Les partis politiques et les organisations activistes vont-ils bénéficier directement, commanditer ou conduire des actions criminelles dans le cyberespace perpétrées par eux-mêmes, des hacktivistes ou des réseaux cyber-maffieux ?

Par Pierre-Olivier Drai

Le milieu politique au sens large du terme[1] est réputé pour son âpreté et parfois pour ses relations complexes avec le milieu criminel. Parallèlement à cela, la « violence numérique[2] » se caractérise par son foisonnement de délits et de crimes et la multiplicité des acteurs. Dans cet article, nous nous interrogerons sur la rencontre entre ces deux univers et sur les perspectives possibles.

1. Etat des lieux

1.1 En principe, une séparation des genres…

À l'heure actuelle, le rapprochement entre « violence numérique » et milieu politique semble, dans le monde occidental, relever plus de l'exception que de la règle. Le monde politique se concentre principalement sur une utilisation « positive » des outils de communication disponibles pour diffuser des idées auprès des partisans, pour faire de la publicité ou bien pour répondre à des critiques (sites institutionnels et affiliés de partage de vidéos, de photos, de textes ; sites de campagne ; blogs et micro-blogging ; présence sur les réseaux sociaux ou dans les mondes persistants, 2nd Life). Cette séparation tient à deux principaux facteurs : la méconnaissance des milieux politiques du monde informatique et la non-nécessité d'un rapprochement à court terme avec les réseaux cybercriminels.

1.1.1 *Les acteurs politiques sont notoirement « à la traine » en matière de high-tech* ;

À l'exception de quelques personnalités ou organisations politiques, le degré de méconnaissance du monde politique avec celui de l'informatique est particulièrement flagrant. Plusieurs facteurs contribuent à cet état de fait :

- Âge et culture d'entreprise des dirigeants : L'exemple le plus fameux reste sans aucun doute celui de Tony Blair, alors Premier Ministre du Royaume-Uni, à la peine devant les caméras pour envoyer un email. Encore aujourd'hui, nombreux sont les élus ou membres du gouvernement qui envoient des SMS à caractère personnel ou prennent des photos sans aucune notion de sécurité de l'information.
- Nouvelle génération plus apte : La génération actuelle (Sarkozy, Obama, Royal pour citer les innovateurs) fait preuve d'une meilleure compréhension des outils disponibles, *cf.* l'utilisation de Twitter ou encore l'amélioration des campagnes sur Internet, mais elle demeure en-deçà de celle des « natifs numériques » (15-35 ans).
- Les « jeunesses » partisanes et les responsables IT : Dans ce paysage numérique un peu désolant, il faut se tourner vers les jeunesses partisanes et les responsables IT pour trouver un niveau de compétence plus adéquat. Ainsi, la présence d'une représentation du Front National dans le monde persistant de Second Life était une initiative du FNJ (Moselle) et la plateforme Désir d'Avenir de Ségolène Royal en 2007 avait été principalement pensée par les « jeunes » du PS. Par ailleurs, les responsables IT constituent un vivier d'expertise sous-employé.

[1] Pour les besoins de cet article nous définirons « politique » comme tout acteur qui agit de manière licite ou illicite dans la sphère publique au nom d'une « idéologie » ; cette définition inclut les partis politiques, les ONGs, les mouvements sociaux ou les organisations terroristes.

[2] Pour les besoins de cet article nous considérerons pêle-mêle l'ensemble des pratiques affectant la sécurité dans le cyberespace ; des plus bénignes (surveillance, lutte contre la censure) aux plus graves (attaques sur l'informatique des infrastructures sensibles). La classification traditionnelle : cybervandalisme, cybercriminalité / cyberdélinquance, cyberterrorisme / cyberguerre est volontairement omise.

Dès lors, il apparaît naturel qu'un usage licite soit privilégié.

1.1.2 *L'offre en matière de délinquance informatique excède largement celle du « Milieu »*

Les enseignements que l'on tire des affaires d'espionnage industriel ou d'espionnage politique mettent l'accent sur l'utilisation « d'officines » plutôt que sur une immixtion entre le milieu politique et la criminalité :

- Le coût, les technologies et les savoir-faire ne sont pas exclusivement détenus par la criminalité. Aussi, à offre égale, la tendance des milieux politiques est de passer par des canaux plus légitimes, quitte à commanditer des actions qui sont elles-mêmes illicites.
- La sphère politique a pour l'essentiel pris ses distances avec la grande criminalité (même si certaines affaires rappellent que des liens peuvent subsister). Il existe néanmoins une exception majeure à cette règle. En effet, les partis « révolutionnaires » de tous bords tendent à être également les acteurs de la criminalité (financement du terrorisme, gages territoriaux).

Dans ce contexte, la notion de séparation des genres politiques / criminels demeure d'actualité. Pourtant, cette première réponse doit être affinée en fonction du type de milieu politique et du pays dans lequel il est présent.

1.2 Affinement de la séparation des genres selon le type d'organisation

Au vu des nombreuses attaques (tous genres confondus) sur le réseau, la séparation des genres doit être affinée en fonction des acteurs et de leurs méthodes propres.

1.2.1 *Haro sur l'Etat, les entreprises, les rivaux* !

Depuis les 15 dernières années (1997-2012), on ne dénombre plus les attaques et incivilités perpétrées contre des acteurs politiques ou institutionnels dans le monde. Ces attaques idéologiquement motivées visent en premier l'Etat (institutions, agences, personnes), en second les entreprises (agroalimentaire, défense, pharmaceutique, information, etc.), enfin, les personnalités, partis ou organisations politiques. Ces attaques prennent différentes formes, résumées dans le tableau ci-dessous :

Argumentation	**Compromission**	**Interdiction**	**Intimidation**
Campagne positive	Collecte de renseignement (stalking, datamining)	Déni d'accès	Manipulation du vote
Publicité (agitprop)	Vol de données	Vandalisme	Bombs & bytes
Campagne de dénigrement (bullying, hate-site, liste)	Publication de données (datadump)	Mise au silence (hacking compte)	Extorsion, chantage
Pourriel	Transmission de données à des tiers		Virus
Désinformation	Usurpation d'identité		
Pollution débat (trolling, griefastrophe)			

Dans la typologie suivante, les organisations clandestines, les activistes et les partis d'extrême utilisent une rhétorique basée sur la relation du faible au fort. Le positionnement antisystème favorise un usage choc (ou pire) de l'informatique en plus d'un usage positif. En matière de réponse à ces attaques, nous nous limiterons à observer les réponses extérieures aux dispositifs de sécurité nationaux (police, gendarmerie, etc.).

1.2.2 *Organisations clandestines*

Acteurs : Indépendamment de l'idéologie promue, les organisations clandestines utilisent l'informatique comme une composante intégrale de leur action autant en termes d'**argumentation** (propagande, transmission des savoir-faire, *cf*. affaire El Aroud) qu'en termes d'**intimidation** (tentative de piratage des logiciels de contrôle des infrastructures, DCS, SCADA, *etc*. *cf*. propagation du virus « Vote » après les attentats du 11 septembre et tentatives d'intrusion 2001-2002).

Cibles : Certains hackers, dits « patriotiques », ont appelé à la lutte contre ces organisations avec des succès variés, concentrant leurs réponses sur l'**interdiction** et la **compromission** (fermetures de sites, publication de données, *cf*. affaires Jester, Raptor, 2012). À la différence d'autres organisations, les organisations clandestines ne reçoivent pas ou très peu de soutien de groupes d'hacktivistes extérieurs à la nébuleuse idéologique à laquelle ils appartiennent.

1.2.3 *Organisations militantes*

Acteurs : La quasi-totalité des associations et mouvances idéologiques utilisent l'informatique à des fins d'**argumentation** (campagne positive, agitprop, dénigrement). En revanche, il apparaît que des mouvements d'hacktivistes offrent leur soutien en parallèle et sans coordination préalable avec les organisations ou les mouvements. Ainsi, durant la crise des étudiants au Québec (2012), les Anonymous canadiens ont lancé une campagne d'**interdiction** (vandalisme) ; il en va de même avec le soutien offert par Anonymous à Greenpeace après les attaques contre les sites de compagnies pétrolières (**interdiction**, **compromission** – vandalisme, publication de données, 2012).

En outre, l'affaire WikiLeaks illustre comment une plateforme peut bénéficier du soutien d'hacktivistes en matière de **compromission** de l'information (transmission de données à un tiers).

Cibles : L'affaire EDF vs Greenpeace (2012) montre que certaines entreprises sont prêtes à passer par des officines pour espionner les organisations (vol de données, collecte de renseignements – **compromission**). Par ailleurs, il est important de souligner que l'activisme des hacktivistes rencontre également l'opposition d'autres hacktivistes qui procèdent à la **compromissions** des premiers (affaires Anonymous, Jester 2012).

1.2.4 *Partis d'extrême*

Acteurs : À la différence des organisations clandestines ou militantes, les partis d'extrême se cantonnent exclusivement à l'**argumentation** (campagne positive, agitprop, dénigrement, désinformation) et il semblerait qu'ils bénéficient de peu de soutien de la part de mouvances hacktivistes.

Cibles : En tant qu'acteurs de la scène politique traditionnelle, les partis d'extrêmes sont soumis au regard inquisiteur de la presse avec les risques de **compromissions** que cela comporte (collecte de renseignements, affaire des candidats du Front National, 2011). Par ailleurs, certains hacktivistes

prennent les partis d'extrêmes pour cibles à des fins de **compromission** (publication de données, affaires NDP, A3P, Blood & Honour, 2012) ou à des fins d'**interdiction** (déni de service, vandalisme, affaire Opération Blitzkrieg Hongrie, 2012).

1.2.5 *Micro-partis*

Acteurs : À la manière des organisations militantes, les micro-partis misent sur la visibilité qu'offrent la Toile et les outils modernes pour exister avec un financement minimum. Leur action se cantonne principalement à de l'**argumentation**. Il conviendra de voir cependant comment des partis tels que le Parti Pirate, émanation politique du site The Pirate Bay condamné pour violation de copyrights se comportera dans les années à venir. Ce parti sera d'autant plus intéressant à suivre que nombre d'hacktivistes soutiennent l'idéologie du Parti Pirate.

1.2.6 *Partis dits* « de gouvernement » *ou* « majoritaires »

Acteurs : Enfin, à l'opposé du spectre informatique se trouvent les partis de gouvernement dont la présence informatique, souvent simpliste, sert exclusivement à des fins d'**argumentation** (campagne, dénigrement).

Cibles : En revanche, ces partis se caractérisent aussi par la fréquence des attaques subies. En France, au Royaume-Uni, aux Etats-Unis, en Australie et très vraisemblablement partout ailleurs, ces partis font l'objet de manœuvres d'**interdiction** (vandalisme, déni de service, usurpation d'identité, *cf.* Nouvelle Galles du Sud, Ségolène Royal, *etc.*). Etonnement, la publication de données de membres des partis majoritaires n'est pas documentée.

1.3 Affinement par type de lieu

Les exemples précités étaient exclusivement focalisés sur le monde occidental où les libertés individuelles sont essentiellement garanties et où, dans l'ensemble, le « jeu » démocratique est respecté par l'ensemble des acteurs. En dehors du monde occidental, la révolte numérique est également porteuse de changements contre des régimes répressifs.

1.3.1 *La dissidence politique en milieu répressif*

Dans un environnement politique répressif la dissidence informatique revêt des accents différents et, au premier chef, sert de moyen de lutte contre la censure. Malgré l'éloignement géographique relatif, les techniques de contournement de la censure et de mobilisation politique constituent des enseignements qui pourraient, à terme, être appliqués dans le monde occidental.

Sans rentrer dans l'histoire des moyens de lutte contre la censure, nous nous bornerons simplement à mentionner ici à titre d'exemple le serveur Picidae (Pivert) mis au point durant la décennie passée. Les solutions technologiques couplées à l'enseignement des tactiques de campagne online via les médias sociaux (*Robert Kennedy Center for Justice and Human Rights* à Florence) permettent aux oppositions locales d'exister sans (trop) se dévoiler.

1.3.2 *Là où tous les coups sont permis*

Parallèlement à cela, d'autres environnements politiques profitent de la faiblesse des moyens gouvernementaux ou du manque de respect de l'Etat de droit pour développer des pratiques insidieuses. La mise au silence de candidats au travers du hacking des boîtes emails ou de divers comptes est observée dans plusieurs pays (Tunisie, Côte d'Ivoire, …).

2. Perspectives

2.1 Les facteurs de radicalisation dans le monde occidental

L'environnement informatique actuel est susceptible de connaître une aggravation à court et à moyen terme en raison des facteurs de radicalisation en cours. La crise économique, le repli identitaire, le renouveau des « internationales » et les parcours des hacktivistes sont autant d'éléments appelés à peser sur l'environnement informatique.

2.1.1 La crise économique

Par le climat anxiogène qu'elle produit, la crise économique est un important facteur de radicalisation et générateur d'un certain désespoir social. En conséquence, elle amplifie fortement les mouvements sociaux, le soutien apporté par Anonymous Canada aux étudiants québécois (opération Québec) illustre comment les mouvements sociaux risquent de se propager dans le cyberespace.

2.1.2 Le repli identitaire

Le repli identitaire (montée des communautarismes, régionalismes, populismes) s'accompagne d'une montée des confrontations idéologiques et parfois physiques au sein de la société. Ainsi, à la manière des organisations militantes ou des partis d'extrême, le besoin de publicité, couplé à un sentiment « patriotique » est susceptible de pousser un certain nombre d'organisations à des « actions d'éclat ». Déjà, des groupes comme le Bloc Identitaire n'hésitent pas à mener des actions « choc » et le cyberespace pourrait constituer un terrain fertile pour d'autres actions.

2.1.3 Le renouveau des « internationales » et de la stratégie du faible au fort

En vertu des moyens de communication actuels, les mouvements idéologiques disposent d'une facilité accrue pour se constituer en « internationales ». À cet égard, il est nécessaire de souligner la proximité des techniques d'information et d'organisation entre les altermondialistes (Seattle, 2000) et les bloggeurs / activistes des « Révolutions Arabes » (2010). Les mouvements des Stagiaires (France, 2006), des Anonymous ou encore celui des Indignés / Occupy ont pu se constituer en « internationales » très promptement. Ces mouvements illustrent par ailleurs le sentiment de vulnérabilité de la population face à des changements difficiles et cultivent une vision activiste basée sur une relation du faible au fort (l'Etat, la classe politique, les entreprises) justifiant l'action.

2.1.4 Des parcours multiples

Enfin, le parcours des hacktivistes est lui-même susceptible d'introduire un certain degré de confusion. Ainsi, au vu des charges retenues contre ceux qui ont été arrêté, il est intéressant de voir comment certains entretiennent une confusion des genres. Nonobstant les délits commis dans le cadre de l'idéologie défendue, les autres charges ou motivations sont révélatrices (enrichissement personnel ou vol de marchandises : cyber-criminalité ; motivations patriotiques : « hackers patriotiques » ; motivations sociales : appartenance à des mouvements comme Occupy).

2.2 Coût, technologies, savoir-faire toujours plus disponibles

Au-delà des facteurs de radicalisation, l'accès aux technologies et aux savoir-faire va croissant. À mesure que la société se familiarise avec les outils de sécurité informatique (offensifs comme défensifs) et que ces derniers font l'objet d'une promotion renforcées (Les cahiers du pirate par ex.), le recours à des actions d'éclat accroît proportionnellement (ainsi des script-kiddies qui aiment à se donner des frissons).

2.3 La difficulté de l'attribution des attaques et la pertinence des outils de forensic

Déjà aujourd'hui, et plus encore à l'avenir, la multiplication des acteurs et des modes d'opérations est susceptible de rendre difficile l'exacte attribution des attaques. Certaines peuvent être revendiquées par des acteurs extérieurs souhaitant en recevoir le crédit, tandis que d'autres attaques peuvent servir à faire « porter le chapeau » à un groupe adverse. Dans ce contexte, les décideurs futurs devront être particulièrement vigilants et les domaines de *computer forensic* et d'expertise judiciaire seront appelés à jouer un rôle encore plus important.

2.4 Aux risques habituels « on land » …

Ainsi, il est d'ores et déjà possible d'identifier un certain nombre de risques futurs ; calques des risques physiques déjà existants et émanations des tendances à la radicalisation contemporaines. La vague de vandalisme des locaux du PS français (oct.-nov. 2012) pourrait aisément s'accompagner d'un cybervandalisme (déni d'accès, site du PS).

Les cambriolages répétés de locaux politiques ou d'appartements de personnalités politiques (Ségolène Royal) ne sont pas sans rappeler les vols de données coutumiers du cyberespace. Un varia sur ce thème se trouve à la confluence d'actions de terrain (Faucheurs d'OGM) et de soutien hacktiviste (hacking de Monsanto et subséquent datadump), créant des alliances objectives.

2.5 … S'ajoutent des risques majeurs

Sans prétendre à l'exhaustivité, nous pouvons par ailleurs identifier quatre familles de risques majeurs propres au cyberespace sur la base d'éléments déjà existants qu'il faudra ajouter aux risques habituels.

2.5.1 Glissement de la frontière vie publique / vie privée

Jusqu'à présent, le rétrécissement de la frontière entre vie publique et vie privée profitait principalement aux cyber-stalkers, détectives privés, paparazzis. Désormais, la continuation de cette pratique ne manquera pas de fournir des éléments toujours plus nombreux aux différents adversaires politiques. Le refus du « droit à l'oubli » constitue un recours particulièrement efficace pour tenter de discréditer un adversaire (affaire Colleen Lachowitz, 2012). Cette tendance semble encore aggravée par le fait que la jeune génération (15-25 ans) semble totalement mépriser le contrôle de son image (*cf*. les habitudes de « sexting » et les produits d'assurance pour effacer les traces) malgré les graves risques encourus (chantage, suicide). La génération appelée à être prochainement élue devra veiller à ne rien laisser traîner sur la Toile.

2.5.2 Manipulation du vote

Plus préoccupant pour la société dans son ensemble, la question de la sécurité du vote électronique (et *a fortiori* lorsqu'il est réalisé à distance) est appelée, tôt ou tard, à susciter l'interrogation sur l'exactitude ou le trucage des résultats. Les élections législatives françaises pour les Français de l'Etranger (2012) ont donné lieu à une démonstration d'*exploit* dans le logiciel permettant d'altérer le vote ; lors des élections américaines de 2012, les failles dans les systèmes électroniques en Ohio et dans le New Jersey ont été mise à jour. Dans ce contexte, la probabilité d'une action malicieuse à moyen terme semble plus que possible et certainement tentant pour un groupe marginal.

2.5.3 Disruption ou actes de violence

Enfin, les enseignements informatiques de la crise russo-estonienne de 2005 sont nombreux. L'étendue des attaques (DDoS et vandalisme) sur les sites institutionnels estoniens (gouvernement, banques, etc.) a été telle que le gouvernement estonien a voulu y voir un réel acte de « cyberguerre » (au point d'en appeler au soutien de l'OTAN). Les tentatives d'accès des logiciels de SCADA ou de DCS rappellent combien certaines infrastructures peuvent intéresser des terroristes. De là à imaginer que des groupes militants clandestins ou non souhaitent s'essayer à un terrorisme informatique, il n'y a qu'un petit pas. En réalité, ce pas a déjà été franchi avec ou sans la donnée idéologique. En 2006, à la suite de la panne d'électricité en Californie, un hacker s'est introduit dans le système de Cal-Iso, en Australie, un hacker écologiquement motivé a procédé à une pollution par des eaux usées (2001) et en Pologne, plusieurs trains ont été détournés par un jeune hacker avec pour conséquences le déraillement de quatre d'entre eux et 12 blessés (2008).

2.6 Et le risque d'atteintes à la personne

2.6.1 Insuline, Pacemaker, RFID

Une dernière catégorie de risque pouvant être idéologiquement motivée est l'atteinte aux personnes. Si la publication d'adresses, de téléphones ou d'emails de militants peut conduire à des règlements de compte, alors il ne faut pas exclure le risque posé par un ciblage spécifique sur les personnes. La technologie médicale allant vers une plus grande informatisation, un certain nombre de vulnérabilités deviennent apparentes. Un chercheur britannique porteur d'une puce RFID s'est lui-même contaminé avec un virus informatique pour vérifier si c'était possible et, récemment, l'alerte a été donnée sur les vulnérabilités des pompes à insulines ou de certains pacemakers. Porter atteinte au bon fonctionnement de l'un ou l'autre appareil reviendrait à commettre un meurtre.

FIN.