Le piratage de TV5 Monde ou l'affirmation d'un discours anti-cyberterroriste

Saïd Haddad[*], Centre de recherche des écoles de Saint-Cyr Coëtquidan, Université de Rennes 2 – LiRIS (EA 7481)

Introduction : Un « impact technique faible » à forte « portée symbolique »

Le mercredi 8 avril 2015, la chaine internationale francophone TV5 Monde (250 millions de téléspectateurs) est attaquée par des pirates informatiques. L'attaque intervient le jour du lancement de TV5 Monde Style HD, nouvelle chaîne thématique dédiée à "l'art de vivre à la française", qui a commencé à émettre notamment au Maghreb et au Moyen-Orient. Cette attaque revendiquée entraîne une interruption des programmes de la chaîne qui se traduit par un écran noir à l'antenne.

L'infrastructure de diffusion (le multiplexage) est attaquée à 20h50. Les infrastructures principales et de secours sont neutralisées d'un seul coup. D'après le directeur informatique de la chaîne, l'on pense tout d'abord à une panne informatique[1]. La disparition, quelques minutes plus tard, de l'ensemble des messageries des serveurs indique qu'il s'agit d'une cyberattaque. Afin d'éviter des dégâts supplémentaires, le système informatique est coupé et les diffusions sont interrompues dès 22h. Le directeur général de TV5 annonce aux agences de presse que « nous ne sommes plus en état d'émettre aucune de nos chaînes »[2]. Parallèlement, le site internet et les comptes twitter et Facebook sont piratés. Des messages de soutien (en arabe, en français et en anglais) à l'organisation Etat islamique (EI) et des messages de propagande sont publiés ainsi qu'un texte adressé au président de la République française (« tu as fait une faute impardonnable »). Tout indique de prime abord, que des hackers de l'EI sont à l'origine de ce piratage avec les mentions « Je suIS IS » et « Cyber Caliphate », même si les liens du groupe revendiquant l'attaque avec l'EI

[*] Saïd Haddad est le chef du département « Information et Communication » de la Direction Générale de l'Enseignement et de la Recherche des écoles de Saint-Cyr Coëtquidan. Il est chercheur au sein du pôle « Mutation des conflits » du CREC Saint-Cyr.

[1] julien Dupont-Calbo Florian Debe Julien, "TV5 Monde : comment les pirates ont débranché la chaîne », *LesEchos.fr*, 9/04/2015, http://www.lesechos.fr/09/04/2015/lesechos.fr/0204290083596_tv5monde---comment-les-pirates-ont-debranche-la-chaine.htm#

[2] *Ibid.*

sont incertains à cette date[3]. Enfin, des documents présentés comme étant des pièces d'identité et des CV de militaires français ont été postés sur Facebook[4]. A partir de 5h du matin, le 9 avril, le système informatique est relancé peu à peu, avec l'aide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le même jour, la chaine reprend ses programmes à 18h00.

L'enquête démarre le 9 avril sous l'égide de l'ANSSI[5] : « Les treize ingénieurs de l'ANSSI dépêchés au siège de la chaîne de télévision ont la conviction que les pirates étaient infiltrés depuis des semaines dans le réseau de TV5[6]. Profitant d'une architecture informatique mélangeant la partie « métier » constituant le cœur du « réacteur » et la partie bureautique, ouvert sur l'extérieur via internet, ils ont a priori pénétré le système via un mail piégé comme cela se pratique dans 95% des piratages. Les experts pensent que les pirates ont ensuite créé des comptes avec des droits d'administrateurs leur permettant de circuler là où ils le souhaitaient »[7].

En juin 2015, des sources judiciaires françaises déclarent que les enquêtes se dirigent à ce stade vers un groupe de hackers russes, soupçonnés d'entretenir des liens avec le Kremlin, désignés par l'acronyme APT 28[8]. Deux ans plus tard, si le Parquet de Paris identifie bien APT 28 ou PawnStorm (autre nom d'APT 28)[9] comme étant les assaillants, aucune conclusion n'est tirée sur le donneur d'ordres[10]. Si l'attaque contre TV5 a « un impact technique faible », elle a « une portée symbolique souhaitée par les attaquants » comme le soulignera quelques mois plus tard l'ANSSI dans sa *Stratégie nationale pour la sécurité du numérique*[11]. Elle va permettre le déploiement d'un discours public bien particulier car s'inscrivant dans un contexte politique, sécuritaire et législatif et qu'il répond à une grammaire bien précise s'illustrant par la convergence entre un discours antiterroriste et un discours sur la menace cyber portés par un ensemble d'acteurs (personnalités politiques, journalistes et experts).

---

[3] Leloup Damien, Untersinger Martin et Tual Morgane, "TV5 Monde, un piratage d'ampleur et de nombreuses zone d'ombre », *lemonde.fr*, 9/04/2015, http://abonnes.lemonde.fr/pixels/article/2015/04/09/tv5-monde-un-piratage-d-ampleur-et-de-nombreuses-zones-d-ombre_4613300_4408996.html

[4] Le ministère de la Défense dément, le 10 avril, que des documents confidentiels aient été publiés.

[5] http://www.ssi.gouv.fr/actualite/attaque-informatique-contre-tv5-monde-lanssi-mobilisee/

[6] Voir à ce propos Untersinger Martin, « Le PIRATAGE de TV5 Monde vu de l'intérieur », *lemonde.fr*, 10/06/2017, http://abonnes.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

[7] Conervin Christophe, « L'attaque de TV5 aurait mobilisé plusieurs dizaines de cyberpirates », *lefigaro.fr*, 13/04/2015, http://www.lefigaro.fr/actualite-france/2015/04/13/01016-20150413ARTFIG00168-l-attaque-de-tv5-aurait-mobilise-plusieurs-dizaines-de-cyberpirates.php

[8] Lichfield John, "TV5 Monde Hack: jihadist cyber attack on French TV station could have Russian link", *independent.co.uk*, 10/06/2015, http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html; DRINKWATER Doug,"French TV station apparently hacked by Russians, not ISIS sympathisers", *SC Media*, 10/06/2015 http://www.scmagazineuk.com/french-tv-station-apparently-hacked-by-russians-not-isis-sympathisers/article/419756/

[9] Hourdeaux Jérôme, « Pawn Storm : deux années de piratage très politiques », *Médiapart*, 27/4/2017, https://www.mediapart.fr/journal/international/270417/pawn-storm-deux-annees-de-piratages-tres-politiques?onglet=full

[10] Paquette Emmanuel, "La justice clôt l'enquête sur la cyberattaque contre TV5 Monde », *l'express.fr,*17/10/2017, https://www.lexpress.fr/actualite/medias/la-justice-clot-l-enquete-sur-la-cyberattaque-contre-tv5-monde_1953268.html

[11] Secrétariat général de la Défense et de la sécurité nationale (SGDN), *Dossier de presse. Stratégie nationale pour la sécurité du numérique*, 16 octobre 2015. Disponible sur : https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_dossierpresse.pdf

A travers l'analyse d'un corpus constitué de déclaration des acteurs précités, nous nous pencherons sur l'émergence d'un discours anti cyberterroriste. Pour ce faire, nous adopterons comme point de départ le cadre analytique de la « securitization » (ou sécuritisation) élaboré initialement par l'École de Copenhague et plus précisément le cadre théorique de la « grammaire spécifique de la cybersécurité » développée par Lene Hansen et Helen Nissenbaum (Hansen et Nissenbaum, 2009).

Menace cybernétique et cyberterrorisme

Basée partiellement sur l'approche renouvelée de la sécurité de l'École de Copenhague représentée par Buzan, Waever et Wilde et développée dans leur ouvrage *Security: A New Framework for Analysis* (Buzan, Waever, Wilde, 1998), la sécurité est ici « une démarche où l'on quitte le cours normal des négociations et des compromis politiques pour entreprendre une construction, un processus de *securitization »* (David, 2000).

Le concept de securitization

Le concept de *securitization* (ou sécuritisation) désigne ainsi « l'instauration intersubjective d'une menace existentielle suffisamment saillante pour avoir des effets politiques substantiels » (Buzan, Waever, Wilde, 1998, p. 25). Ainsi, pour qu'il y ait securitization, le public ou l'*audience* doit accepter l'instauration de cette menace existentielle. L'acceptation de cette menace existentielle ainsi que des mesures politiques substantielles qui en découlent, résulte du caractère essentiellement linguistique du processus de sécuritisation. S'inspirant de John Austin et de John R. Searle[12], Ole Weaver affirme que l'énonciation du mot sécurité constitue l'acte : le discours sécuritaire est un acte de langage (Weaver, 1995, p. 52-53). Entendue ici comme pratique discursive, la théorie de la sécuritisation postule que le mot sécurité a un caractère performatif (Balzacq, 2016, p. 195), un énoncé performatif étant « un énoncé qui, sous réserve de certaines conditions de réussites, accomplit l'acte qu'il dénomme, c'est-à-dire fait ce qu'il dit faire du seul fait qu'il le dise » (Kerbrat-Orecchioni, 2016, p. 9).

Le discours sur la menace cybernétique fait de cette dernière un enjeu de sécurité. Toutefois, pour parler de cybersécurité, un lien doit être établi entre la sécurité informatique et la securitization, entre la sécurité informatique et les notions traditionnelles de la sécurité nationale, mouvement porté par les « autorités gouvernementales, les chefs d'entreprises et les leaders des autres secteurs non gouvernementaux » (Nissenbaum, 2005). Ce mouvement de la sécurité informatique à la sécurité cybernétique (*computer security to cyber security*) (Hansen Nissenbaum, 2009, p. 1160)

[12] Austin John, *Quand dire, c'est faire*, Paris, Le Seuil, 1970 ; Searle John R., *Les actes de langage, essai de philosophie du langage*, Paris, Herman, 1970 et *Sens et expression,* Paris, Minuit, 1982.

s'accompagne d'une articulation entre plusieurs objets référents (*referent objects*), c'est-à-dire les objets menacés que sont la sécurité nationale, la sécurité de l'État, la sécurité privée et la sécurité des réseaux. Ces objets référents sont liés par une dynamique d'articulation et de compétition qui donne sa cohérence au discours sur la cybersécurité. Toujours selon Hansen et Nissenbaum, la sécurité du réseau et la sécurité individuelle sont des objets référents essentiels mais leur importance politique relève des connexions ou des liens entretenus avec des objets référents collectifs que sont l'État, la nation, la société et l'économie.

La grammaire de la cybersécurité

Ce faisant, le discours sur la cybersécurité répond à une grammaire bien particulière telle que définie par les deux auteures précitées : l'hypersécuritisation *(hyper securitization*), les pratiques de sécurité quotidiennes (*everyday security practices*) et la technification (*technification)* qui constituent les spécificités du discours sur la cybersécurité, des « modalités de sécurité spécifiques au secteur du cyber ».

Par hypersécurisation, il faut entendre l'extension de la sécuritisation au-delà d'un niveau normal de menace. Il s'agit d'amplifier les menaces, afin de pouvoir recourir à des mesures elles aussi excessives. Le discours recourt à la logique du conditionnel, à l'instantanéité et aux effets combinés ou à l'effet domino qu'une attaque dans le cyberespace provoque (financier, militaire, économique, sociétal). Il s'agit à la fois d'exagérer les menaces et promouvoir des contre-mesures excessives. Le recours à l'imprécision (la menace est par essence floue) crée une « ambiguïté cruciale au sein du discours sur la cybersécurité » (Hansen, Nissenbaum, 2009, p. 1164). Une ambiguïté, qui constitue une ressource pour les locuteurs (émetteurs et récepteurs), « le flou [n'étant] pas un problème des énoncés, mais une ressource que la langue offre à ses utilisateurs » (Krieg-Planque, 2017, p. 155). Le registre de la peur, consubstantiel au discours sur la menace s'articule au procédé de la mémoire discursive, c'est-à-dire l'utilisation de la mémoire collective dans un discours (Moirand, 2007). Il s'agit ici de faire des analogies historiques, de comparer, de rappeler un évènement passé afin de susciter une émotion certaine chez l'auditeur. Le passé est ainsi mobilisé en tant « que référence légitime ».

La mobilisation des individus constitue le deuxième élément de cette grammaire. Il s'agit ici de lier les catastrophes annoncées à l'expérience quotidienne et familière des individus. Cela signifie que l'acceptation du discours public de sécurité est facilitée par la résonnance avec des expériences concrètes des individus. Le discours sur la responsabilité de l'auditeur s'inscrit également dans ce registre grammatical mais dans le même temps, l'individu est considéré comme une potentielle menace.

Les divers discours mobilisant les individus et la collectivité sont pourvus d'une double visée informative et prescriptive (Née, Oger et Sitri, 2017)[13], les actes de langages relevant généralement de la catégorie des « directifs » et de celle des « promissifs ».[14]

Enfin, la technification est le troisième volet du discours. Le recours aux scientifiques et autres experts permet de légitimer le discours. Cette crédibilisation du discours de sécuritisation est d'autant plus efficace que le discours des experts apparaît comme étant normativement neutre (Hansen, Nissenbaum, *op.cit.*) ; ce faisant, les experts sont des acteurs du processus du sécuritisation tant dans le registre de l'hypersécuritisation que celui des pratiques quotidiennes (parler avec autorité au grand public).

Le cyberterrorisme

Qualifiées par le responsable du comité de coordination de la cyberdéfense de l'Estonie « de sorte de terrorisme » (*a kind of terrorism*) (Hansen, Nissenbaum, *op. cit.*, p. 1169), les cyberattaques dont a été victime l'Estonie au printemps 2007 ont marqué la connexion, sur le plan médiatique, entre la sécurité informatique et les notions traditionnelles de la sécurité nationale. Le lien entre terrorisme et technologie informatique est toutefois ancienne : elle est présente dans la littérature américaine sur la sécurité nationale dès 1991 (Dunn- Cavelty, 2007, p. 19) et apparaît dans la production académique en 1996 lorsque Barry Collin définit le cyberterrorisme comme « la convergence du monde physique et virtuel »[15] (Desforges, 2011). Aux lendemains des attentats du 11 septembre 2001, le lien entre menace terroriste et cyberespace s'affermit : ainsi al Qaïda devient une figure emblématique du cyberterrorisme. Dans un article du Washington Post intitulé « Cyber Attacks by Al Qaeda Feared *»,* il est, par exemple, fait mention d'une plus grande attention aux activités de ce groupe dans l'espace cyber[16]. Ce lien a lieu alors que s'est opérée depuis quelques années la transformation de la figure du hacker (Dagiral, 2008 ; Conway, 2009) et s'inscrit dans un mouvement plus large, celui du « processus conflictuel de construction de règles de l'espace numérique » (Hayat, Paloque-Berges, 2004).

Si la formule a fait florès depuis, il n'existe pas de consensus sur la définition du cyber terrorisme à l'instar de la notion de terrorisme (Weinberg, Pedahzur, Hirsch-Hoefler, 2004). Ainsi que le souligne Alix Deforges (*op. cit*), deux acceptions se dégagent : la première selon laquelle « le

[13] Émilie Née, Claire Oger et Frédérique Sitri, « Le rapport : opérativité d'un genre hétérogène », *Mots. Les langages du politique,* 114, 2017, p .9-24.

[14] Selon les catégories distinguées par John R. Searle dans *Sens et expression*, *op. cit.*. Les directifs « constituent des tentatives de la part du locuteur de faire faire quelque chose par l'auditeur » tandis que les promissifs « sont des actes dont le but est d'obliger le locuteur à adopter une certaine conduite future », Catherine Kerbrat-Orecchioni, *op. cit.,* p. 20-21.

[15] Collin Barry, « The Future of CyberTerrorism : Where the Pysical and Virtual Worlds Converge », *11th Annual International Symposium on Criminal Justice Issues*, 1996.

[16] Gellman Barton "Cyber attacks by al Quaeda feared", The Wahshingon Post, 27/6/2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html

cyberterrorisme doit regrouper l'ensemble des pratiques en lignes des groupes terroristes », la seconde selon laquelle « le terme doit être restreint à un type d'accès précis, celles qui utilisent le réseau internet comme arme et/ou cible ». En dépit des différences de perspective (par l'acteur, par l'action), « la notion de cyberterrorisme paraît finalement peu opératoire pour comprendre les conflictualités à l'œuvre dans le cyberespace », traduirait les obsessions américaines apparues après 2001, et relèverait de l'ordre du discours (Kempf, 2014, p. 88). La faiblesse opératoire étant accentuée par l'absence de victimes, blessées ou tuées par des actes cyberterroristes comme le soulignent P.W Singer et A. Friedman (2014, p. 96). Un vocabulaire spécifique s'est néanmoins diffusé pour désigner les pratiques en ligne des groupes djihadistes, que cela soit al Qaïda ou l'EI, le cyberdjihadisme, l'utilisation d'internet par ces acteurs étant ici centrale (Desforges, *op. cit.*).

En dépit de ces divergences conceptuelles, il est à noter que ce terme s'est imposé dans le discours public et que « l'imaginaire de la menace » qui repose sur la convergence de la peur du terrorisme et de la peur de la technologie (Conway, 2009) s'inscrit ainsi dans le processus d'hypersécuritisation décrit plus haut.

La journée du 9 avril : mobiliser, rassurer et politiser

Le discours anti-terroriste a trois effets principaux : mobiliser, rassurer, politiser (Fragnon, 2009). La mobilisation passe par une stratégie de construction de l'ennemi, c'est-à-dire une logique d'exclusion des terroristes de la communauté humaine et par la revendication de valeurs communes. Le rassurement passe par « la présentation d'une maîtrise de l'action publique » tandis que la politisation traduit l'explication du sens de l'action terroriste en l'inscrivant dans un « récit général » sur la marche du monde » (*ibid.*). Le discours antiterroriste fait ainsi écho à la grammaire particulière de la cybersécurité évoquée plus haut et à ses spécificités que sont l'hypersécuritisation, les pratiques de sécurité quotidiennes et la technification. La journée du 9 avril, le lendemain de la cyberattaque, va voir une multiplication de déclarations de la part des membres du gouvernement, des hommes et femmes politiques et des experts que les médias vont faire dialoguer (Veniard, 2018, p. 92) et les médias eux-mêmes.

La prise de parole gouvernementale

Condamnation et annonces de mesures à la hauteur de cette attaque vont rythmer la journée du 9 avril. La première à s'exprimer est Fleur Pellerin, ministre de la Culture et de la Communication et de fait autorité de tutelle de la chaine, qui sur twitter manifeste « tout [son] soutien et [sa] solidarité aux équipes de la chaîne @TV5MONDE, victimes d'un véritable acte terroriste @YvesBigot ». Elle est suivie par la ministre de la Justice, Christiane Taubira qui déclare « Pas de doute, ils ne supportent ni éducation, ni culture, ni libre information ni liberté » et par Annick Girardin, secrétaire d'Etat au Développement et à la Francophonie selon laquelle « Pirater

#TV5MONDE est écœurant et lâche. Elle véhicule la langue française, célèbre sa diversité, créé des ponts entre francophones du monde ». Condamnation et soutien à la rédaction de TV5 Monde sont exprimés également par le premier Ministre Manuel Valls pour qui « L'attaque du réseau #TV5MONDE est une atteinte inacceptable à la liberté d'information et d'expression. Soutien total à la rédaction ». Enfin, Axelle Lemaire, secrétaire d'Etat au numérique exprime son « Soutien à @TV5MONDE, on ne fera pas taire la France. La cybersecurité est un outil essentiel de la souveraineté » En plus de ces tweets, communiqués, interviews à la presse et déclarations devant la représentation nationale vont émailler cette journée où trois ministres, celle de la Culture, celui de l'Intérieur, Bernard Cazeneuve et celui des Affaires étranger, Laurent Fabius seront les plus présents sur la scène médiatique. Les trois se rendent dès le 9 avril matin au siège de TV5[17].

Une « mobilisation totale »

Ainsi, au sortir de la visite à TV5, le ministre de l'Intérieur annonce qu'une enquête est lancée ainsi que la création de 500 emplois supplémentaires pour lutter contre le cyberdjihadisme[18]. Il affirme que « sur le plan juridique, humain et technologique, la mobilisation est totale ». Dans l'après-midi, au Sénat, en réponse à une question, il annoncera que le parquet de Paris a saisi la Direction centrale de la police judiciaire et la Direction générale de la sécurité intérieure pour conduire l'enquête et que « même si cette enquête a commencé, si elle doit se déployer, il y a de fortes présomptions que des groupes ayant des intentions terroristes aient pu commettre cet acte ». Par ailleurs, il annoncera que la réaction de l'Etat face à cette attaque s'inscrit dans le cadre de la politique engagée depuis le début du quinquennat, un quinquennat marqué par les attentats de janvier 2015 :

« Depuis le début de ce quinquennat, ce sont 432 emplois supplémentaires qui ont été créés au sein de la Direction générale de la sécurité intérieure. Son budget a été augmenté de 10 millions d'euros par an pour lui permettre d'acquérir les meilleurs moyens technologiques. Au terme des attentats du mois de janvier, le président de la République et le Premier ministre ont décidé d'abonder ces effectifs de 500 pour ce qui concerne la Direction générale de la sécurité intérieure. Ce qui signifie des moyens en analystes, en informaticiens, en linguistes qui, bien entendu, sont, pour une partie d'entre eux, compétents pour lutter contre la cybercriminalité […].

[17] "Trois ministres au chevet de TV5 Monde, victime de piratage", *lemonde.fr*, 9/04/2015, http://abonnes.lemonde.fr/pixels/article/2015/04/09/trois-ministres-au-chevet-de-tv5-monde-victime-de-piratage_4612207_4408996.html

[18] *Ibid*, voir également http://www.bfmtv.com/mediaplayer/video/bernard-cazeneuve-annonce-la-creation-de-500-emplois-pour-lutter-contre-le-cyberjihadisme-492605.html

Ce sont des moyens humains et budgétaires : 233 millions d'euros sur trois ans dont 80 millions permettront la modernisation des moyens numériques et technologiques du ministère. Et puis ce sont des instruments juridiques nouveaux : la loi du 13 novembre avec le blocage administratif des sites, la possibilité de procéder à des perquisitions à distance sur les ordinateurs ; et la loi renseignement dont je veux dire vraiment très solennellement devant votre Assemblée qu'elle est destinée à protéger les Français face à des risques du type de celui qui s'est produit ce matin, qui porte atteinte aux libertés, dans le respect scrupuleux des libertés publiques. En dotant nos services de renseignement des moyens dont ils ont besoin, sous le contrôle d'une Haute Autorité administrative et d'une instance juridictionnelle, le Conseil d'État »[19].

Quant au ministre des Affaires étrangères, il déclarera dans un premier temps après la visite que « Tout sera mis en œuvre pour identifier les auteurs de cette attaque et les traduire en justice. Une fois de plus, les terroristes prennent pour cible la liberté d'expression et d'information. Notre détermination pour combattre le terrorisme est totale. »[20]. Le même jour sur *iTélé* : « Ce qu'il faut retenir en particulier c'est que ces terroristes, et on va vérifier la revendication, utilisent toutes les nouvelles techniques et c'est la raison pour laquelle nous avons eu raison de nous mobiliser sur la cybercriminalité. Mais il s'agit là d'une attaque d'une nouvelle ampleur, qui doit rendre extrêmement attentives toutes les télévisions et Mme Pellerin va recevoir l'ensemble des responsables. Tout est mis en œuvre pour à la fois, retrouver les auteurs, les punir, rétablir l'antenne et éviter que de telles attaques cyber-terroristes puissent menacer la liberté d'expression à l'avenir »[21].

Annoncée le même jour, a lieu une réunion en urgence regroupant les ministres de la Culture et de la Communication, de l'Intérieur ainsi qu'une vingtaine de patrons de médias. Le gouvernement, par l'intermédiaire de ses deux ministres, appelle ainsi à la « vigilance » des médias, les enjoint à « rehausser leur niveau de précaution », soulignent que des attaques similaires peuvent se reproduire et propose l'aide de l'Etat pour la mise en place des mesures préventives ou correctrices[22]. Durant cette réunion, le ministre de l'Intérieur affirme que « La cybercriminalité, les cyberattaques, sont une réalité, et non pas un fantasme de l'administration, de mes services »[23].

[19] http://discours.vie-publique.fr/notices/153001015.html; voir également http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Attaque-de-TV5-Monde
[20] http://discours.vie-publique.fr/notices/153000976.html
[21] http://discours.vie-publique.fr/notices/153000975.html
[22] http://www.larepubliquedespyrenees.fr/2015/04/09/apres-l-attaque-contre-tv5monde-paris-appelle-les-medias-a-la-vigilance,1244505.php ;
[23] « Attaque de TV5Monde : le gouvernement veut sensibiliser les médias », rfi.fr, 9/04/2015, http://www.rfi.fr/france/20150410-attaque-tv5-monde-france-gouvernement-medias-cazeneuve-pellerin

Entre condamnation des menaces, défense des valeurs (liberté d'expression, souveraineté), affirmation de la détermination des autorités et annonce de mesures de lutte contre le terrorisme, l'Etat s'y engageant, émerge un discours de responsabilisation et d'éducation, dirigé essentiellement vers les entreprises des médias autour de leur sécurisation sur le plan informatique.

La désignation du terrorisme djihadiste

La désignation d'un terrorisme spécifiquement djihadiste est plus explicite chez les parlementaires. Ainsi dans l'opposition de droite, le député UMP Christian Estrosi déclare via un tweet: « Piratage TV5 Monde revendiqué par jihadistes démontre une fois de plus l'état de guerre où nous trouvons face au terrorisme islamo-fasciste » tandis que son collègue Eric Woerth juge sur Radio Classique/ LCI) ce piratage « très inquiétant » et digne « d'un film de science-fiction ». Le secrétaire national à la culture de l'UMP, David-Hervé Boutin, « dénonce cet acte lâche contre la liberté d'expression et d'information" dans un communiqué tout en appelant à trouver des solutions pour lutter contre « ce phénomène préoccupant pour nos libertés »[24]. Le Parti socialiste déclare que « la culture et les médias sont devenus aux quatre coins du monde des cibles privilégiées pour les mouvements qui entendent imposer par la terreur leur vision extrémiste » et que **«** face à l'obscurantisme, le Parti socialiste apporte tout son soutien à l'ensemble des acteurs culturels, de la presse, des médias et de la communication qui, au quotidien, œuvrent pour la liberté d'expression et l'enrichissement culturel »[25]. La sénatrice écologiste Esther Benbassa, vice-présidente de la Commission d'enquête sur l'organisation et les moyens de la lutte contre les réseaux djihadistes en France et en Europe déclare qu'à l'heure où « les pouvoirs publics français essayent de trouver les moyens de stopper la propagande jihadiste sur internet **»,** ce piratage « met en évidence qu'il est temps de comprendre que les terroristes mènent la guerre également sur la toile ». **«** Tout doit être mis en œuvre pour ne pas perdre sur ce front »[26]. L'utilisation du terme *guerre* dans l'espace politique et médiatique, « chargé d'une mémoire collective (…), c'est-à-dire une mémoire constituée des faits et des discours tenus dans l'espace et les médias» après les attentats du 11 septembre 2001 (Veniard, 2016, p.93) s'accompagne de l'expression *guerre contre le terrorisme* qui a refait son apparition chez les responsables politiques à la faveur du déclenchement de l'opération Serval au Mali en janvier 2013 (Haddad, 2017, p. 225).

[24] http://www.rtl.fr/actu/politique/tv5-monde-la-classe-politique-condamne-unaninement-le-piratage-7777328825
[25] Ibid.
[26] Ibid.

Le recours à la mémoire discursive se retrouve également dans une interview du député Eduardo Rihan Cypel, membre socialiste de la Commission de la Défense et des forces armées, qui déclare sur RTL, le 9 avril, que « Ce qui nous guette c'est un possible cyber-11 septembre, une sorte de cyberattaque qui toucherait le monde physique »[27].

Entre guerre et prudence

Les média reviennent sur l'attaque en faisant une large place aux déclarations ministérielles, celles des dirigeants de TV5, en donnant la parole aux experts. Le soir de l'attaque, le directeur de TV5 avait évoqué sur You Tube, « une attaque d'une puissance inouïe »[28]. La directrice du numérique de la chaîne abondera en ce sens et fera remarquer qu'a été menée « une attaque très bien préparée et très bien réalisée car notre système était excessivement sécurisé »[29]. Bien que l'attaque ait été qualifiée par un certain nombre d'experts d'attaque « d'une simplicité biblique, le degré zéro du hacking mais une méthode toujours aussi efficace »[30], va s'opérer un cadrage de la menace singulier autour de la puissance des attaquants. Le recours à l'argument de la « bonne préparation » et de la « bonne réalisation » de l'attaque s'inscrit plus largement dans l'usage du qualificatif « sophistiqué » mentionné à chaque cyberattaque (Buchanan, 2017). Ressource pour le locuteur qui en est ici la victime, la surestimation de la cyberattaque permet à la fois de minimiser ses responsabilités (ses propres failles) et de réduire les coûts économiques de l'attaque, notamment ceux de la (cyber) assurance *(ibid.*, p. 5-6)[31]. Cette surestimation participe du processus d'hypersécuritisation.

Les unes consacrées à la cyberattaque sont publiés le surlendemain de l'attaque, le 10 avril. L'heure de l'attaque et une autre actualité[32]. Les unes sur la cyberattaque y font soit allusion directement comme *Le Figaro* du 10 avril qui titre ainsi en une : « Cyberattaque : la nouvelle arme des islamistes », ou indirectement comme *Libération* du 11 et 12 avril titrant en une :

[27] http://www.rtl.fr/actu/societe-faits-divers/faut-il-avoir-peur-du-cyberterrorisme-7777323956

[28] Déclaration d'Yves Bigot sur You Tube, http://rue89.nouvelobs.com/2015/04/09/lattaque-tv5-cyber-djihadiste-dune-ampleur-sans-precedent-258584. Expression réutilisée le lendemain, sur iTélé, https://www.dailymotion.com/video/x2m5abi

[29] https://www.dailymotion.com/video/x2m58vo

[30] L'attaque est qualifiée de « simple dans son déclenchement » et « très sophistiquée dans son déroulé avec un logiciel compliqué », les hackers étant de bon niveau, une longue préparation ayant été nécessaire, selon les enquêteurs, voir : "Piratage de TV5 Monde, un seul mai aura suffi ! », *zdnet.fr*, 14/04/2015 http://www.zdnet.fr/actualites/piratage-de-tv5-monde-un-mail-aura-suffi-39817926.htm. « TV5 Monde : de vieilles ficelles pour un piratage sans précédent », *france24.com, 10/04/2015*, http://www.france24.com/fr/20150410-tv5-piratage-chaine-arr%C3%AAt-cybercalifat-television-audiovisuel-cyberdjihad/

[31] Elle est également une ressource pour les entreprises spécialisées dans la sécurité informatique, que l'on pourrait rapprocher des entrepreneurs de morale, définisseurs de normes (ici de sécurité), cf. BECKER Howard. S, *Outsiders*, Métaillé, 1985, p. 171-188.

[32] L'heure de l'attaque et une autre actualité (la crise au FN et la grève à Radio France, rencontre Obama-Castro) expliquent certainement ce décalage. Plus réactives, certaines chaînes d'information en continu diffuseront des documentaires sur le thème du cyberterrorisme » Voir par exemple BFM Business*, Le cyberterrorisme, nouveau champ de bataille ?*, https://www.dailymotion.com/video/x2m6wgy

« Tous épiés, tous suspects » à propos de la loi sur le renseignement qui est discutée au parlement ainsi que *L'Humanité* du 13 avril qui consacre au projet de loi sa page Débats et Controverses.

Un certain nombre d'experts va intervenir durant les premiers jours. Que cela soit au sein d'organes spécialisés (*zdnet.fr ; itespresso.fr*[33]*, reflets.info*) ou dans les médias généralistes[34]. La plupart sont des experts en sécurité informatique. L'on peut constater que les avis sont partagés : ainsi les modes opératoires et la gravité de l'attaque sont considérés soit comme des opérations de guerre ou soit comme des opérations menés par des « pieds nickelés ». Les interventions des différents experts oscillent entre pédagogie et appels à la vigilance. Il en est ainsi de l'intervention de Nicolas Arpagian, directeur scientifique à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ) qui, lors de l'émission de *RTL* évoquée plus haut, appelle à la responsabilité de tous les utilisateurs d'internet.

Mais puisque tout semble converger vers les djihadistes de l'EI, les médias sollicitent des spécialistes de ces questions : il en est ainsi de Mathieu Slama, présenté comme un spécialiste de la communication de crise, qui intervient dans *Le Figaro* du 9 avril 2015 sur la stratégie médiatique de l'EI[35]. Il en est ainsi de Wassim Nasr, journaliste à *France 24* qui va être plus prudent quant à l'identité des hackers, ces derniers se revendiquant de l'EI et non étant commandités. Quelques jours après sur i-Télé, il reviendra sur ce point en soulignant à la fois la pauvreté de l'arabe du communiqué, l'utilisation du sigle ISIS au lieu d'IS[36].

Guillaume Poupard, directeur de l'ANSSI, déclarera également dès le 10 avril sur *Europe 1* « qu'il faut être très prudent sur l'origine de l'attaque » et « que parfois on a des surprises une fois qu'on découvre qui sont les attaquants »[37].

---

[33] Auffray Christophe, « Ce que l'on sait de l'attaque de TV5 Monde : en fait, presque rien », zdnet.fr, 10/04/2015, http://www.zdnet.fr/actualites/ce-qu-on-sait-de-l-attaque-de-tv5-monde-en-fait-presque-rien-39817794.htm, GUERRIER Philippe, « Cyberattaque TV5 Monde : ce qui a marqué les experts de la sécurité IT », *itespresso.fr*, 10/04/2015, http://www.itespresso.fr/cyber-attaque-tv5-monde-ce-qui-a-marque-experts-securite-it-93413.html#; « Piratage de #TV5Monde : l'opération cyber-pieds nickelés, *reflets.info*, 10/04/2015 https://reflets.info/articles/piratage-de-tv5monde-l-operation-cyber-pieds-nickeles

[34] "Lutte contre le cyberterrorisme : des moyens insuffisants », *francetvinfo.fr,* 9/04/2015, https://www.francetvinfo.fr/faits-divers/terrorisme/piratage-de-tv5-monde/lutte-contre-le-cyberterrorisme-des-moyens-insuffisants_872707.html

[35] Slama Mathieu, « Cyberattaque contre TV5 monde : la guerre médiatique décryptée, le figaro.fr*, 9/04/2015,* http://www.lefigaro.fr/vox/monde/2015/04/09/31002-20150409ARTFIG00252-cyberattaque-contre-tv5-monde-la-guerre-mediatique-de-daesh-decryptee.php

[36] « Piratage de TV5Monde : le groupe « CyberCaliphat » est-il vraiment lié à Daesh », *20minutes.fr*, 9/04/2015, https://www.20minutes.fr/societe/1583123-20150409-piratage-tv5monde-daesh-cache-vraiment-derriere-groupe-cybercaliphat ; « TV5 : rien n'émane de l'EI en terme de revendication », Itélé, 9/04/2015, https://www.dailymotion.com/video/x2m6e2x. L'utilisation de l'acronyme IS est également questionnée par la presse étrangère, le *Daily Beast* s'étant déjà étonné quelques semaines auparavant que les hackers d'ISIS s'appellent ISIS (ce qu'ils ne font jamais) : SIEGEL Jacob, YOUSSEF Nancy A., "'ISIS' Hackers Love American Folk-Punk; Don't Know the Name of Their Own Terror Group", , *thedealybeast.com,* 13/01/2015,http://www.thedailybeast.com/articles/2015/01/12/isis-hackers-love-american-folk-punk-don-t-know-the-name-of-their-own-terror-group.html

[37] http://www.europe1.fr/mediacenter/emissions/l-interview-de-jean-pierre-elkabbach/videos/poupard-on-est-face-a-une-menace-nouvelle-2424225

Conclusion : des discours qui se confondent

Le discours sur la menace cyberterroriste est facilité par le contexte dans lequel s'est déployée l'attaque contre TV5. Un contexte marqué par un mouvement européen qui voit des Etats comme la France, l'Allemagne ou la Grande Bretagne introduire la menace cybernétique dans les stratégies nationales de sécurité et de défense et faire de la cyberdéfense une priorité nationale (Haddad, 2018). Mais également par une actualité récente illustrée par la recrudescence des cyberattaques depuis le début de l'année 2015 qui ont suivi les attentats de Paris de janvier et dans un contexte de hausse des engagements militaires français à l'étranger, au Levant (lancement de l'opération Chammal en septembre 2014) et dans la bande sahélo-saharienne (opération Serval en janvier 2013 et opération Barkhane depuis août 2014).

Le discours public qui se met en place à l'occasion de la défiguration du site internet de TV5 s'inscrit dans un processus doctrinal en cours dans le domaine de la cybersécurité. L'objet des interventions des autorités gouvernementales est de sensibiliser la population et de dessiner une représentation efficace du potentiel cybernétique de l'Etat (capacité d'anticipation de la menace et de rétorsion). La mise en place d'un discours d'hypersécuritisation s'accompagne lors de la crise d'un discours de rassurement, les entreprises médiatiques n'étant pas considérées comme des opérateurs d'importance vitale[38]. Ce discours va se déployer toute l'année 2015 et trouver sa concrétisation le 16 octobre lors de la publication par le Premier ministre de la *Stratégie nationale pour la sécurité du numérique* « destinée à accompagner la transition numérique de la société française » de consolider la sécurité d'une « République numérique »[39] . La convergence des discours sur la menace cyber et le discours antiterroriste est l'occasion de promouvoir la loi sur le renseignement, qui sera adoptée le 24 juin 2015[40]. Et ce en dépit des nuances, voire des réserves qui sont apparues dans les médias concernant certains aspects de la cyberattaque (origine des attaquants, ampleur de l'attaque, conséquences politiques à travers la loi sur le renseignement).

[38] Un opérateur d'importance vitale « gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population », ANSSI, *Défense et sécurité des systèmes d'information. Stratégie de la France*

[39] Anssi, *Stratégie nationale pour la sécurité du numérique,* octobre 2015. Disponible sur : https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

[40] http://abonnes.lemonde.fr/societe/article/2015/06/25/la-loi-renseignement-definitivement-adoptee_4661553_3224.html ; loi validée le 23 juillet par le Conseil Constitutionnel à l'exception de trois dispositions : http://abonnes.lemonde.fr/pixels/article/2015/07/23/le-conseil-constitutionnel-censure-trois-articles-de-la-loi-sur-le-renseignement_4696112_4408996.html

Bibliographie

Balzacq Thierry, *Théories de la sécurité. Approches critiques,* Paris, Presse de Sciences Po, 2016

Buchanan Ben, *The Legend of Sophistication In Cyber Operations*, Harvard Kennedy School, 2017/1, Belfer Center for Science and International Affairs

Buzan Barry, Weaver Ole et De Wilde Jaap, *Security: A New Framework for Analysis*, Boulder, Lynne Rienner Publishers, 1998.

Conway Maura, « Le cyber-terrorisme. Le discours des médias américains et ses impacts », *Cités* 2009/3 (n° 39), p. 81-94

Dagiral Eric, « Pirates, Hacker et activistes : déplacements et dilutions de la frontière électronique », *Critiques*, n° 733-734, 2008, p ; 480-495

Desforges Alix, "Cyberterrorisme : quel périmètre?", *Fiche de l'IRSEM*, n°11, décembre 2011, http://www.irsem.defense.gouv.fr

Dunn-Cavelty Myriam, "Cyber-Terror. Looming Threat or Phantom Menace? The Framing od the US Cyber-Threat Debate", *Journal of Information Technology & Politics*, vol. 4(1), 2007, p. 19-36

Fragnon Julien , *Le discours antiterroriste. La gestion politique du 11 septembre en France*, Thèse de doctorat de science politique, Université Lyon 2, 2009, URL : http://theses.univ-lyon2.fr/documents/lyon2/2009/fragnon_j/download

Haddad Saïd, "Une grammaire de la cybersécurité française ou la construction d'une stratégie nationale de cyberdéfense (2008-2017)", *Stratégique,* 117, 2018

Haddad Saïd, "Managing the Media during the War in Mali: Between Restriction and Pragmatism", in Irina Goldenberg, Joseph Soeters, Waylon H. Dean (eds.*), Information Sharing in Military Operations*, Springer International Publishing, 2017, 221-234

Hansen Lene, Nissenbaum Helen, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly*, 53, p. 1155-1173

Hayat Samuel, Paloque-Berges Camille, "Transgressions pirates", *Tracés. Revue de Sciences humaines*, 26, 2014, p. 7-19

Kempf Olivier, « Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, n°152-153, 2014, p. 82-97

Kerbrat-Orecchioni, Catherine, *Les actes de langage dans le discours. Théorie et fonctionnement*, Paris, Armand Colin, 2016

Krieg-Planque Alice, *Analyser les discours institutionnels*, Paris, Armand Colin, 2017

Moirand Sophie, « Discours, mémoires et contextes : à propos du fonctionnement de l'allusion dans la presse », *Corela*, HS-6 | 2007, http://journals.openedition.org/corela/1567#tocto2n1

Nee Émilie, Oger Claire et SITRI Frédérique, « Le rapport : opérativité d'un genre hétérogène », *Mots. Leslangages du politique,* 114, 2017, p .9-24

Nissenbaum Helena, "Where computer security meets national security", *Ethics and Information Technology,* 7, 2005, p. 61-73

Singer P.W and Friedman Allan, *Cybersecurity and Cyberwar. What everyone needs to know,* Oxford University Press, 2014

Veniard Marie, "La presse devant les attentats terroristes : usages journalistiques du mot guerre", *Mots. Les langages du politique,*116, 2018, p. 91-109

Weaver Ole, "Securitization and Desecuritization", in Ronnie D. Lipschutz (ed.), *On Security,* New York, Columbia University Press, 1995, p. 46-87

Weinberg Leonard, Pedahzur Ami & Hirsch-Hoefler Sivan (2004) "The Challenges of Conceptualizing Terrorism", *Terrorism and Political Violence*, 16:4, 2004, p. 777-794