# Oups, vos élections ont été piratées ! Vraiment ?

Martin Untersinger
untersinger@lemonde.fr

Le Monde

L'onde de choc du piratage contre le Comité national démocrate (DNC), révélé au printemps 2016, ne s'est toujours pas dissipée. Son caractère remarquable ne provient pas de ses caractéristiques techniques mais plutôt de la manière dont il a surgi dans le champ politique, institutionnel et diplomatique en y modifiant la perception de la menace informatique. Il a donc représenté, pour le journaliste spécialisé en sécurité informatique une série de questions et de défis nouveaux.

Le point de vue développé ici ne sera pas celui d'un juriste spécialisé en droit international ou en géopolitique, ni celui d'un diplomate ou d'un haut fonctionnaire, pas plus que celui d'un expert technique. Il sera celui d'un journaliste, placé mécaniquement aux confluents de ces trois positions. Ce point de vue, s'il a le défaut de ne pouvoir réellement permettre une position d'expertise sur les trois domaines, a le mérite d'éclairer les épisodes de ces derniers mois, qui ont été, eux aussi, à la confluence de la technique, de la géopolitique et de la politique.

De ce point de vue, la couverture de cette attaque et de ses suites a nécessité de dépasser le simple champ technique de la sécurité informatique. D'un côté, l'attaque ne pose pas de défi technique particulier pour le journaliste spécialisé. Mais elle a rapidement posé une difficulté assez inédite en ce qu'elle a immédiatement dépassé le champ purement technique. Elle a provoqué un vent de panique dans les chancelleries occidentales, a servi d'outil de communication pour certaines personnalités politiques françaises et s'est inscrite dans un moment géopolitique et médiatique complexe. Si la compréhension technique des événements était nécessaire, elle n'était pas suffisante. Il a fallu, sans doute pour la première fois à ce niveau de médiatisation, recourir à d'autres outils que la seule grille de compréhension technique pour suivre cette affaire, ce qui a posé une série de questions, anciennes et nouvelles, pour les journalistes couvrant la sécurité informatique.

# 1 Comment le piratage du Democratic National Committee a dépassé le seul cadre technique

## 1.1 Aux États-Unis

### Piratage du DNC, techniquement basique

Au printemps 2016, la firme Crowdstrike est appelée par le Comité national démocrate (DNC), l'organe central du parti politique américain, pour enquêter sur une potentielle intrusion dans ses systèmes [1]. Elle y découvre deux groupes d'assaillants, Cozy Bear et Fancy Bear, bien connus des experts en sécurité informatique. Le premier a pénétré dans le réseau dès l'été 2015, rejoint par le second en avril 2016. Le rapport de Crowdstrike souligne la très grande sophistication technique des outils déployés par les attaquants et disent avoir identifié « des méthodes avancées correspondant aux capacités d'un État » [1]. Mais pour qui suit ces deux groupes, étudiés depuis des années, ça n'est pas vraiment une surprise. La gravité de l'intrusion résulte moins des capacités offensives des attaquants et de la technicité de l'intrusion que d'une succession d'erreurs humaines qui en a aggravé les conséquences.

Une fois à l'intérieur du réseau, les équipes techniques du DNC n'ont pas mené la vie dure à ces deux groupes. Malgré plusieurs appels du FBI, qui repère Cozybear dès le mois de septembre 2015, le technicien (sous-traitant) ne réagit pas car il pense être victime d'un « canular », selon un mémo interne récapitulant les échanges entre le DNC et les autorités que s'est procuré le New York Times [2]. Plusieurs mois passent : dans l'intervalle, le FBI contacte à plusieurs reprises le DNC, lui demande de prendre des mesures, et l'avertit en novembre de la communication de données vers l'extérieur, sans succès [2]. Symétriquement, le FBI ne montre guère de zèle : aucun agent ne se déplace en personne au DNC pour les alerter alors que leurs bureaux sont tout proches [2] et qu'il s'agit d'un organisme critique pour les élections américaines à venir. De surcroît, les défenses informatiques mises en place à l'époque étaient faibles, notamment à cause d'un manque de moyens. Le DNC était équipé d'un filtre anti-spam standard et ce n'est que mi-avril, sept mois après la première alerte, qu'ils ont installé « des outils robustes » [2].

Le 22 mars, le deuxième groupe d'assaillants pénètre dans le DNC par le biais d'un e-mail de hameçonnage. Il rentre aussi, le 19 mars, dans la boîte mail de John Podesta, directeur de campagne d'Hillary Clinton, suite à une erreur de frappe du technicien à qui le courriel a été soumis [2].

Bref, on a rapidement fait le tour des évènements techniques. Mais ce piratage prend rapidement un tour très différent.

### Publication des documents

Le 14 juin, le Washington Post révèle [3], citant Crowdstrike et le DNC, que des « pirates gouvernementaux russes » ont pénétré les réseaux du parti démocrate. Dès le lendemain, un individu utilisant le nom de Guccifer 2.0 et se présentant comme le pirate du DNC publie certains documents internes [4] et annonce avoir confié le reste à WikiLeaks. Il affirme être un « pirate solitaire » et nie tout lien avec la Russie. En juin, le site DCLeaks apparaît en ligne et commence à publier certains documents [2]. Enfin, le 22 juillet, WikiLeaks publie ce qui semble être l'intégralité des documents issus du DNC [5]. Le 7 octobre suivant, le site commence à publier les courriels de John Podesta [6]. Wikileaks a toujours dit que leur source n'était pas les services russes [7].

C'est un stade crucial dans ces événements : l'espionnage d'une campagne politique est une chose, condamnée mais admise ; la publication du fruit de cet espionnage est beaucoup moins courant et n'a pas du tout le même poids politique et diplomatique. D'un côté, les agences de renseignement font ce pour quoi elles sont payées, anticiper et informer le pouvoir politique ; de l'autre, elles ont un impact direct sur la réalité et influencent, dans les faits, le scrutin. Ces courriels sont-ils issus du piratage du DNC et de la boîte e-mail de M. Podesta ? Ce piratage a-t-il été mené ou piloté par les services russes ? C'est tout l'enjeu de la séquence qui s'ouvre alors.

### Attribution par les autorités, un processus lent et politique

Ce n'est que plusieurs mois après le piratage que les autorités ont officiellement mis en cause la Russie. Mais la lenteur de ce processus n'a que peu à voir avec la difficulté technique de l'attribution. Elle s'explique plutôt par les lourdes implications diplomatiques et politiques d'une telle accusation.

Dès la fin du mois de juillet, des membres des services de renseignement évoquent anonymement dans la presse une responsabilité russe. On parle alors d'espionnage, pas de tentative d'influence [8]. Au même moment, le DNC pousse les autorités à faire une attribution publique. Selon le New York Times, le directeur de la NSA, l'amiral Rodgers, était en faveur d'une riposte [2]. Mais les autorités rechignent : reconnaître officiellement qu'un État s'en prend à votre processus électoral, c'est jeter le discrédit sur ce dernier, chose que ne pouvaient se permettre les autorités américaines à seulement quelques semaines de l'élection. Par ailleurs, Obama a expliqué qu'il avait peur que cela pousse l'État russe à s'en prendre au système de vote [9], largement électronique aux États-Unis.

Le 5 septembre, Barack Obama fait finalement une allusion sibylline, mais notable, aux événements [10]. « Nous avons eu des problèmes avec des cyberintrusions de la Russie, et d'autres pays, dans le passé. Et, vous voyez, on se dirige vers une nouvelle ère où plusieurs pays vont disposer de capacités importantes. Et franchement nous avons des capacités plus importantes que quiconque, offensivement et défensivement » déclare le président américain en marge du G20, en Chine. Tous les experts de la diplomatie « cyber » sont unanimes : ce message n'est pas anodin, c'est un signal clair adressé à la Russie.

Le 7 octobre, le même jour que la publication par WikiLeaks des courriels de John Podesta, le département de la sécurité intérieure (DHS) et le directeur du renseignement national (DNI), l'instance qui chapeaute les agences de renseignement américaines, publient un communiqué [11] dans lequel ils estiment être « assurés que le gouvernement russe a dirigé la récente compromission d'e-mails de personnes et d'institutions américaines, y compris d'organisations politiques », afin « d'interférer avec le processus électoral ». C'est la première fois que le pouvoir américain désigne clairement la Russie, mais le contraste avec l'attribution, par Barack Obama, très solennellement, en direct à la télévision, à la Corée du Nord de l'attaque contre Sony Pictures [56], est frappante. La situation est très différente, et cela se voit.

Le 29 décembre, Barack Obama décide de prononcer des sanctions [12]. Le GRU (renseignement militaire), le FSB (renseignement intérieur), trois entreprises ou organisations et plusieurs cadres du GRU sont visés. Aleksey Belan et le fameux Evgeniy Bogachev [13] sont également sur la liste des sanctions, mais le lien avec le piratage du DNC est loin d'être clair, notamment parce que c'est le département du Trésor qui est à l'origine de leur inscription sur cette liste. Par ailleurs, Obama prononce l'expulsion de 35 diplomates russes et la fermeture de deux bâtiments appartenant à la Russie, mais là encore le motif n'est pas l'interférence dans l'élection, mais le traitement réservé à Moscou aux diplomates américains, contrairement à ce qu'ont écrit de nombreux médias.

Ce n'est que le 6 janvier, après l'élection mais avant la prise de pouvoir de Donald Trump, que la direction du renseignement publie un rapport, nourri par le FBI, la NSA et la CIA [14]. Ses conclusions ne font guère de place aux éléments techniques, mais sont très claires et sans précédent :

> « Nous avons établi que le président russe Vladimir Poutine a ordonné une campagne d'influence en 2016 visant la campagne électorale américaine. Les objectifs de la Russie étaient de nuire à la confiance du public dans le processus démocratique, de dénigrer

> Hillary Clinton, et de saper sa capacité à être élue et, potentiellement, à présider. Nous estimons également que Poutine et le gouvernement russe ont développé une préférence claire pour le président Trump [et qu'ils] aspiraient à contribuer à [son] élection en discréditant M$^{me}$Clinton. »

Selon ce rapport, les opérations du Kremlin sont allées au-delà du simple piratage. « La campagne menée contre les élections américaines comportait des publications de données, des intrusions dans les comités électoraux au niveau local et de l'État ainsi que de la propagande ». Il fait ainsi référence aux médias russes d'État ainsi qu'à un « réseau de trolls ».

Le 29 décembre [15], puis le 10 février [16], le CERT US publie lui aussi deux rapports : s'il ne s'agit pas d'attribution, puisque ces deux documents font successivement référence au communiqué d'octobre et au rapport de janvier, ils détaillent les activités des deux groupes retrouvés dans les réseaux du DNC (IOC, recommandations...) et font clairement le lien avec la Russie. Ils n'apportent cependant guère d'éléments techniques nouveaux.

### Mais pas de piratage du vote en lui-même

Assez rapidement, on observe un glissement chez certains politiques et certains médias. D'une campagne d'influence, organisée suite à un piratage sur les systèmes d'un parti politique, on tend à décrire une opération destinée à altérer les votes eux-mêmes. S'il existe un vaste faisceaux d'indices concordants pointant du doigt la Russie dans le piratage du DNC et des courriels de John Podesta, il n'existe aucun élément permettant de dire que le système de vote a été attaqué ou altéré.

Dans leur rapport, le FBI, la CIA et la NSA écrivent d'ailleurs qu'ils n'ont « pas évalué l'impact que les activités russes ont eu sur le résultat des élections ». Les trois services indiquent cependant que les services russes se sont introduits « dans des éléments de multiples organismes électoraux locaux et au niveau des États » mais que « les systèmes visés par les acteurs russes n'intervenaient pas dans le décompte des votes ».

La crainte n'est cependant pas dénuée de fondement, les États-Unis recourant massivement aux machines à voter, dont la faible résistance aux attaques n'est plus à démontrer. Même si aucun recompte d'ampleur n'a été ordonné après le résultat de l'élection de novembre, des chercheurs ont audité les résultats dans trois États. Cette analyse, pour différentes raisons, est restée très partielle, mais elle a conduit les experts, parmi les

plus qualifiés en matière de vote électronique, à écarter avec certitude l'hypothèse d'une manipulation d'ampleur [17].

### 1.2 En France, les politiques s'emparent du sujet

L'onde de choc du piratage du parti démocrate n'a pas tardé à atteindre la France. La situation a ceci de particulier qu'à la différence des États-Unis, aucun événement notable destiné à influencer l'élection ne semble avoir eu lieu à l'heure où nous écrivons ces lignes.

Sur la base d'une dizaine d'entretiens réalisés ces derniers mois avec plusieurs responsables et haut fonctionnaires chargés de ces questions, il est possible de situer au début de l'automne, alors que les responsables américains commencent à se faire plus précis dans leurs accusations, le moment où les responsables français commencent à s'interroger sur une éventuelle interférence russe dans les processus électoraux à venir en France.

Cette prise de conscience se traduit d'abord par l'organisation, le 26 octobre, par l'Agence nationale de sécurité des systèmes d'information (ANSSI), d'un séminaire destiné aux partis politiques [18]. Selon plusieurs sources, il s'agit essentiellement de sensibilisation plus que de formation. Le niveau technique des participants est variable, selon le poste et les responsabilités de la personne qui s'est déplacée. Les niveaux de vigilance et de préparation sont, eux aussi, très variables.

#### Déclarations de MM. Hollande et Ayrault

C'est dans ce contexte que la question des attaques informatiques est pour la première fois évoquée au plus haut niveau de l'État. Le communiqué publié après le Conseil de défense organisé le 15 février aborde le sujet [19]. Lors du Conseil restreint de défense du 1er mars, un point sur les mesures de protection informatique autour de l'élection est présenté [20].

> « [Le président] a pris acte des mesures de protection supplémentaires prises sur les systèmes informatiques impliqués dans les opérations électorales. Afin qu'aucune action malveillante ne puisse venir entacher la campagne et le vote, le Président de la République a demandé une mobilisation de tous les moyens nécessaires de l'État. »

Mais les déclarations les plus intéressantes, témoignant de l'inquiétude des autorités, sont celles de Jean-Marc Ayrault, le ministre des affaires étrangères, dans l'hémicyle de l'Assemblée nationale [21]. Le 15 février, ce

dernier déclare que la France « n'acceptera aucune ingérence (...) dans [son] processus électoral », « pas plus de la Russie d'ailleurs que tout autre État, il en va de notre démocratie, il en va de notre souveraineté, il en va de notre indépendance nationale » :

> « [Il faut] faire clairement connaître les limites à ceux qui seraient tentés de porter atteinte à ce principe de la non-ingérence et le faire clairement et y compris en prenant des mesures de rétorsion lorsque cela est nécessaire, car aucun État étranger ne peut influencer le choix des Français, aucun État étranger ne peut choisir le futur président de la République. »

Cette déclaration, qui utilise les termes de « souveraineté », « d'indépendance nationale » et de « rétorsion » n'est pas un effet de manche : elle fait partie de la stratégie de dissuasion que tente de construire la France, et témoigne du fait que les dirigeants français prennent alors cette affaire très au sérieux.

### Annulation du vote électronique

Autre moment important témoignant de la tension institutionnelle autour des piratages, l'annonce, le 6 mars, par le secrétaire d'État chargé des Français de l'étranger, Matthias Fekl, du renoncement au vote électronique, disponible aux élections législatives pour les 1,3 million de Français inscrits sur les listes consulaires depuis 2012, en raison du « niveau de menace extrêmement élevé de cyberattaques » [22].

Cette décision a été prise après deux audits, en décembre 2016 et en février 2017 [23] qui ont convaincu l'ANSSI de rendre un avis défavorable. C'est principalement la perspective d'une attaque en déni de service, à laquelle la plateforme de vote était particulièrement sensible, qui a motivé cette décision. Même si cela ne touche pas le décompte des votes en lui-même, ce type de nuisance aurait eu « un impact important sur l'image du fonctionnement de la démocratie » selon les termes de Guillaume Poupard, le directeur de l'ANSSI [24].

Lors du second audit a été découvert une fuite de données issue d'un test réalisé par les équipes du prestataire responsable du développement de la plateforme. Ces données étaient susceptibles, sinon de permettre l'entrée, du moins de faciliter la tâche d'attaquants désireux de pénétrer dans le système. Au final, l'ANSSI a rendu un avis défavorable quant à la mise en œuvre du vote électronique.

### Macron affirme être attaqué

Dernier épisode symptomatique du débordement du sujet des attaques informatiques dans la sphère politique, les accusations formulées par le mouvement d'Emmanuel Macron. Le 14 février, le secrétaire général de En Marche !, Richard Ferrand, publie une tribune dans Le Monde [25], accusant la Russie de peser sur la campagne électorale française.

Le responsable cible les déclarations de Julian Assange, qui selon lui a laissé entendre qu'il disposait d'informations concernant M. Macron ; les médias d'État russes publiant de fausses informations ; et les comptes sur les réseaux sociaux qui les « relaient massivement ». Mais il estime également que le site de son candidat est attaqué. Il livre des explications pour le moins floues :

> « Le site internet du mouvement En marche ! et ses infrastructures font l'objet de plusieurs milliers d'attaques mensuelles sous diverses formes. L'objectif est de pénétrer dans nos bases de données et nos boîtes mail afin de les pirater. Ces attaques proviennent principalement d'Ukraine, pour près de la moitié d'entre elles. Ce qu'indique de manière certaine la nature de ces attaques, c'est qu'elles sont organisées et coordonnées par un groupe structuré, et non par des hackers solitaires. »

Interrogé dans un second temps [26], Mounir Mahjoubi, le responsable de la campagne numérique d'Emmanuel Macron apporte un éclairage sur ces accusations. On comprend alors qu'il s'agit d'« attaques » communes pour un site Web public (déni de service, tentatives d'injections SQL, scans de ports...), même si M. Mahjoubi fait perdurer le flou en estimant que certaines attaques « sont plus intelligentes, mais beaucoup plus rares et beaucoup plus dangereuses, notamment des tentatives de connexion à nos bases de données ».

Une visite dans les locaux de En Marche ! et un long échange avec les responsables techniques de la campagne ne dissiperont pas l'impression que cette tribune était surtout une opération de communication, même si « le volume [d'attaques] est ridicule [à savoir disproportionné] par rapport aux données dont on dispose », selon le principal technicien de la campagne, ancien employé d'une entreprise très réputée dans le milieu (avec qui nous avons pu nous entretenir à la condition de ne pas dévoiler son identité) [27].

## 1.3 Ailleurs

Ce contexte n'est pas propre à la France.

### Accusations en Allemagne

Le 7 décembre, Hans-Georg Maassen, le chef du renseignement intérieur allemand a déclaré dans une interview qu'il existait « de plus en plus de preuves de tentatives d'influence de l'élection fédérale » et de la conduite de « cyberespionnage agressif » contre les politiques allemands [28, 29]. Lors d'une conférence, un responsable du renseignement intérieur avait révélé que la Russie avait entrepris des « mesures actives » pour influencer l'opinion publique [30] et Angela Merkel avait dit lors d'une conférence de presse que des piratages destinés à influencer la politique allemand étaient « possibles » [30]. Les autorités avaient déjà indiqué que le groupe APT 28 était derrière le piratage des systèmes du Bundestag [31].

On atteint même une forme d'affolement au lendemain d'une panne d'Internet et de téléphone qui a touché près d'un million d'Allemands [32]. « Des attaques comme celle-ci, les conflits hybrides comme les qualifie la doctrine russe, font désormais partie de la vie quotidienne, et nous devons apprendre à les gérer » a déclaré à ce sujet Angela Merkel [33]. Peu après l'attaque, interrogé dans la Süddeutsche Zeitung [28] sur la perspective d'une ingérence étrangère dans les élections, le chef du renseignement extérieur avait expliqué que « des cyberattaques sont lancées dans le seul but de provoquer de l'incertitude politique. [...] Ces tentatives d'interférence se concentrent sur l'Europe et sur l'Allemagne en particulier. Une forme de pression s'exerce sur le discours public et sur la démocratie, ce qui est inacceptable ».

Selon Deutsche Telekom, l'attaque viendrait d'une tentative d'enrôler certains de ses matériels à un botnet [34], peut-être le fameux Mirai [35] et en février, un individu a été arrêté à l'aéroport de Luton, à Londres [36], et le lien avec la Russie semble avoir été écarté.

### Inquiétudes ailleurs en Europe

Au Royaume-Uni, le chef du MI6, lors d'une conférence de presse en décembre 2016, a déclaré que la guerre hybride et les États « utilisant des moyens aussi variés que les cyberattaques, la propagande ou la subversion du processus démocratique » représentaient une menace pour le pays. Si la Russie n'a pas été explicitement mentionnée, l'allusion était très claire [37]. Le Government Communications Headquarters (GCHQ) a contacté en mars les partis politiques pour les sensibiliser aux risques de piratage [38]. Selon la presse britannique, c'est la perspective de piratages venus de Russie qui a motivé cette alerte [39]. Toujours de l'autre côté de la Manche, un rapport parlementaire publié le 12 avril [40] avance

comme explication de l'indisponibilité du site d'inscription sur les listes électorales, peu avant le référendum sur le maintien du pays dans l'Union européenne, une attaque en déni de service, dont la Russie aurait pû être à l'origine. Aucune preuve formelle n'est avancée et l'auteur du rapport reconnaît lui-même ne fournir que des « preuves indirectes » [41]. Un autre rapport, gouvernemental celui-là, attribuait l'indisponibilité au trop grand nombre de connexions simultanées, mais légitimes, sur le site.

Enfin, aux Pays-Bas, les pouvoirs publics ont décidé de renoncer au vote électronique lors des élections générales de 2015 en raison des menaces de piratage [42].

Bref, des États-Unis à l'Europe, de la sphère technique au monde politique et institutionnel, les questions de la sécurité informatique et du « piratage » des élections ont été posées dans de nombreux domaines.

## 2 Comment raconter l'histoire : les enjeux liés à la couverture journalistique de cette affaire

### 2.1 Peu de faits rigoureusement établis

#### Les principales questions

De nombreuses questions doivent être posées pour établir ou non la réalité de la tentative russe d'interférer avec les élections américaines. Pour des raisons de simplification, d'autres ont été plus exhaustifs [43], nous n'en retiendrons que trois, très schématiques :

- Le régime russe est-il à l'origine des piratages du DNC et de Podesta ?
- Le cas échéant, est-ce le régime russe qui a fait fuiter les documents ?
- Le régime russe a-t-il mené une campagne de propagande et de manipulation des réseaux sociaux ?

**Le régime russe est-il à l'origine des piratages ?** La réponse à la première question ne sera jamais définitivement établie, les difficultés de l'attribution technique étant bien connues. Le doute ne semble en revanche guère permis sur l'implication ou non de APT 28/29 (ce qui n'est pas la même chose que « le régime russe » ou « la Russie ») dans le piratage du DNC. Les activités d'APT 28/29 font partie des phénomènes les plus étudiés en matière de sécurité informatique. Pas moins de treize entreprises ont consacré 31 analyes à APT 28/29, selon le décompte établi en début d'année par le CERT US [16] : il s'agit donc de groupes dont les outils, les méthodes et les infrastructures commencent à être très bien connues.

Outre CrowdStrike, FireEye et Fidelis ont abouti à la même conclusion après analyse des échantillons du malware retrouvé sur les réseaux du DNC [44]. Entre autres indications, l'adresse IP d'un C&C utilisée dans l'attaque du Bundestag (APT 28 [45]) a été retrouvée hardcodée dans le malware du DNC et les deux attaques partageaient un même certificat SSL [46].

Ce qui amène une seconde question, APT 28/29 sont-ils des groupes d'espionnage étatique russes ? Rien ne le prouve à ce stade. Cependant, le faisceau d'indices, à la fois épais et ancien, d'un lien fort entre APT 28/29 et l'État russe rend cette hypothèse très crédible. Sans lister l'intégralité des éléments, la localisation et la nature de leurs cibles (pays d'Europe de l'est et centrale et dans une moindre mesure de l'OTAN, opposants russes, infrastructures politiques européennes et américaines...), l'accumulation de preuves indirectes retrouvées dans leur code, les ressources et la qualité technique de leurs opérations, le fait que les attaques menées par ces groupes coïncident avec les intérêts et la doctrine russes sont de très fortes indications. Cette accumulation de preuves peut aussi être destinée à camoufler le véritable auteur. On serait alors devant une des plus vastes opérations de « false flag » jamais créées. Ce n'est pas à exclure mais ce serait, sans doute et comme souvent, surestimer le poids du complot dans la marche du monde, au détriment du hasard ou de l'incompétence [47].

Brian Bartholomew, de Kaspersky, a ainsi récemment confié au Guardian que même si son entreprise évitait généralement de faire de l'attribution, il devenait difficile de parvenir à une autre conclusion que des acteurs russes étaient derrière APT 28 [48]. Sur son blog, Bruce Schneier a estimé que « la constellation de preuves attribuant l'attaque du DNC est exhaustive » [49]. D'autres experts de qualité sont cependant, à raison également, beaucoup plus sceptiques [50, 51].

**Le régime russe a-t-il fait fuiter les documents ?** WikiLeaks a toujours affirmé que la Russie n'était pas sa source. Dans leur rapport, la CIA, le FBI et la NSA estiment avec un haut niveau de confiance que les services russes ont « relayé » les documents à WikiLeaks, sans pour autant apporter de preuve. Guccifer 2.0, qui s'est présenté comme le pirate du DNC, a affirmé avoir transmis les documents à WikiLeaks.

Il est tout à fait possible que les services russes ne soient pas la source directe de WikiLeaks et que les documents aient transité par d'autres biais ou intermédiaires. Difficile de savoir qui a fourni les documents à WikiLeaks, qui a toujours vigoureusement protégé, techniquement notamment, ses sources, d'autant que le principe de protection des sources est crucial

au journalisme. Il paraît cependant peu probable, notamment au vu du timing (Guccifer 2.0 apparaît le lendemain de l'annonce par le DNC de son piratage) que les documents de WikiLeaks ne soient pas ceux qui ont été prélevés dans les systèmes du DNC. Sur ce point également rien n'est totalement certain.

**Le régime russe a-t-il mené une campagne de propagande et de manipulation des réseaux sociaux ?** Cette question est périphérique au sujet de cet article. Cependant, les agences de renseignement américaines ont estimé que la Russie avait déployé son appareil de propagande sur les réseaux sociaux et dans les médias, notamment via ses médias officiels et ses fameux « trolls ». Par ailleurs, en France, l'équipe d'Emmanuel Macron a accusé la Russie de mobiliser cette armée de trolls et de manipuler les réseaux sociaux pour nuire à leur candidat.

La propagande russe, par le biais de certains médias comme RT ou Sputnik, est avérée. Elle reste dans les limites de ce que font toutes les puissances mondiales depuis des décennies. Seules changent son ampleur, décuplée par Internet, et peut-être son agressivité. En revanche, une manipulation occulte des réseaux sociaux, pour faire « remonter » artificiellement des sujets, et propulser des « fake news » dans le débat public est une accusation plus grave. L'attribuer à la Russie est beaucoup plus compliqué. Des enquêtes de presse ont par exemple montré que dans certaines villes d'Europe de l'Est s'étaient spécialisées dans les « fake news », mais pour un but seulement mercantile [52]. Par ailleurs, les campagnes politiques de tout bord n'ont pas besoin de la Russie pour tenter de tourner les réseaux sociaux à leur avantage.

## Problème des sources

Le journaliste qui se penche sur ces questions aux confins de la technique, du monde du renseignement, de la géopolitique et du politique, se trouve confronté à un problème de sources.

**Les limites des sources étatiques** Une des sources principales d'information pour le journaliste sur le premier versant, américain, de l'affaire, ce sont les États-Unis eux-mêmes. D'abord, lorsque ses institutions ou leurs membres s'expriment de manière officielle. C'est le cas lorsque le DHS et le DNI publient en octobre le premier communiqué d'attribution. C'est aussi le cas lorsque s'expriment le président américain ou les parlementaires américains membres du comité de contrôle du renseignement. C'est enfin

le cas lorsque le FBI, la CIA et la NSA publient leur rapport, au mois de janvier. Ensuite, lorsqu'ils s'expriment sous couvert d'anonymat. Comme en France, le « off » est très pratiqué dans la presse américaine, particulièrement lorsque cela touche aux sujets régaliens comme l'espionnage ou la sécurité nationale. La pratique est très institutionnalisée et de nombreux « officials » ont fait fuiter des informations de cette manière.

La première forme d'expression de l'État américain pose question. C'est une évidence : dans une affaire impliquant deux États, leurs agences et organes respectifs poursuivent leur propre intérêt, et la vérité en est parfois victime. Les agences de renseignement américaines l'ont montré par le passé, notamment dans les mois qui ont précédé l'invasion de l'Irak de Saddam Hussein. C'est d'autant plus vrai que les relations entre les États-Unis et la Russie sont très délicates depuis quelques années, et que les États-Unis peuvent être tentés d'accabler la Russie pour gagner un avantage diplomatique sur d'autres fronts (Syrie, Ukraine...) en l'isolant sur la scène internationale.

La seconde pose encore plus de questions : une des règles journalistiques oblige, en théorie, à fournir l'identité et la qualité des interlocuteurs dont les propos sont reproduits, afin que les auteurs de ces propos puissent en être tenus responsables. Le « off » est une manière de contourner cette responsabilité : parfois, elle est nécessaire, quand une personne court un risque lorsqu'elle s'exprime. Mais souvent, le « off » est utilisé pour contourner cette responsabilité. En clair, les journalistes n'inventent pas de responsables anonymes, et ceux qu'ils citent sont souvent des interlocuteurs pertinents, mais il est difficile pour le lecteur ou l'expert de situer ces intervenants. Les informations qui filtrent par ce biais dans la presse américaine doivent donc être prises avec des pincettes, plus ou moins grandes selon le média ou le journaliste qui les relaient.

Ces sources posent aussi problème parce qu'elles n'ont pas fourni de preuves irréfutables, notamment techniques, de l'implication de l'État russe et de sa tentative d'ingérence dans l'élection. Mais elles sont incontournables car comme on l'a vu dans la première partie, aux États-Unis, la question du piratage du DNC et de la boîte e-mail de Podesta dépasse le simple cadre technique. Ou plutôt, l'histoire n'est plus vraiment celle du piratage, mais celle de la manière dont les États-Unis et son gouvernement réagissent à ce piratage.

En France, les sources étatiques (ANSSI, Élysée...) sont aussi incontournables. Mais à l'heure où nous écrivons ces lignes et à la différence des États-Unis, aucun piratage important visant la campagne n'a eu lieu. L'histoire a donc été plutôt de savoir quels étaient les préparatifs, les

précautions mises en place par l'État pour parer à d'éventuels risques, ce qui ne pose pas le même type d'enjeux.

**Les entreprises de sécurité informatique** Dans l'affaire du piratage du DNC, l'entreprise Crowdstrike a représenté la première source d'information, et la plus reprise, notamment avec son rapport « Bear Midst » [1]. C'est très fréquent que la seule source d'information sur une attaque soit l'entreprise qui a examiné les systèmes ciblés. C'est logique, mais ça n'est pas sans poser problème : Crowdstrike est payé par le DNC, il y a donc un intérêt à exagérer la menace, à sous-estimer les manquements, à montrer que les attaquants étaient très puissants. Se baser uniquement sur ses conclusions, ce serait tenter de résoudre un crime en n'écoutant que la victime [50]. Cela peut paraître évident à des professionnels du domaine, mais c'est tout à fait crucial pour les journalistes, qui doivent évaluer la pertinence d'une source d'information. Le problème qui se pose alors aux journalistes est important car souvent, ces entreprises sont les seules à avoir accès à la « scène de crime » et disposent donc d'un monopole de l'expertise technique. Dans le meilleur des cas, le journaliste peut nuancer ou relativiser le propos, très rarement l'infirmer ou le confirmer.

Par ailleurs, les entreprises ont des affiliations nationales, étatiques, qui les contraignent dans ce qu'elles peuvent dire, sans pour autant que la nature et la portée de ces contraintes soient véritablement connue.

Plus largement, on peut s'interroger sur le rôle des entreprises et de leurs salariés, qui sont devenus des contre-espions malgré eux. Ces derniers se retrouvent en position de détecter, de suivre et d'interrompre des actions de renseignement, sont précipités dans le jeu géopolitique, souvent malgré eux. C'est une situation nouvelle dont on a, semble-t-il, pas encore mesuré toutes les implications.

**Quels observateurs pour les conflits numériques ?** Le piratage du DNC et de la boîte e-mail de John Podesta ont très rapidement été présentés comme les symptômes d'un affrontement de deux pays dans l'espace numérique. Outre les entreprises de sécurité informatique et les États – lorsque ces derniers s'expriment, ce qui est rare – il n'y a guère de source tierce, d'observateurs neutre ou alternatif pour permettre aux journalistes de comprendre ce qu'il se passe réellement en la matière.

À l'inverse d'autres conflits plus physiques, ce type d'affrontement n'a, par définition, que peu d'observateurs. Même pour les conflits hybrides ou nouveaux, comme ceux qui se déroulent en Syrie ou en Ukraine, les journalistes, sans parler du fait qu'ils peuvent se rendre sur place, peuvent

s'appuyer sur des observateurs, des organisations non gouvernementales, des experts extérieurs. On peut penser, pour le cas de la guerre en Syrie, à l'Observatoire syrien des droits de l'homme, au site Bellingcat ou à de nombreuses ONG présentes sur zone. Bien sûr, ces acteurs possèdent également, comme toutes les sources, leurs biais. Mais elles permettent aux journalistes d'obtenir un point de vue supplémentaire, et dans certains cas des preuves solides sur ce qu'il se passe sur le terrain.

Il est difficile d'envisager des acteurs similaires pour les conflits numériques. Les contingences techniques liées aux attaques informatiques font qu'un tel acteur n'est pas très crédible. Mais pourquoi ne pas imaginer une organisation de professionnels, capable d'expertiser techniquement mais de manière neutre, les affirmations des protagonistes ? Cette question mérite d'être posée tant la composante informatique des conflits va prendre une place importante dans les relations internationales.

Dans un domaine similaire, le Citizen Lab de l'université de Toronto est devenu en quelques années une source neutre d'analyse des menaces informatiques qui pèsent sur les dissidents des pays dits à risque. Les universités pourraient prendre une place plus grande dans la fourniture d'expertise technique.

### Autres difficultés

**Contexte américano-russe très tendu** L'accusation américaine contre la Russie s'est insérée dans un contexte très tendu entre la Russie et le monde occidental. Éprouvée par le conflit en Ukraine et en Syrie, la relation entre Washington et Moscou s'est fortement dégradée ces dernières années. Cela se traduit notamment par une très grande polarisation du débat public : ceux qui émettent des doutes ou rappellent les limites du processus d'attribution technique mené par les États-Unis sont accusés d'être des zélotes du Kremlin, tandis que ceux qui pointent la stratégie délétère de la Russie, en ligne et hors-ligne, sont accusés d'être soumis à la « désinformation » des médias occidentaux. Ce contexte n'aide guère à la nuance.

**L'authenticité des documents** Le cas ne s'est pas présenté et WikiLeaks n'a jamais publié de faux documents, mais pourra se poser dans le futur : dans les cas où une ingérence étrangère est soupçonnée, comment s'assurer que les documents publiés ou qui parviennent aux médias ne sont pas manipulés ? La question se pose systématiquement lorsqu'un journaliste reçoit un document. Mais lorsqu'on parle de milliers ou de centaines

de milliers de documents, qu'un État est peut-être à la manoeuvre et que les documents peuvent être publiés tels quels sur Internet, la question pourrait s'avérer très délicate à résoudre.

**Sujet technique** Ce sujet est par excellence aux confluents des spécialités de la diplomatie et de la sécurité informatique, le type d'article qui nécessite d'appeler un diplomate ou un professeur de relations internationales puis de contacter un expert en sécurité informatique.

Cela pose une difficulté, car cette double compétence est difficile à trouver : les journalistes spécialisés en sécurité informatique ne sont pas nécessairement les plus compétents pour saisir les implications diplomatiques d'un piratage, alors qu'à l'inverse l'habitué des arcanes des négociations internationales n'est généralement pas apte à saisir les subtilités de la sécurité informatique.

Cela peut parfois aboutir à des erreurs importantes. On peut par exemple penser à l'article du Washington Post annonçant à tort que des pirates russes avaient été retrouvés dans une centrale électrique du Vermont [53].

## 2.2 Un épisode majeur

### L'attribution comme processus politique

Il serait facile, presque logique, pour le journaliste face à l'incertitude des faits et le problème des sources que nous venons d'évoquer, d'abandonner, d'écrire que du point de vue technique, rien n'est certain et que tout ce qui dépasse ce cadre technique doit être rejeté faute de preuve.

Ce ne serait pas satisfaisant : quoi que l'on pense de l'attribution technique, des preuves qui ont été avancées et de leur caractère ou non définitif, le fait est que les autorités américaines ont attribué les piratages du DNC et de la boîte e-mail de John Podesta au régime de Vladimir Poutine. Le taire et renoncer à en expliquer l'impact et les ramifications sous prétexte que les preuves sont insuffisantes serait renoncer au journalisme. Il semble qu'il soit possible de concilier les deux : pointer les limites du processus d'attribution technique et ses carences, tout en interrogeant les conséquences et le cadre dans lequel les États-Unis ont décidé d'accuser un autre État. Il faut faire la différence entre l'attribution technique – qui ne sera jamais totalement satisfaisante – et l'attribution comme processus et décision politiques et diplomatiques.

Un article du site Buzzfeed [54], qui cite une dizaine de haut fonctionnaires (anonymes) américains qui étaient impliqués dans la réponse au

piratage du DNC, montre très bien à quel point le processus technique d'attribution stricto sensu et la décision de pointer du doigt celui qu'on estime responsable sont deux moments différents. Une fois la certitude acquise au sein de l'administration, ce sont des considérations très diplomatiques qui prennent le pas : comment répondre de manière à faire cesser les intrusions sans risquer l'escalade ? Par quel moyen (technique notamment) cet objectif est-il le plus susceptible d'être atteint ? Faut-il que cette attribution soit publique, et si oui, quand et comment doit-elle intervenir ? On n'est plus du tout dans un champ technique, on a dépassé l'attribution au sens strict du terme. Il ne faut pas renoncer à raconter ces événements et les exposer tant ils sont cruciaux pour comprendre les enjeux contemporains autour des attaques informatiques.

### Un épisode sans précédent

Même si les preuves techniques peuvent être considérées comme insuffisantes, le piratage du DNC et tous les événements qui ont suivi sont importants, voire inédits.

**L'attribution publique : un phénomène rare** D'abord, c'était seulement la quatrième fois que les États-Unis attribuent à un pays une attaque les visant (Chine [55] et Corée du Nord en 2014 [56], et Iran en 2016 [57]). Hors des États-Unis, c'est également rare. L'Allemagne a directement pointé du doigt la Russie pour l'attaque contre le Bundestag [31] tandis que la France n'a jamais procédé à une attribution directe, quand bien même elle dispose d'éléments, par exemple suggérant l'implication d'APT 28 dans le piratage de TV5 Monde [58].

**La nouvelle donne de l'ingérence** Au surplus, c'est la première fois qu'on parle non pas d'espionnage économique ou politique mais d'un piratage destiné à semer le trouble dans la vie démocratique d'un pays. Bien sûr, ce type d'ingérence n'est pas nouveau, certains pays comme les États-Unis s'en étant fait une spécialité dans certains pays d'Amérique du Sud. Certaines unité de renseignement occidentales disposent d'unités spécialisées dans la désinformation et la manipulation, comme le GCHQ [59]. Cependant, aucune opération connue de cette unité n'a visé un pays dans son intégralité ou des processus électoraux démocratiques.

Il y a par exemple une vraie différence avec les révélations récentes de WikiLeaks sur la France [60]. Les documents publiés sont très intéressants et montrent que la CIA s'est penchée de très près sur l'élection française de

2012, et dévoile les sphères de la vie politique de l'époque qui lui semblait d'un intérêt tout particulier. Mais il ne s'agit pas d'influence, simplement de surveillance. L'espionnage n'est pas une donnée nouvelle, à l'inverse des manœuvres d'ingérences.

Influencer sur le processus électoral était un processus long, coûteux et complexe. Aujourd'hui, Internet rend la démarche beaucoup plus facile et accessible à des États – et d'autres acteurs – qui n'avaient pas ce type de moyens auparavant. C'est d'autant plus inquiétant que ce type d'ingérence peut non pas viser à faire élire un individu, mais plus largement à pourrir le débat démocratique et l'espace public.

**Un sujet majeur pour les démocraties** Une des raisons pour lesquelles les accusations américaines ont fait grand bruit jusqu'en Europe, c'est qu'elles affirment que ces attaques remplissent un objectif géopolitique bien précis, et s'inscrivent dans un contexte mondial qui rend l'utilisation de ce type d'attaques tout à fait pertinente.

« L'opération correspond à la doctrine militaire russe, connue sous le nom de "doctrine Gerasimov", du nom de l'actuel chef des armées. Ce nouvel état d'esprit élargit ce qui est considéré comme une cible militaire, et ce qui relève de la tactique militaire », explique ainsi Thomas Rid, qui n'a aucun doute sur la responsabilité de la Russie, ce qui ne l'empêche pas d'être un des meilleurs experts mondiaux du sujet [61].

Le New York Times – il est lui aussi convaincu de l'implication russe – voit dans cette attaque un exemple « d'arme low-cost à fort impact que la Russie avait testé en Ukraine et qui a été pointé sur les États-Unis, avec une efficacité dévastatrice. Pour la Russie, avec une économie affaiblie et un arsenal nucléaire qu'elle ne peut utiliser sous peine de déclencher une guerre totale, le pouvoir informatique s'avère être l'arme parfaite : bon marché, difficile à détecter, difficile à attribuer. » [2] De nombreux chercheurs et haut fonctionnaires occidentaux partagent cette analyse et estiment que la Russie est en train d'écrire le manuel de la guerre contemporaine [62, 63].

Par ailleurs, nos démocraties sont mal équipées pour gérer ce type d'attaques qui touche à peu de frais le cœur de leur architecture. Thomas Rid [46] :

> « Au final, les démocraties ont un double désavantage. Les campagnes électorales et les organisations qui y participent sont une cible facile : des réseaux improvisés et mal sécurisés, du contenu très sensible, le tout combiné à la réticence des forces de l'ordre de

> se mêler de ce qui peut se transformer en capharnaüm politique ultra-sensible. »

Sur ce dernier point, la France, pays doté de cadres institutionnels et électoraux très rigides, est un exemple parlant. Il a fallu prendre en compte la menace pour insérer l'ANSSI dans le circuit du contrôle de l'élection, cet organisme rattaché au premier ministre pouvant difficilement se pencher directement sur la sécurisation de partis politiques en pleine campagne. Pendant la campagne, c'est la commission de contrôle de la campagne électorale qui pouvait solliciter l'ANSSI à la demande d'un candidat [64]. Ce type d'architecture, qu'il a fallu faire valider au plus haut sommet de l'État, montre qu'un peu d'innovation institutionnelle était nécessaire.

**Des règles de droit encore lointaines** Il est encore trop tôt pour dire quel impact la séquence de ces derniers mois autour des élections aura sur la manière dont les attaques informatiques sont gérées par les États. Elle est en tout cas intervenue alors que les États essaient d'établir, notamment dans le cadre de l'ONU, des règles de comportement sur Internet [65]. Les accusations américaines ont déjà rendu les négociations, qui doivent arriver à une étape importante à la fin du mois de juin, beaucoup plus difficiles. La question fait souvent sourire les experts techniques, mais la cybersécurité est un aussi un sujet géopolitique majeur. Cela a par exemple été un facteur de tensions extrêmements fortes entre les États-Unis et la Chine jusqu'en 2015, mais il s'agissait alors d'espionnage économique.

## Conclusion

Les piratages survenus lors de l'élection américaine ont été notables à plusieurs points de vue : ils ont été attribués par les États-Unis à un État rival ; une accusation d'interférence dans l'élection et de favorisation d'un candidat inédite qui a propagé une vague de peur en Europe.

Bien des sujets liés à ce piratage ont dépassé le simple cadre technique : jamais sécurité informatique n'aura été aussi diplomatique et politique. Ce n'est pas nécessairement une mauvaise chose, mais montre que nos institutions (médias et politiques notamment) ne sont pas nécessairement équipés pour l'irruption de ce phénomène et que, symétriquement, le secteur de la sécurité informatique ne dispose peut-être pas des structures lui permettant d'aborder cette nouvelle dimension. Les accusations américaines ont fait se dessiner un paysage inquiétant, où on craint de devoir s'habituer à ce que les piratages ne s'en prennent pas seulement aux intérêts financiers

mais visent aussi le fonctionnement de notre vie publique. Aux États-Unis, la question des machines à voter reste extrêmement brûlante : outre une faiblesse technique largement documentée, un morcellement des modalités administratives de ce vote électronique, le fonctionnement particulier du système électoral américain et l'utilisation très marginale des dispositifs de contrôle pourraient faire des prochaines élections en 2020 un épisode particulièrement mouvementé de l'histoire américaine. « Il est plus facile de pirater l'élection présidentielle américaine que je ne le pensais. Même mes étudiants en première année auraient pu truquer l'élection » racontait l'universitaire Alex J. Halderman, après 10 années passées à étudier le vote électronique, à Hambourg en décembre [17].

Une des questions fondamentales que devront résoudre les démocraties dans le futur, c'est comment réagir de manière transparente et juste et maintenir un semblant de stabilité dans le fameux « cyberespace » face à des attaques asymétriques. Les accusations américaines, même si elles sont crédibles, laissent un goût amer, comme le résumait très bien en décembre le journaliste de The Intercept, Sam Biddle [50] :

« Nos représentants et nos agences de renseignement nous demandent de réagir à une attaque qui est quasiment de nature militaire – on nous dit que c'est "la guerre". Quand un gouvernement étranger conduit (ou soutient) un acte de guerre contre un autre pays, il est tout à fait possible qu'il y ait une réplique similaire. On parle donc d'une situation où les États-Unis peuvent envisager une réplique militaire (numérique ou non) contre la Russie, en se basant sur des consultants privés et des notes secrètes des agences de renseignement. Si vous aimez suffisamment ce pays pour être en colère à l'idée qu'on truque les élections, vous devrez être terrifiés par la perspective de tensions militaires avec la Russie basées sur des preuves cachées. Il n'y a pas besoin de regarder longtemps en arrière pour trouver un cas où reprocher à tort à un État étranger d'avoir soutenu une attaque contre les États-Unis s'est dramatiquement retourné contre nous. »

Ou, dans un autre style, Donald Trump : « Je pense que les ordinateurs ont beaucoup compliqué nos vies. L'ère des ordinateurs fait que personne ne sait exactement ce qu'il se passe. » [66]

## Références

1. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
2. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

3. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html
4. https://guccifer2.wordpress.com/2016/06/15/dnc/
5. https://wikileaks.org/dnc-emails/
6. https://wikileaks.org/podesta-emails/
7. http://edition.cnn.com/2017/01/04/politics/assange-wikileaks-hannity-intv/
8. https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html
9. https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html
10. http://www.politico.com/story/2016/09/obama-russia-cyber-arms-race-227732
11. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national
12. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and
13. http://www.lemonde.fr/international/article/2017/03/14/fantomas-le-hackeur-prefere-du-pouvoir-russe_5094319_3210.html
14. https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf
15. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY\%20STEPPE-2016-1229.pdf
16. https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
17. http://www.lemonde.fr/pixels/article/2016/12/30/il-est-facile-de-pirater-l-election-americaine-assurent-des-specialistes-du-vote-electronique_5055823_4408996.html
18. http://www.lemonde.fr/pixels/article/2016/12/21/des-attaques-informatiques-a-visee-politique-envisageables-en-france_5052650_4408996.html
19. http://www.elysee.fr/communiques-de-presse/article/conseil-de-defense-24/
20. http://www.elysee.fr/communiques-de-presse/article/conseil-restreint-de-defense-22/
21. http://www.lemonde.fr/pixels/article/2017/02/15/cyberattaques-la-france-menace-de-mesures-de-retorsion-tout-etat-qui-interfererait-dans-l-election_5080323_4408996.html
22. http://www.diplomatie.gouv.fr/fr/services-aux-citoyens/actualites/article/francais-de-l-etranger-modalites-de-vote-aux-elections-legislatives-06-03-17
23. http://www.lemonde.fr/pixels/article/2017/03/09/pourquoi-le-vote-electronique-des-francais-de-l-etranger-pour-les-legislatives-a-t-il-ete-annule_5092022_4408996.html
24. https://www.nextinpact.com/news/103560-lanssi-sexplique-sur-annulation-vote-electronique-francais-l-etranger.htm
25. http://www.lemonde.fr/election-presidentielle-2017/article/2017/02/14/ne-laissons-pas-la-russie-destabiliser-la-presidentielle-en-france_5079213_4854003.html

26. http://www.lemonde.fr/pixels/article/2017/02/14/en-marche-denonce-des-attaques-informatiques-organisees-et-convergentes_5079539_4408996.html
27. http://www.lemonde.fr/pixels/article/2017/03/03/presidentielle-les-equipes-des-candidats-sont-elles-preparees-aux-cyberattaques_5088811_4408996.html
28. https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html
29. http://in.reuters.com/article/germany-russia-idINKBN13X16C
30. http://www.politico.eu/article/russian-influence-german-election-hacking-cyberattack-news-merkel-putin/
31. http://www.bbc.com/news/technology-36284447
32. https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862
33. https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks
34. https://www.telekom.com/en/media/details/the-open-interface-myth-445290
35. https://www.nextinpact.com/news/102306-mirai-variante-sattaque-aux-routeurs-900-000-clients-deutsche-telekom-touches.htm
36. http://www.france24.com/en/20170223-briton-arrested-over-deutsche-telekom-hacking
37. https://www.buzzfeed.com/jimwaterson/mi6-chief-says-fake-news-and-online-propaganda-is-a-threat-t
38. http://www.independent.co.uk/news/uk/politics/gchq-russian-hacking-cyber-attack-threat-uk-political-parties-general-election-threat-kremlin-a7625226.html
39. https://www.thetimes.co.uk/edition/news/gchq-russian-cyber-threat-touk-elections-20wl9s51d
40. https://www.publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/49602.htm
41. https://www.buzzfeed.com/jimwaterson/lets-all-ask-a-few-more-questions-before-claiming-russia
42. http://www.rfi.fr/europe/20170204-pays-bas-cyberattaque-sites-ministeres-vote-electronique
43. https://www.emptywheel.net/2016/12/10/evidence-prove-russian-hack/
44. https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html
45. https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
46. https://motherboard.vice.com/en_us/article/all-signs-point-to-russia-being-behind-the-dnc-hack
47. Librement adapté d'une citation https://qqcitations.com/citation/206965 dont l'authenticité semble sujette à caution.
48. https://www.theguardian.com/world/2017/jan/06/vladimir-putin-us-election-interference-report-donald-trump
49. https://www.schneier.com/blog/archives/2017/01/attributing_the_1.html

50. https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/
51. https://reflets.info/on-avait-dit-mollo-sur-le-cyber/
52. https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.jn5n4PWOE\#.dvWpZzJ34
53. https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html
54. https://www.buzzfeed.com/hayesbrown/how-russia-hacked-obamas-legacy?utm_term=.wy79m1L68\#.lw949xqyL
55. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
56. https://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html
57. https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector
58. http://www.lemonde.fr/pixels/article/2015/06/09/piratage-de-tv5-monde-l-enquete-s-oriente-vers-la-piste-russe_4650632_4408996.html
59. https://theintercept.com/2014/02/24/jtrig-manipulation/
60. http://www.liberation.fr/planete/2017/02/16/comment-la-cia-a-espionne-la-presidentielle-francaise-de-2012_1548921
61. https://motherboard.vice.com/en_us/article/all-signs-point-to-russia-being-behind-the-dnc-hack
62. https://www.buzzfeed.com/sheerafrenkel/the-new-handbook-for-cyberwar-is-being-written-by-russia?utm_term=.ugOxoK3VO\#.axL1NwgVO
63. http://www.lemonde.fr/pixels/article/2016/10/14/entre-les-etats-unis-et-la-russie-des-relents-de-guerre-froide-dans-le-cyberespace_5013801_4408996.html
64. http://www.cnccep.fr/communiques/cp2.html
65. http://www.lemonde.fr/pixels/article/2017/04/06/la-france-a-la-recherche-d-un-delicat-ordre-public-dans-le-cyberespace_5106838_4408996.html
66. http://gizmodo.com/donald-trump-computers-have-complicated-lives-very-gre-1790577332