes ses formes (zoophilie, pédophilie…) a la vente de médicaments contrefaits , en passant par le spamming , la création, vente et diffusion de logiciels malveillants ainsi que le « phishing » et la location de « botnets » clés en main.
L'expression marketing « le client est roi » a toute sa valeur chez la RBN, car tant que ce dernier paye, il peut se livrer, sans restrictions aucune, a ses activités cybercriminelles sans craindre que la police vienne un jour frapper a sa porte.
Exemples de certaines activités de la RBN :
Les équipes de la RBN ont modifiés et améliorés le « CoolWebSearch » , un « browser hijacker » ou littéralement « pirate de navigateur web » , qui est un logiciel malicieux capable de modifier les options du navigateur en changeant la page de démarrage ou celle de recherche dans le but de le dirigé vers des sites web hébergés par la RBN. Ainsi, des milliers d'internautes se sont retrouvés a naviguer sur des sites web dont ils ne soupçonnaient même pas l'existence.
En 2006, ils ont propagés sur la Toile le trojan Ursnif, qui exploitait une faille du VML (Vector Markup Language) , un langage de création de graphismes vectoriels sur les pages web et , grâce a ce trojan , ils ont alimentés leurs réseaux de « botnets » en centaines de milliers de « zombies ».
En 2007, la Dream Coder Team , un groupe de 3 pirates russes liés a la RBN , innovent en mettant en vente , mais aussi en l'utilisant a leur propre compte, le MPack , une trousse a outils du pirate, qui exploitée les failles de sécurités de plusieurs navigateurs web tel que Internet Explorer , Mozilla et Opéra.

Ainsi, MPack après son insertion dans le code source d'un site web , se chargé de d'analyser les ordinateurs des victimes se connectant a ce site web, en vue de chercher des failles et , si il en trouvé ,il les exploité automatiquement.
Mis en vente entre 700 et 1000 dollars, MPack disposé d'un support technique, mais aussi de mises a jours des nouvelles failles , vendues entre 100 et 200 dollars par nouveau module d'exploitation de vulnérabilités, voire même jusqu'à 10000 dollars si c'était une faille « 0-Days ».
Grâce à MPack, les hackers de la RBN ont réalisés un des plus beaux coups de l'Histoire de la cybercriminalité en infiltrant le site web de la Bank Of India. MPack fut inséré dans le code source du site de la banque et tous les clients qui s'y connectaient se voyaient rediriger vers un site de la RBN qui tenté d'injecter plus de 22 programmes malveillants et une fois le « boulot » terminé, les victimes étaient a nouveau renvoyés vers le site de la banque pour se connecter a leurs comptes et permettre ainsi aux pirates de récupérés leurs données bancaires.
Entre 2007 et 2008, plusieurs versions de MPack virent le jour mais plusieurs hackers lui ont emboités le pas en développant de nouvelles trousses a outils toujours plus performante tel que «Neosploit », et dont le marché est évalué a des centaines de millions de dollars.
A son apogée, MPack avait contaminé plus de 2 millions d'ordinateurs a travers le monde.
En 2008, ils furent derrière le « botnet » Torpig, qui fut diffusé grâce au rootkit Mebroot.Avec des serveurs C&C basés au Soudan et en Russie, Torpig représenté plus de 30% du trafic mondial des « botnets ».
Il permit à ses créateurs de voler plus de 500000 détails de comptes bancaires.

La RBN faisait appel aux services de EstDomain, une compagnie d'hébergement basée aux Etats-Unis dans l'Etat du Delaware et , ayant son siége a Tartu en Estonie.
EstDomain servait d'hébergeur et de bureau d'enregistrement de noms de domaines Internet (registrar) , ainsi elle permettait d'acheter des noms de domaines sans avoir besoin de donner sa vraie identité , le meilleur moyen de rester intraçable par les enquêteurs.
Son PDG , Vladimir Tsastin , au lourd passé criminel (entre 2001 et 2004 , il escroqua plus de 60000 dollars a des banques estoniennes) fut inculpé pour plusieurs charges dont la falsification de documents et le blanchiment d'argent.
Reconnu coupable en Estonie, il continua de géré d'autres sociétés écrans, tel que Rove Digital , qui servait de contrôle des « botnets ».
Il fut arrêté en 2011 par le FBI , lui et d'autres de ses concitoyens lors de l'opération GhostClick , qui mit fin a la cyber-arnaque DNSChanger.
Derrière EstDomain, se trouvait Atrivo/Intercage, une autre compagnie d'hébergement basée a Condord en Californie, qui ouvrait grand les portes de ses serveurs a tout le répertoire des activités cybercriminelles, et les jours qui suivirent sa fermeture, le taux de spam mondial s'est fortement réduit , avant de repartir a la hausse.
Un autre acteur majeur de la RBN était Nikolai McColo , un russe de 19 ans a l'époque, fondateur de la société éponyme , basée a San José en Californie toujours, qui servait a héberger la plate-forme de commandes du plus grand réseau de « botnets » au monde (Mega-D , Srizbi, Pushdo, Rustock et Warezov) , qui tous réunis , contrôlés des millions d'ordinateurs a travers le monde et générés 75% du

trafic mondial de spam et utilisés pour lancer des attaques DDOS ultra-puissante (ils furent utilisés contre l'Estonie et la Géorgie entre autres).
Une fois que ses FAI (fournisseurs d'accès Internet) lui ont coupée le jus, le trafic mondial de spam baissa de 67% la même nuit.
Il trouva la mort dans un accident de voiture suite à un « rodéo » dans les rues de Moscou en septembre 2007.
A son heure de gloire, les multiples acteurs de la RBN brassés, selon les estimations de plusieurs experts et sociétés de sécurité informatique, un chiffre d'affaire de 150 millions de dollars.
Et ce n'est pas fini, car à chaque fois qu'une tête est coupée, plusieurs autres font leur apparition.

ZEUS

« *L'Olympien du cyber-crime* »

Le programmeur de ce cheval de Troie (trojan) en avance sur son temps a bien choisi le nom au moment de le baptiser, car à l'instar de son alter-ego Olympien, ce trojan était le dieu le plus puissant du cyber-crime.
Zeus, outil cybercriminel de référence sur la Toile ces 5 dernières années, est un trojan « Made in Ukrania », codé par un pirate de génie, visant a la base les systemes Windows.
Plu tard, dans une version améliorée, il visera aussi les téléphones Blackberry et ceux fonctionnant sous Android.
Il fut révélé au grand jour en juillet 2007, quand il fut utilisé pour voler des informations du Département des Transports américain et se développa d'une manière fulgurante, a tel point qu'en 2009 , Zeus avait infecté plus de 20 millions d'ordinateurs dont ceux de Bank Of America , la NASA , Amazon , ABC et Oracle entre autres.
A l'inverse de ses concurrents, Zeus n'a pas été conçu pour utilisation personnelle, mais plutôt pour une utilisation a grande échelle, car son concepteur, des la fin de l'année 2006 , l'a mis en vente et on pouvait le télécharger dans de nombreux forums spécialisés a un prix oscillant entre 700 et 5000 dollars , selon les options que voulait l'acheteur , accompagné d'un manuel d'utilisation en anglais et en russe , ainsi que des offres d'hébergement pour en faire un serveur C&C.
Il faut dire qu'il a connu un grand engouement de la par des cyber-braqueurs car l'investissement de base été vite compensé et on pouvait en tirer des bénéfices juteux.
Zeus ne se contentait pas de voler les informations personnelles de ses victimes, il était spécialement conçu pour voler les informations bancaires en utilisant la méthode du « form-grabbing » , méthode consistant a injecter de faux champs dans les formulaires de la page visitée.
Un de ses fichiers source consisté en une liste de tous les sites web de toutes les banques du monde.Impossible d'y échapper.
Ainsi , imaginons que votre ordinateur soit infecté par Zeus. Une fois que vous tapez dans la barre de navigation l'adresse du site de votre banque, automatiquement Zeus communique avec sa base de données pour savoir si ce site y est listé. Si c'est le cas (impossible que sa ne le sois pas vu qu'il a dans son « ventre » les adresses web de plus de 5000 banques a travers le monde) , il se met aussitôt a injecter des champs supplémentaire dans la page sur laquelle vous êtes selon la programmation que lui a faite son « master ».
Ainsi , au lieu d'avoir seulement les champs « login » et « mot de passe » , il peux aussi vous ajouter les champs « numéro de carte bancaire » , « clé » et « PIN ».

Pour ce faire , Zeus utilise la méthode du «Man in the browser » ou « l'homme dans le navigateur » c'est-à-dire qu'il se met entre vous et votre ordinateur et change selon la manière dont il a été programmé , les informations que vous voyez sur la page que vous visitez.
Zeus a été répandu selon les schémas classiques de diffusion des logiciels malveillants : soit par implémentation de code malicieux dans des pages web (Drive-by download) qui fait que la simple visite d'un site fait de vous une victime, soit par le spam, ces courriels polluant vous invitant a télécharger des documents ou des chansons et vidéos ou en vous envoyant vers des sites piégés , et par la méthode du « Binding » ,qui consiste a mélanger le virus a un logiciel tel que Windows , Photoshop etc. et a les mettre en téléchargement gratuit sur les sites de partages.
Une autre des spécificités de Zeus est son utilisation d'un système de protection contre les copies pirates , en générant une clé , tous comme Windows ou n'importe quel autre logiciel payant et , évoluant au fil des versions, il a aussi élargi son spectre d'attaque en visant les tablettes et les smartphones , car ce sont des marchés très porteurs pour les pirates.
Après avoir programmés l'exécutable et l'avoir répandus, les hackers utilisés les données récupérées pour transférer de l'argent dans des comptes bancaires ouverts par des « mules » , des gens utilisant des faux papiers d'identité et en échange d'une commission , ils se chargeaient ensuite de transférer l'argent par Western Union aux pirates.
Ainsi ,lors d'une opération du FBI en 2010, plus de 100 personnes furent interpellées parmi elles , 90 « mules » aux Etats-Unis et le reste en Ukraine et en Angleterre, qui ont détournées plus de 390 millions de dollars.
Fin 2010 , le créateur de Zeus, vendit le code source au créateur de son concurrent SpyEye et plusieurs ont vus dans ce geste une intention de se retirer , mais en 2011 , le code source de Zeus fuita sur Internet , ce qui prédit l'apparition prochaine d'un nouveau trojan encore plus ingénieux que son ancêtre.

Les réseaux sociaux

« *J'ai beaucoup d'amis ! »*

Les réseaux sociaux sont devenus une partie intégrante de nos vies.
Qui d'entres vous n'a pas de profil Facebook ou Twitter ?
Le «web social » représente une mine d'informations sans précédent, regorgeant d'informations personnelles ou confidentielles sur les gens, les compagnies, les gouvernements et utilisé par les pirates pour dresser le profil de leurs cibles.
La moyenne mondiale d'usage des réseaux sociaux est de 2,5 heures par jour et par internautes.
Largement de quoi laisser beaucoup d'informations a portée du premier venu.
Les attaques sur les réseaux sociaux sont divisées en deux catégories :
La première est le « social engineering ».
L'attaquant fait un tour sur les profils Facebook , Twitter etc. de sa cible , récolte des informations sur son parcours , ses préférences, ses passions, sa situation sociale etc. , dresse une cartographie des ''amis '' de sa cible et ensuite se lie ''d'amitié'' avec elle , en faisant semblant de partager beaucoup de points communs avec elle ,dans le but non avoué de la mettre en confiance et pouvoir abuser de sa naïveté pour lui soutirer les informations dont il a besoin pour la piéger.

La deuxième est la création de réseaux :
Une personne , un organisme ou une société , décide de se créer un réseau dans un but lucratif.
Rien de plus simple.
Pour un budget compris entre 300 et 600 dollars, ils peuvent s'offrir un robot qui crée des centaines voir des milliers de faux profils , les alimente en fausses informations et photos pour les faire passer pour des vrais, ajoute les personnes qui partagent les opinions ou les intérêts recherché par l'instigateur , les invite a rejoindre des groupes ou a aimer des pages et peut même partager des liens de sites piégés avec tous les contacts de tous ses faux profils.
Le meilleur moyen de se faire un bon réseau de « zombies » pour alimenter un « botnet », car si les gens sont de plus en plus réticents a cliquer sur les liens dans les emails, ils le font avec plaisir quand c'est un de leurs « amis » qui l'a posté sur leur profil.

Mais les réseaux sociaux ne servent pas seulement aux gens mal intentionnés, ils sont très utilisés par les agences de renseignements pour récolter des informations sur les gens qu'elles visent, a tel point

que les réseaux sociaux ont révolutionnés le mode de fonctionnement des espions : plus besoin de faire des planques , des filatures, de crocheter des serrures pour installer des micros etc. , la cible elle même fait tout le travail en affichant a tous le monde ce qu'elle fait , ou elle est et avec qui elle est en contact.

Peu d'entre vous d'ailleurs savent que In-Q-Tel, un fond d'investissement de la CIA est actionnaire de beaucoup de réseaux sociaux tel que Facebook , Digg , Twitter ,Pinterest etc..Suffit de faire un tour sur le site web de ce fond d'investissement pour s'en assurer, il l'affiche sans complexe sur sa page d'accueil.

Au bon vieux temps , chercher des informations sur une personne couté de l'argent , de nos jours…..quelques clics suffisent.

Bienvenue chez les cyber-criminels.

1.2 trilliards d'argent volé en 2012, 65% des internautes victimes de cyber-crimes,1,5 millions de victimes par jour,556 millions par an, 18 par secondes,2 sur 3 adultes victimes de cyber-arnaques.
Aujourd'hui ,personne n'est a l'abris du cyber-crime, surtout qu'il a émigré sur les téléphones mobiles et les tablettes.
Un anti-virus ? Il faut déjà qu'il puisse se protéger lui-même.
La messe est dite, un jour ou l'autre, vous vous ferez voler votre argent !

Mon sit-in sur Internet !

Anonymous

« *Anonymes….mais pas tant que sa ! »*

A part si vous vivez dans une grotte en Afghanistan et que vous utilisez des pigeons voyageurs pour correspondre, vous devez sans doute avoir entendus parler des Anonymous, ce collectif de hackers international ayant souvent fait la Une des médias ces dernières années.
Un groupe dont les règles sont inspirées du film Fight Club : « Ne jamais parler d'Anonymous, ne révèle jamais ta véritable identité, n'attaque pas les médias car on ne tue pas le Messager » et dont le logo fut d'abord inspiré du tableau de René Magritte ,mais avec un point d'interrogation a la place de la pomme avant de devenir le masque de Guy Fawks ,conspirateur révolutionnaire anglais du 15eme siècle mis en scène dans le film V for Vendetta.
Mais peu d'entre vous connaissent l'histoire de ce groupe, ses origines et ses multiples acteurs. Dans cette partie, nous allons lever le voile sur ce collectif qui causa par ses actions plus de mal que de bien car croyant agir pour le bien de l'Humanité, ils n'ont finalement réussis qu'a semer la panique.
L'Enfer est pavé de bonnes intentions.
Tout commence avec le « trou du cul d'Internet », le fameux 4chan.
4chan fut créer par Christopher Pool, adolescent américain ayant grandit comme beaucoup de ses pairs devant un écran de télévision avec la télécommande dans la main gauche et la manette d'une console de jeu dans la droite.
Passionné de mangas, le jeune Christopher passé ses journées sur Internet a la recherche d'images de vidéos et d'autres mangas-dépendants comme lui.Ainsi au fil des recherches, il trouva un forum japonais ,2chan, créer en 1999 par Hiroyki Nushimina, et qui faisait fureur au pays du Soleil Levant.
Christopher, sous le charme, copia le concept de 2chan en prenant le code source, qui été ouvert et disponible sur Internet, le traduisit et donna naissance a 4chan.
A ses débuts , 4chan ne nécessité pas d'inscription , juste un pseudo (nickname) et avait la particularité de ne rien sauvegarder , les anciennes discussions disparaissaient ,remplacées par les nouvelles.
Une année plu tard, Christopher lu l'essai d'un programmeur qui faisait l'éloge de l'anonymat sur les forums de discussions, car disait-il, les nicknames poussaient les utilisateurs à devenir vaniteux et imbus de leurs personnes.
Adhérant à cette philosophie, Christopher intégra le module « Forced Anon » (anonymat forcé), développé par ce même programmeur, sur certaines parties du forum.

A partir de ce moment une bataille rangée à base de « posts » commença entre les partisans des nicknames et ceux de l'anonymat. Les premiers appelèrent les seconds, les Anonymous.
Et les Anonymous gagnèrent la bataille et « Forced Anon » fut intégré sur toutes les parties du forum.
4chan, qui fut créé à la base pour partager des images et des liens de mangas, bascula rapidement en une sorte de fourre-tout, ou on peut trouver toutes sortes d'images obscènes et des liens vers des sites que les moteurs de recherches tel que Google ne peuvent indexés par soucis de respectabilité.
Liens vers des sites de pédophilie, de zoophilie, des images violentes et choquantes, du racisme, du foutage de gueule, des insultes a tours de bras, rien ne manqué sur 4chan.
Pourquoi ?
Parce que les utilisateurs, couvert par l'anonymat, laissés libre cours a leurs cotés obscurs.
Mais aussi parce qu'une majorité des utilisateurs de 4chan étaient des adolescents souffrant de tous les maux dont souffrent les sociétés modernes : parents divorcés, abandon scolaire, rejet de la société, toxicomanie et alcoolisme et remplissais leur temps libre en déversant toutes leur haines et tous leur vices sur ce forum.
Chose qui fut confirmée par une longue enquête de Fox11 qui surnomma 4chan, « la machine de la haine sur Internet ».
En 2008, deux étapes important furent franchies et qui firent connaitre les Anonymous au reste du monde.
Tout commence par l'affaire Joseph Fritzl , un ingénieur autrichien qui enferma sa fille dans le sous-sol de sa maison et la viola pendant 24 ans.
L'info fut relayée par la toute la presse et indigna le monde entier.
Chez les Anonymous de 4chan, cette affaire ne suscita que des amusements et des commentaires ironiques et pour marquer le coup, certains d'entre eux créèrent un faux compte sur Twitter qu'ils appelèrent @basementdad (le papa du sous-sol) et se lancèrent le défi d'avoir un million de followers sur ce compte, combat qui été engagé a l'époque entre l'acteur Ashton Kutcher et la chaine CNN.En moins de 24 heures , ils réussirent a attirer 300000 followers et atteignirent un demi-million avant que Twitter ne désactive le compte.
Vien ensuite l'affaire de l'Eglise de Scientologie.
Cette secte, fondé par Ron Hubard , un écrivain de science-fiction , et qui proclame être une religion est , depuis sa création, l'objet de toutes les controverses.
Elle est notamment connue pour exercer toutes sortes de pressions sur ses détracteurs et ses ex-membres, allant de l'intimidation à l'espionnage en passant par les tribunaux.
Et cela même sur Internet, depuis que certains de ses ex-membres se sont mis à faire fuiter des documents confidentiels de la secte sur Usenet en 1994.
Cette fois, c'est une vidéo de Tom Cruise (adepte de la secte), dans un délire total, qui fut l'objet de la discorde.
Initialement tournée à des fins de propagandes, la vidéo ne fut pas dévoilée par l'Eglise de Scientologie a cause de l'attitude totalement déjantée de Tom Cruise sur la vidéo, mais aussi a cause du non-sens total des paroles qu'il prononce dessus.
Mais la vidéo fuita et se retrouva sur Youtube.
Elle ne resta pas longtemps en ligne, car la Scientologie menaça Google de poursuites judiciaires.

Le géant du web, déjà embourbé dans une plainte de Viacom, qui demandée un dédommagement d'un milliard de dollars a cause de la violation de ses droits d'auteurs, décida de supprimer la vidéo.
Un site d'information américain, Gawker, la mis en ligne a son tour sur l'un de ses blogs, au nom de la liberté d'information (surtout pour attirer des visiteurs).
L'article de Gawker fut repris par les Anonymous qui en débattirent longtemps sur 4chan. Sur une des discussions, un jeune proposa d'attaquer la Scientologie et beaucoup s'enflammèrent à l'idée de pouvoir se battre contre une organisation dotée de moyens financiers colossaux et d'une armée d'avocats.
Etant donnée la difficulté de s'organiser sur 4chan , vu qu'il suffit de rafraichir la page pour ne plus trouver la discussion tellement le flux est continu, les Anonymous emballés par l'idée de l'assaut décidèrent d'aller sur IRC pour pouvoir planifier tranquillement leur bataille.
IRC ou Internet Relay Chat, est l'ancêtre de MSN, PAL talk et autres outils de tchat. Créer en 1988 par Jarko , qui travail actuellement pour la branche suédoise de Google , IRC est basé sur un systèmes de plusieurs réseaux et ne nécessite pas de compte pour s'y connecter , juste un client IRC (tel que mIRC). Une fois connecté sur un des réseaux, il suffit de créer un chanel (chambre de discussions) ou de rejoindre une des milliers déjà crées par d'autres.IRC permet aussi de rester anonyme en utilisant un proxy.
Ainsi, ils rejoignirent le réseau EFNet (un des plus anciens) et créèrent le chanel #OpScientology. Les « Anons » choisirent de lancer un DDOS contre les sites web appartenant a la Scientologie, qui avant cette attaque, était une exclusivité des cybercriminels.
Ne disposant pas de « botnets », les « Anons » utilisèrent des instruments de « stress-test » de serveurs tel que le défunt Gigaloader.com et Jmeter, et ils créèrent aussi un site web regroupant toutes les coordonnées des avocats et des multiples centres de la Scientologie a travers le monde , en demandant a tous les membres de 4chan de les bombarder d'appels téléphoniques, d'envoyer des fax de papiers noir destinés a épuiser leur cartouches d'encre et de leurs commander des taxis et des pizzas.
Depuis cette attaque, la devise des « Anon » fut : Si nous avons pu battre la Scientologie, alors nous pouvons vaincre n'importe qui !

Deux ans s'écoulèrent sans aucun autre coup d'éclat des Anonymous, quand en septembre 2010 , l'indien Girish Kumar , patron de Aiplex , fit une sortie tonitruante dans la presse , en annonçant qu'il travaillé en tant que « tueur a gages » pour Bollywood , en attaquant des sites web qui permettent aux gens de télécharger des films piratés. Il donna en exemple sa récente attaque sur le site de partage de torrents, The Pirate Bay, sur lequel il lança un DDOS qui le rendit indisponible pour 2 jours.
L'article fut repris à nouveau par les Anon sur 4chan et Aiplex fut victime le jour suivant d'un DDOS qui fit regretter à son patron sa sortie.
Surfant sur leurs succès, les Anon passèrent à la vitesse supérieure en s'attaquant à la RIAA et la MPAA (associations américaines de défense des droits d'auteurs).
Pour leurs troisième victime, la Copyright Alliance, ils choisirent d'infiltrer le site grâce a une injection SQL et remplacèrent son contenu d'origine par un index de liens de films, jeux et chansons piratés et publièrent aussi sur le même site une base de données de 500 Mo d'emails de la compagnie londonienne de protection des droits d'auteurs.

Après cela, les participants de l'opération Payback commencèrent à travailler sur une infrastructure de communication pour Anonymous car de plus en plus de réseaux IRC refusés de les accepter a cause de leurs opérations.
Certains louèrent des serveurs , d'autres en achetèrent et créèrent ainsi le premier réseau IRC pour Anonymous, qu'ils baptisèrent AnonOps ,avec plusieurs chanels juste pour les membres d'Anonymous, certains publics , d'autre privées.
La suite , elle , appartient désormais a l'Histoire, Mastercard, Paypal , Sony …et la liste des victimes des Anon est encore longue , et les arrestations de ses membres aussi.

Télécomix

« *Un nouveau modem vous appel* »

Télécomix

Télécomix est une organisation mondiale de « hackers de la liberté », lancée officiellement en 2009 dans le but de s'opposer aux lois de surveillance des télécommunications discutées au parlement européen et dont les 300 membres, à l'opposé d'Anonymous, ne cachent pas leurs identités pour agir.
Composée de plusieurs hackers de divers horizons, certains militants du Parti Internet Suédois, d'autres du Chaos Computer Club et certains « indépendants » ,Télécomix a depuis sa création , luttée contre la censure et les systèmes de surveillance , sans pour autant entrer en confrontation directe avec des gouvernements ou des multinationales.
Le but clairement affiché de Télécomix est de pouvoir offrir, a titre gracieux, des outils et des systèmes permettant de contourner la censure et la surveillance pour les populations des régimes dictatoriaux pour leurs permettre de communiquer sans passer par la case prison.
Leur première opération remonte au début de la Révolution Tunisienne.
Anticipant la « fièvre des réseaux sociaux », le gouvernement de Ben-Ali coupa l'accès à Facebook pour éviter que la population ne poste des vidéos montrant la répression sanglante des manifestants.
Télécomix propose alors aux militants tunisiens de leurs envoyés les vidéos pour qu'ils puissent les diffuser sur les réseaux sociaux.
Après que le régime de Ben-Ali soit tombé, les Télécomix vinrent en aide aux égyptiens après qu'eux aussi soient sortis dans les rues pour demander la chute de la dictature instaurée pendant 30 ans par Hosni Moubarak.
Ainsi, ils reproduisirent le même scénario qu'avec les tunisiens, en postant les vidéos des répressions sur Facebook et Youtube et ont même mis en place des miroirs (copies de sites Internet) et des proxys pour postés les vidéos qui n'étaient plus accessibles.
Le régime de Moubarak alla plus loin en coupant carrément l'accès a Internet le 28 janvier 2011 et la , les Télécomix se sont jetés corps et âmes dans la bataille , en mettant en place , avec l'aide de certains fournisseurs d'accès , des centaines de lignes d'appel pour modems classiques, permettant ainsi a tous les égyptiens disposant d'un téléphone fixe (les lignes fixe n'avaient pas été débranchées par le régime) ,

de pouvoir se connecter a Internet et continuer a poster des photos et des vidéos des exactions de forces de l'ordre mais aussi de continuer a communiquer entre eux pour s'organiser face a la répression sanglante du régime.
Ils firent la même chose aussi en Libye, mais leur fait d'armes le plus important est la bataille qu'ils ont livrées (et continuent de livrer) au régime de Bachar Al Assad.
Les Télécomix ont envoyés des e-mails en masse a tous les internautes syriens avec des manuels pour contourner la censure, en leurs proposant les méthodes qui ont fait leurs preuves dans les autres pays révoltés.
Le combat des Télécomix n'est toujours pas fini et tant que des Etats continueront à appliquer la «dictature du web », il ne sera jamais fini.

Le Hacktivisme :

Le mot « hacktivisme », mélange de hack et activisme, fut inventé en 1996 par Omega, un membre du collectif de pirates, The Cult Of The Dead Cow et désigne l'utilisation d'ordinateurs et de réseaux informatiques en tant que formes de manifestations et de protestations politiques.
Depuis longtemps des hommes se sont dressés contre l'oppression et la tyrannie des gouvernements, parfois aux périls de leurs vies, mais depuis l'avènement des ordinateurs et des réseaux de télécommunications, les combattants de la liberté ont eu une plate-forme inespéré pour passer leurs messages, recruter des sympathisants et mener des actions : Internet.
Pour comprendre le hacktivisme, il faut revenir des dizaines d'années plus loin.
Si le mot hacker fait froid dans le dos de nos jours, invoquant dans l'esprit de la populace , des jeunes adolescents assis dans la pénombre de leurs chambres , volant des identités et des cartes de crédits et utilisant leurs savoir-faire pour provoquer la destruction et le chaos, a la base il fut inventé par le mathématicien John Forbes Nash Jr en 1940 pour designer une solution rapide permettant de résoudre un problème.
Les activistes, eux, sont la depuis longtemps, mais ont connus leurs apogée durant les années 60 et 70, durant les vagues de manifestations pour stopper la guerre au Vietnam. De ces contestations sont nées les contre-cultures telles que les Hippisme etc., cherchant un monde libre, des gouvernements œuvrant en toute transparence, la paix dans le monde etc.
Les hackers, eux, cherchèrent dès leurs débuts à briser les monopoles des sociétés commerciales sur les outils de télécommunications, en voulant qu'ils soient a la portée de tout le monde et gratuitement, ainsi en 1970, John Drapper réussit à pirater avec un sifflet offert dans les boites de corn-flakes Captain Crunch, les serveurs des lignes de téléphones fixe de la société américaine AT&T. Le phreaking était né.
De la rencontre sur les campus des universités américaines entre des étudiants activistes et des hackers fut né le hacktivisme, mais pas dans sa version que nous connaissons de nos jours.
Les hacktivistes des années 70 et 80 cherchaient plutôt a contrer les sociétés commerciales en développant des solutions alternatives, ainsi vit le jour en 1982 a Berlin , le Chaos Computer Club , ou des hackers bricolés des gadgets et toutes autres choses en rapport avec les ordinateurs pour les céder gracieusement a la communauté ,un an plu tard , Richard Stallman ,lança au Etats-Unis le projet GNU , visant a établir créer des logiciels « libres » c'est-à-dire gratuit et dont le code source est ouvert.
En 1989, les hackers infectèrent les ordinateurs de la NASA avec le ver WANK (Worms Againt Nuclear Killers) en signe de protestation contre le développement de nouvelles armes nucléaires, ainsi tous les ingénieurs de la NASA en allumant leurs ordinateurs découvrirent un message qui ne les laissa pas de marbre : « Vous parlez de paix dans le monde tout en préparant la guerre ».
Dans les études de cas précédentes, nous avons vus deux conceptions et formes différentes de l'hacktivisme , la première, criminelle sur les bords, menée par des adolescents ne mesurant pas la portée de leurs actes et ses répercussions , voulant connaitre leur quart d'heure de gloire en s'attaquant a tout le monde et finissant par s'aliénés même leurs soutiens, car si ils ont réussis certains jolis coups comme la participation a l'arrestation de pédophiles ou la divulgation des 5 millions d'emails de Stratfor

, société d'intelligence économique texane ,qui montra a quel point des gouvernements et les diplomates et journalistes de tous bords ont donnés des informations a Stratfor en échange d'argent sur des comptes suisses, ils n'empêchent que les Anonymous , par leurs actes non réfléchis ont finis par plantés des clous dans le cercueil de la liberté d'Internet car l'action violente a pour conséquence une réponse violente et beaucoup des gamins d'Anonymous croupissent maintenant en prison et les Etats et sociétés victimes de leurs témérités sont plus que jamais déterminés a sonner la fin de la récré sur Internet.

La deuxième, celle des Télécomix, est beaucoup plus noble, et verse dans l'essence même de l'hacktivisme : développer des solutions alternes pour contrer l'hégémonie des gouvernements et des sociétés capitalistes.

Le combat est long, les armes inégales, mais les hacktivistes ne laisseront jamais la flamme de la liberté s'éteindre.

Epilogue

Fermez vos ordinateurs, enterrez les six pieds sous terre.

Jettez votre smartphone dans les toilettes et tirez la chasse.

Cassez votre tablette en milles morceaux.

Et enfin priez…..priez pour que l'Apocalypse ne soit pas numérique…priez pour que l'Antéchrist ne soit pas un virus, un trojan ou une bombe logique.

Amen