L'hacktivisme

François PAGET (Chercheur chez McAfee Labs)

Juillet 2013, Article n°II.3

Dans le domaine de la sécurité informatique, l'hacktivisme couvre une part non négligeable des cyber-menace actuelles. Dans les pages suivantes, nous détaillerons ceux qui s'en revendiquent en comparant leurs motivations, leurs méthodes d'action et l'impact de leurs actes à ceux des autres acteurs de la cybercriminalité.

L'hacktivisme au sein de la cybercriminalité

Les profils de cybercriminels sont multiples. Ils ont amené de nombreux chercheurs à créer leur propre typologie des acteurs de la cybercriminalité. Nous en retiendrons trois.
La première date de 2012, elle émane de Raoul Chiesa, qui l'a mise en place au démarrage de la seconde phase de son étude sur le profil des hackers (The Hackers Profiling Project – HPP V2.0 – 2011-2015) [1]. Présentée dans le tableau ci-dessous, sa classification est encore provisoire et passe aujourd'hui par 9 profils distincts.

Profile	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they may act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

FIGURE 1 : PROFILS DE CYBERCRIMINELS (D'APRES ROBERT CHIESA)

[1] http://www.flemminggulf.com/cms/uploads/conference/downloads/Raoul%20Chiesa%20DAY%202.pdf

Dans une classification de ce type, l'hacktiviste peut se retrouver dans nombres de ces catégories : il peut être, par exemple, un script kiddie [2], un hacker éthique ou un cyber-guerrier.

Une seconde représentation nous est offerte dans le rapport Verizon d'avril 2013 [3]. Ici le point de départ est la filiation de l'attaquant à un groupe (le crime organisé, l'état ou l'activisme).

	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

FIGURE 2 : PROFIL DES CYBERCRIMINELS (SOURCE VERIZON)

Non représentés dans ce schéma mais non oubliés dans le rapport, on trouve aussi l'entreprise avec son personnel et ses partenaires ainsi que la personne isolée.

L'étude des diverses typologies des acteurs de la cybercriminalité, dont les deux détaillées ci-dessus m'ont amené à créer le schéma suivant dans lequel on retrouve tous les acteurs mentionnés (à gauche), avec, sur fond rouge, les trois majeurs du moment : le crime organisé, les états et les hacktivistes.

[2] En français : gamins du script. Leur tranche d'âge est 10 à 18 ans. S'ils sont plus jeunes (9 à 16 ans) ils sont parfois également surnommés lamers (en français : boiteux) ou encore packet monkeys (en français : singes des paquets réseau).

[3] http://www.verizonenterprise.com/DBIR/2013/

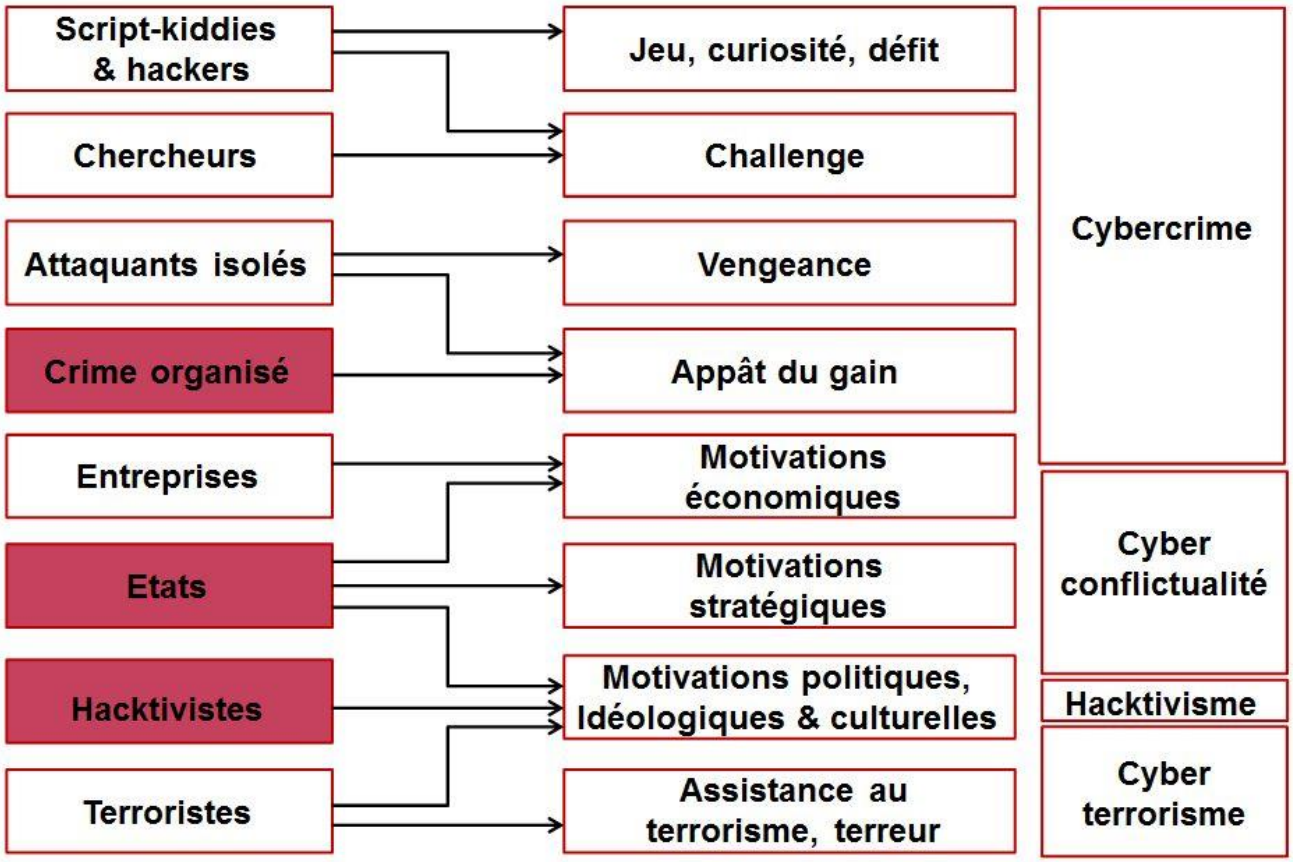

FIGURE 3: PROFIL DES CYBERCRIMINELS (SOURCE FRANÇOIS PAGET – MCAFEE)

Au centre de ce graphique, et reliés aux acteurs se retrouvent leurs principales motivations. Il est bien évident que des cas d'exception existent, et qu'un acteur malveillant, agissant au titre de son entreprise, peut parfois vouloir agir par vengeance.
A droite, les différents niveaux d'affrontement sont listés au regard des motivations et des acteurs avec qui ils interfèrent. On voit ainsi que les intentions des hacktivistes rejoignent aussi les domaines de la cyberconflictualité [4] et du cyberterrorisme.

Hacktivisme : une rencontre entre hackers et activistes

L'hacktivisme est un néologisme issu des termes hacker et activiste. Il semble avoir été utilisé pour la première fois en 1996 par un membre du groupe Cult of the Dead Cow [5] (*to describe hacking for political purposes* [6]).

Définition du hacker

Dans les années 80, bien moins connu qu'aujourd'hui, le mot hacker circulait dans la sphère des passionnés d'informatique et véhiculait une image assez positive (citons par exemple le livre de

[4] Dans ce schéma le terme de cyberconflictualité est préféré au terme de cyber-guerre. Le terme guerre induit l'existence parallèle d'un conflit armé. Même si les attaques informatiques en ce domaine peuvent mettre en cause la souveraineté d'un Etat, elles n'entrent pas forcément dans le cadre d'un conflit armé puisque le seuil qui caractérise l'usage de la force n'est pas atteint.
[5] Organisation hacker fondée en 1984 à Lubbock au Texas aux Etats-Unis. Elle est connue pour avoir, entre autre, créé, en 1998, Back Orifice, logiciel client/serveur d'administration et de prise de contrôle à distance de machines utilisant le système d'exploitation Windows.
[6] Hacktivism: From Here to There: http://www.cultdeadcow.com/cDc_files/cDc-0384.html

Steven Levy, publié en 1984, qui porte le titre Hackers: Heroes of the Computer Revolution [7]). Même s'il contenait une part de transgression, le terme exprimait un idéal en se manifestant par un engagement militant en faveur d'une information libre, partagée et décentralisée.

Le terme a changé au fil des années, devenant petit à petit synonyme de vandalisme et de vol informatique. Aujourd'hui, ses définitions sont innombrables. Positives, péjoratives ou négatives, elles vont du programmeur informatique passionné, brillant et adepte de l'open source au simple curieux, en passant par le délinquant qui pénètre par infraction un système informatique pour voler ou détruire des données.
Faisant référence aux archétypes des films de westerns américains, les hackers furent alors classifiés par couleur en référence à celle des chapeaux des cow-boys qui en sont les héros (le cow-boy au chapeau blanc est le gentil héro, celui au chapeau noir est le méchant).
Aujourd'hui la distinction par couleur est toujours utilisée, même si son origine est maintenant oubliée de beaucoup. Une troisième couleur a aussi été ajoutée : le gris. Il y a donc :

- Le hacker *white hat* ne s'aventure pas dans l'illégalité. Il discute d'intrusion informatique, de programmation et de techniques de hacking. Il se considère comme un passionné de sécurité informatique et veut en faire profiter ses relations. S'il découvre une faille, il ne la divulguera pas publiquement, mais en fera part, souvent sans contrepartie, aux spécialistes du domaine qui pourront la combler.

- Le hacker *grey hat* discute et teste les méthodes criminelles. Sans rien détruire, il n'hésite pas à s'introduire dans des systèmes informatiques de façon illégale. S'il découvre une faille, s'il met la main sur un programme malveillant, ou s'il parvient à « craquer » un logiciel, il mettra sa découverte à disposition de tous sans se préoccuper, ni des mauvais usages qui pourraient en être fait, ni des implications légales pouvant régir cette pratique. Ne se fiant qu'à sa propre déontologie, il pourra aussi vendre « au plus offrant » ses découvertes ou sa compétence.

- Le hacker *black hat* enfreint régulièrement la loi. Il utilise ses compétences de façon nuisible et représente une menace réelle. Il pénètre les systèmes informatiques en cherchant à nuire aux personnes (physiques ou morales) qui en sont les propriétaires.

A ne pas confondre avec les hackers, les script-kiddies utilisent, sans vraiment les comprendre, donc généralement de façon maladroite, leurs programmes et leurs techniques. Les objectifs des script-kiddies vont du simple amusement au vandalisme assumé.

Définition de l'activisme

Selon le dictionnaire Larousse, l'activisme est un système de conduite qui privilégie l'action directe [8], en particulier dans les domaines politique et sociétal. De leur côté, en 1997, les professeurs de droit, Raymonde Crête et Stéphane Rousseau, reprenaient dans un de leurs ouvrages [9] et après les avoir traduits, les définitions du Merriam Webster's Collegiate Dictionary (10ème édition) et du American Heritage Dictionary. Ils définissaient l'activisme comme "une doctrine ou une pratique qui met l'accent sur une action directe et vigoureuse, plus particulièrement pour exprimer son appui ou son opposition à l'égard d'une question controversée" ou encore "une théorie ou une pratique basée sur une action militante".

[7] http://digital.library.upenn.edu/webbin/gutbook/lookup?num=729
[8] http://www.larousse.fr/dictionnaires/francais/activisme/945
[9] Crête R. et Rousseau S. (1997), « De la passivité à l'activisme des investisseurs institutionnels au sein 9des corporations : le reflet de la diversité des facteurs d'influence ». http://lawjournal.mcgill.ca/documents/42.CreteRousseau.pdf

Cyber-activisme & hacktivisme

Parfois proches du militantisme libertaire (désir de préserver la liberté d'entreprendre, la liberté individuelle, la liberté d'expression, la liberté pour la circulation des données), des activistes utilisateurs du Net se sont petit à petit engagés à la construction d'un activisme en ligne. A l'image de certains activistes qui n'hésitèrent pas à pénétrer le périmètre interdit de centrales nucléaires européennes [10], ceux qui se revendiquent aujourd'hui de leur idéologie, mais préfèrent agir sur Internet, ont décidé qu'ils pouvaient, au nom de leur conviction, s'introduire dans des espaces numériques qui leur sont interdits.

Pour le professeur Dorothy Denning, l'hacktivisme couvre « des opérations utilisant les techniques de hacking à l'encontre de sites internet dans l'intention de perturber le fonctionnement normal mais sans causer de dégâts sérieux » [11].

Dans un document de 2012 [12], la société CEIS les présente ainsi :

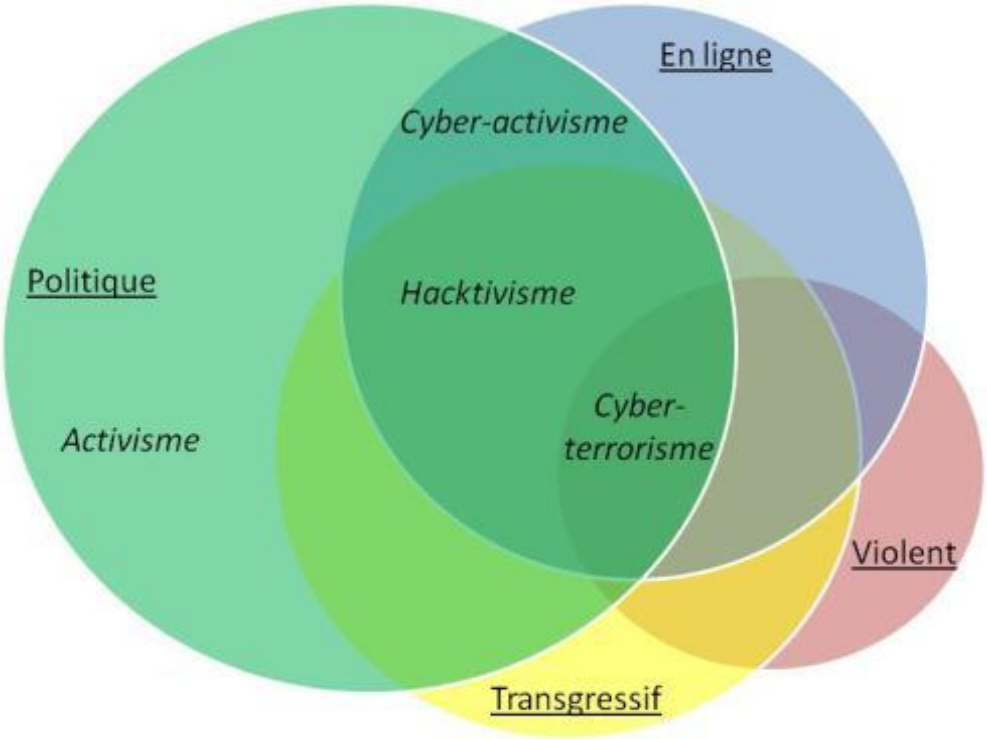

FIGURE 4 : PROFIL DES ACTIVISTES (SOURCE CEIS)

On y retrouve de manière illustrée la définition de l'hacktivisme par Alexandra Samuel [13] qui définit le mouvement comme « l'utilisation non-violente d'outils digitaux illégaux ou transgressifs à des fins politiques ».

Ce schéma et cette définition sont intéressants car ils permettent de distinguer l'hacktiviste du cyber-activiste. Ce dernier n'emprunte pas de formes transgressives pour s'exprimer mais se contente de transposer son « activisme » dans le cyberespace (par l'envoi de mail, par ses publications sur Twitter

[10] Comme ce fut par exemple le cas dans les centrales de Bugey et de Civaux, le 2 mai 2012.
[11] http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (page 241)
[12] http://www.defense.gouv.fr/content/download/200639/2219639/file/OMC2012T3.pdf
[13] Alexandra SAMUEL, Hacktivism and the Future of Political Participation, Thèse de l"Université de Harvard, Cambridge Massachusetts, septembre 2004, p.2 : "hacktivism is the non violent use of illegal or legally ambiguous digital tools in pursuit of political ends".
http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

ou Facebook, par l'animation d'un blog…). Il laisse aux seconds le soin d'actions plus radicales les entraînant régulièrement à braver la loi (défiguration de sites, dénis de service, piratage, etc.).

Hacktivisme et cyber-terrorisme

L'amalgame est parfois fait entre activisme, éco-terrorisme et terrorisme. Aujourd'hui certaines publications généralistes en affublent même certains membres d'Al Qaeda [14]. Cette diversité de vue nous montre la difficulté de l'exercice qui consiste à définir ce terme dont les caractéristiques avancées peuvent changer d'un pays à autre, selon qu'il est qualifié de par nos critères comme état démocratique, autoritaire, religieux ou extrémiste.

Intégrant le concept de violence, le schéma ci-dessus (figure 4) devrait permettre de différencier hacktivisme et cyber-terrorisme.
Mais même du côté des Anonymous, les opinions divergent. Selon la définition du cyber-terrorisme par Mark Pollitt (« attaque préméditée et politique motivée contre les systèmes d'information, programmes informatiques et données par des sous-groupes nationaux ou agent clandestin de laquelle résulte des actes de violence contre des cibles non combattantes » [15]), certaines actions du groupe relèvent en effet du cyber-terrorisme. A l'opposé, Dorothy Denning, en 2001, insiste sur le fait que les terroristes, même s'ils utilisent Internet, préfèreront toujours les bombes aux bytes [16] et sa définition de « dégâts sérieux » ne rejoint peut-être pas celle des « actes de violence » de Mark Pollitt.

Pour notre part, c'est effectivement l'échelle de violence qui accompagne l'acte militant qui nous permet de le qualifier, ou non, d'activiste ou d'hacktiviste. Citons à ce titre l'action activistes de certains yéménites qui luttent de façon non violente contre la politique des États-Unis et l'usage des drones pour éliminer les djihadistes d'AQAP (Al Qaeda in the Arabian Peninsula).

La question se pose donc de savoir si les Anonymous ou les autres entités que nous allons décrire maintenant quittent, ou non, la sphère hacktiviste lorsqu'ils mettent la main sur des documents militaires ou diplomatiques confidentiels (voire secret-défense) et les diffusent comme cela fut fait à plusieurs occasions par Wikileaks.

Les profils hacktivistes

Le terme d'hacktiviste cache bien des profils. Nous allons ici en détailler les quatre plus médiatisés.

Anonymous

Les plus nombreux se regroupent sous la bannière Anonymous. Leur militantisme coopératif est basé sur des équipes d'individus à la fois focalisées sur la défense de causes très diverses à caractère local ou liées à des mouvements globaux comme l'alter mondialisme ou la lutte contre la Scientologie. Ils sont rejoints par de nombreux militants « post--it » [17], activement engagés à certains moments, dormants à d'autres, mais restant informés (connectés) au groupe pour agir dès qu'un projet à défendre les galvanise. Anonymous est donc plus une idée qu'un groupe. C'est un réseau de réseaux qui se fait et se défait selon les projets et les opportunités.
Ce sont les opérations de soutien à WikiLeaks, en 2011, qui ont fait connaître Anonymous au grand public. Ils furent dès lors vus avec une certaine bienveillance par les uns alors que d'autres les considérèrent comme de nouveaux délinquants. Un an et demi plus tard, les dissensions internes et le manque d'objectifs clairs leur ont parfois fait perdre des

[14] http://www.20minutes.fr/ledirect/1079689/yemen-arrestation-deux-activistes-al-qaida
[15] http://www.cs.georgetown.edu/~denning/infosec/pollitt.html
[16] http://faculty.nps.edu/dedennin/publications/Cyberwarriors%20-%20Harvard.pdf

[17] http://www.cesep.be/ETUDES/ENJEUX/De%20l'activisme%20en%20ligne%20au%20militantisme%20de%20terrain%20_%20les%20nouvelles%20formes%20d'engagement%20Etude%20CESEP%202012.pdf (lire page 4)

sympathisants. De même, leur volonté absolue d'anonymat gêne certaines ONG qui aimeraient pourtant profiter de cette soif d'engagement parfois mal maîtrisée. Courte dans la durée mais parfois fort pénalisante les actions des Anonymous restent néanmoins toujours aussi nombreuses en 2013 qu'en 2011.

Pseudo cyber-armées

D'autres hacktivistes se retrouvent dans des groupes s'autoproclamant « cyber-armées ». Dans son premier rapport trimestriel de l'année 2013 [18], la société McAfee en liste 14 ayant mené des actions au cours des trois premiers mois de l'année. En voici la liste:

- 3xp1r3 Cyber Army (Bangladesh),
- Afghan Cyber Army,
- Alarakai Cyber Army (ils se dissent proche al-Qaeda),
- Armenian Cyber Army,
- Bangladesh Cyber Army,
- Brazilian Cyber Army,
- Indian Cyber Army,
- Iranian Cyber Army,
- Muslin Liberation Army (MLA),
- Pakistan Cyber Army,
- Philippine Cyber Army,
- Syrian Electronic Army (SEA),
- Tunisian Cyber Army,
- Turkey Cyber Army.

Les pays dont ces groupes sont originaires se retrouvent, comme tous les autres, classifiés dans le rapport de Reporters Sans Frontières au sein du classement mondial de la liberté de la presse. Dans ce rapport, le pays le mieux placé est au rang 1 (Finlande) et le dernier au rang 179. Si l'on excepte l'Arménie, tous les pays hébergeant ces cyber-armées se retrouvent à des rangs au-delà de 100. Et 9 sur les 13 ont un rang entre 138 et 176.
Il n'est donc pas faux d'affirmer que ces groupuscules fleurissent surtout dans des pays à tendances totalitaires et extrémistes.

Leurs membres sont des patriotes (authentiques ou manipulés) souvent qualifiés de cyber-guerriers. Ils prétendent agir au nom de leur gouvernement en soutenant généralement des thèses ultranationalistes. Leur réel engagement politique est souvent limité et leur idéologie confuse.
La frontière entre Anonymous et "cyber-armées" est néanmoins très poreuse, les premiers décidant parfois de soutenir un temps les seconds. Ce fut à plusieurs reprises le cas ces derniers mois à l'occasion du conflit Israélo-Palestinien [19].

Ces groupes mènent des attaques de « faible intensité » (attaques DDoS [20] éphémères, défacements de sites). Lorsque le niveau de technicité est important il nous semble plus raisonnable de les qualifier de cyber-terroristes (ou d'aide au terrorisme).

[18] Document non publié à l'heure j'écris ces lignes (j'en suis l'auteur).
[19] Opérartion Pilar of Defense - Anon déclare la "guerre" à l'IDF(Official Israel Defense Forces) rejoignant ainsi des groupe d'hacktivistes Pakistanias à tendance anti-Israel: http://www.cyberwarnews.info/2012/12/01/300-sites-hacked-by-anonymous-pakistan/
[20] DDoS (Distributed Denial of service / Déni de service distribué) : Attaque informatique ayant pour but de rendre indisponible à ses utilisateurs légitimes un service Internet. Elle peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web, empêcher la distribution de courriel dans une entreprise ou rendre indisponible un site internet.
Le déni de service (DoS) est provoqué par une seule source. Dans le cas d'une utilisation de machines réparties sur le réseau et formant, le plus souvent un botnet, l'attaque prend le nom de déni de service distribué.

Militants

Plus ancrés dans la vie que les Anonymous et à l'opposé des idées des cyber-guerriers en matière de liberté d'expression, on rencontre des militants plus réfléchis qui utilisent principalement Internet et les réseaux sociaux comme moyens de liaison et outils de propagande et de renseignement. Mi hacktiviste et mi cyber-activiste (selon qu'ils enfreignent ou non la loi), on trouve parmi eux des sympathisants des mouvements « Indignés » et« Occupy » qui ne reconnaissent plus la légitimité de la puissance politique et économique à laquelle ils sont soumis.
Le groupe Telecomix est un parfait exemple de cette double identité. Cyber-activiste, ils ont soutenu, depuis l'étranger, les révolutions arabes et sont proches, aujourd'hui, des opposants à l'aéroport de Notre-Dame des Landes. Hacktivistes, ils participaient, en 2010 aux campagnes de mirroring afin de remettre en ligne le site CopWatch après son interdiction d'accès à partir du territoire français [21]. Ils se moquent parfois des Anonymous qu'ils considèrent comme des gamins agités sans compétence technique.

En janvier 2013, des militants de la cause hacktiviste, possibles précurseurs des altermondialistes numériques de demain, initièrent une campagne en vue de promouvoir une légalisation pour un DDoS militant. Comparant le défacement à un affichage de banderole et le DDoS à un sit-in devant la porte d'entrée d'une entité qu'ils souhaitent bloquer, ils proposèrent d'instaurer, comme cela se fait avant une manifestation conventionnelle, un processus de déclaration préalable auprès des autorités : on spécifierait dans cette déclaration les dates, les cibles et les durées d'un blocage numérique. Laissant présager l'émergence d'ONG 2.0, discutable idéologiquement, mais respectable en nos démocraties, ils suggéraient l'émergence d'institutions déclarées, reconnues et établies sur Internet à même de prendre la tête de la protestation comme peut le faire un syndicat ou un parti politique dans la vie réelle. Une pétition qui n'a attiré que quelques milliers de signataires a d'ailleurs été déposée en ce sens sur le site de la Maison Blanche [22].

Opportunistes

Le mouvement hacktiviste compte aussi beaucoup d'opportunistes qui pratiquent le piratage et le défacement de site de manière totalement anarchique. Sous prétexte de faire passer un message ils ne semblent en fait intéressés que par l'aspect sportif ou quantitatif : le gagnant étant celui qui aura fait le plus beau hack ou qui aura défacé le plus de sites en un minimum de temps.

Conclusion

Après le soutien à Wikileaks, à la fin 2010, les grandes opérations lancées l'année suivante par les Anonymous (#OpSony, opération GreenRight, #Antisec, #OpCartel, etc.) portaient des idées libertaires. Elles eurent un certain succès et furent suivies, en 2012, de quelques autres opérations d'envergure, mais plus limitées dans le temps (#OpMegaUpload, opération Stop SOPA, #OpWcit, #OpWestBoroChurch, #OpAngel).

Depuis un an, nous sommes entrés dans une époque où la seule signature Anonymous est souvent délaissée. Et même si le slogan *« Nous sommes Légion. Nous ne pardonnons pas. Nous n'oublions pas. Redoutez-nous »* est toujours autant employé, ceux qui l'utilisent s'appliquent à signer leurs actes au nom d'un groupe ou d'une idéologie qu'ils souhaitent plus reconnaissable. Le simple masque de Guy Fawkes ne suffit plus : il faut rester anonyme mais se faire remarquer et pouvoir revendiquer clairement la responsabilité de ses attaques. Nombre d'actions représentatives lancées en 2013 (#OpIsrael, #OpUSA, #OpPetrol, etc.) sont de cet ordre. Utilisant l'imagerie créée par Anonymous,

[21] http://fr.scribd.com/doc/68777613/20111014-TGI-Paris-Copwatch
[22] http://www.01net.com/editorial/583847/anonymous-une-petition-pour-que-les-attaques-en-ddos-deviennent-legales/

elles sont l'œuvre d'individus agissant depuis le Moyen-Orient et l'Afrique du Nord dont les tendances djihadistes s'expriment clairement dans leurs communications.

Le mouvement hacktiviste se radicalise. Alors que les acteurs d'hier s'inquiétaient pour nos libertés, les mots d'ordre entendus aujourd'hui supportent des idéologies plus extrémistes et bien moins respectables. La voix du militant épris de liberté est recouverte par celle du cyber-guerrier. Cette nouvelle donne ne fait qu'amplifier les menaces qui pèsent sur nos démocraties qui doivent prendre très au sérieux ce nouveau paramètre.