La communauté du renseignement américaine depuis le 11-septembre : les limites d'une renaissance

Gildas Le Voguer, Université Rennes 2

Mots clés: communauté du renseignement, guerre contre le terrorisme, transparence, cyberespace.

Keywords : intelligence community, war on terror, transparency, cyberspace.

À l'instar de l'attaque contre la base navale de Pearl Harbor, qui avait conduit les États-Unis à renoncer à leur politique isolationniste, les attentats du 11-septembre les contraignent à réviser leur politique étrangère. Après la fin de la guerre froide, l'administration du président Bill Clinton puis celle de George W. Bush ont tenté de formuler un nouveau paradigme susceptible de remplacer celui de l'endiguement, qui prévalait depuis la fin de la Seconde Guerre mondiale. En vain. Il aura donc fallu le 11-septembre pour que la guerre totale au terrorisme (« Global War on Terror ») devienne l'alpha et l'oméga de la politique étrangère des États-Unis. Il ne s'agit pas d'un simple réexamen de la lutte contre le terrorisme menée jusqu'alors mais d'un véritable bouleversement conceptuel, qui implique une révision des moyens à mettre en œuvre pour mener la guerre annoncée. Cela commence par les services de renseignement américains, qui doivent se réinventer après avoir tragiquement failli.

Malgré leur incapacité à prévenir les attentats du 11-septembre, le président Bush leur conserve sa confiance et, en se rendant au quartier général de la CIA à Langley en Virginie dès le 26 septembre 2001, il apporte de manière ostensible son soutien aux agents de la communauté du renseignement, qui sont alors sous le feu des critiques. À cette occasion, il déclare :

> There's no question that I am in the hall of patriots, and I've come to say a couple of things to you. First, thanks for your hard work. You know, George [Tenet] and I have been spending a lot of quality time together. There's a reason. I've got a lot of confidence in him, and I've got a lot of confidence in the CIA. And so should America.

Depuis le 11-septembre, George W. Bush a en effet rencontré à plusieurs reprises George Tenet, nommé directeur de la CIA en juillet 1997. Le 17 septembre, le

président signe un *Memorandum of Notification*, c'est-à-dire une directive qui justifie la mise en œuvre d'une action spéciale et qui est ensuite remise aux commissions du Congrès chargées de contrôler l'activité des services de renseignement. Cette directive entérine le plan que Tenet lui a soumis quelques jours plus tôt et qui a pour objectif de mener des opérations spéciales contre Al-Qaïda. Le lendemain, George Bush adopte une nouvelle directive, accordant à la CIA une rallonge budgétaire de 800 millions de dollars. Ainsi, malgré le 11-septembre, la CIA demeure indispensable et elle ne tarde pas à le démontrer avec l'opération *Jawbreaker*, qui conduit des hommes de l'agence à être les premiers à pénétrer en Afghanistan le 27 septembre.

La CIA devient ainsi un instrument privilégié de la guerre contre le terrorisme et l'on est prêt à lui accorder une grande liberté d'action, comme le dit le vice-président Dick Cheney « The gloves are off. The president has given the agency the green light to do whatever is necessary. Lethal operations that were unthinkable pre-Sept. 11 are now under way. » (Woodward, 2021) Pour l'agence, et en particulier pour les hommes du *Directorate of Operations* de la CIA, on renoue ainsi avec la longue tradition de l'action clandestine de l'agence. Bien entendu, avec l'action du FBI sur le front intérieur et les opérations de surveillance de la NSA à l'extérieur, les autres composantes de ce que l'on nomme « la communauté du renseignement américaine », participent aussi de 2001 à 2021 à cette « renaissance » même si la CIA, à cause du caractère spectaculaire de ses actions spéciales, demeure l'objet d'une plus grande attention médiatique. Mais cette renaissance était probablement vouée à l'échec.

D'une part, en faisant de la guerre contre le terrorisme son principal objectif, la communauté du renseignement a eu tendance à s'affranchir, certes avec la caution de l'administration Bush, de certaines règles inhérentes à la démocratie américaine. Ce faisant, ses actions ne pouvaient pas ne pas susciter la curiosité des médias et la vigilance d'une partie du Congrès et elle a dû bientôt faire face à d'embarrassantes révélations. D'autre part, la priorité accordée à la guerre contre le terrorisme a conduit cette même communauté à négliger l'émergence de nouveaux défis, en particulier dans le cyberespace.

Nouvelle orientation : la guerre contre le terrorisme

L'orientation donnée par le président Bush à sa politique étrangère se concrétise notamment avec, en septembre 2002, la nouvelle *National Security Strategy of the United States*, un document qui depuis 1986 est établi à échéances régulières afin de définir les objectifs du gouvernement pour la préservation de la sécurité nationale. Dans ce document, qui définit les termes de la « doctrine Bush », il est demandé à la communauté du renseignement de s'adapter à la nouvelle situation et d'accorder une place de choix à la guerre contre le terrorisme :

> Intelligence – and how we use it – is our first line of defense against terrorists and the threat posed by hostile states. Designed around the priority of gathering enormous information about a massive fixed object – the Soviet bloc – the Intelligence Community is coping with the challenge of following a far more complex and elusive set of targets.

Deux ans plus tard, après la remise du rapport concernant les attentats du 11-septembre, le Congrès vote l'*Intelligence Reform and Terrorism Prevention Act* (IRTPA), une loi qui conduit à une profonde réorganisation du renseignement américain, à commencer par la création d'un *Director of National Intelligence* (DNI), sous l'autorité duquel la communauté du renseignement est désormais placée. En ce qui concerne plus précisément la guerre contre le terrorisme, le *Terrorist Threat Integration Center* (TTIC) établi par le président Bush en mai 2003 est remplacé par un *National Counterterrorism Center* (NCTC), un organisme qui a pour mission de superviser les activités antiterroristes des agences de renseignement fédérales telles que la CIA et le FBI et qui est placé sous la responsabilité de l'*Office of the Director of National Intelligence* (ODNI).

En octobre 2005, la première version de la *National Intelligence Strategy of the United States*, le document stratégique qui donne les grandes orientations en matière de politique de renseignement, confirme que la guerre contre le terrorisme est bien un objectif fondamental pour la communauté du renseignement. Le premier des six objectifs assignés au renseignement américain est dénué de toute ambiguïté: « Defeat terrorists ». À vrai dire, contrairement à l'administration Bush, la communauté du renseignement se prépare à cette transformation depuis plusieurs années. En effet, George Tenet a suivi de très près les attentats qui ont frappé, directement ou non, les États-Unis au cours des années 1990.

Il est vrai que la CIA a été la première touchée lorsque, au matin du 25 janvier 1993, deux de ses agents sont abattus par un jeune Pakistanais alors qu'ils

s'apprêtent à entrer au quartier général de Langley. Quelques jours plus tard, le 26 février, une bombe placée dans le sous-sol du *World Trade Center* de New York tue six personnes. Parmi les attentats perpétrés contre des intérêts américains à l'étranger, il faut surtout retenir ceux du 7 août 1998, qui détruisent de manière simultanée les ambassades américaines de Nairobi et Dar es-Salaam. En guise de représailles, le 20 août, le président Clinton lance plusieurs frappes aériennes contre Al-Qaïda, provoquant la mort d'une douzaine de personnes. Mais pour George Tenet la réponse n'est pas adéquate : « Instead of considering alternative approaches to the less-than-ideal cruise missile attacks, policy makers seemed to want to have things both ways : they wanted to hit Bin Ladin but without endangering U.S. troops or putting at significant risk our diplomatic relations. » (123) Quelques mois plus tard, le 3 décembre, il rédige un mémorandum sommairement intitulé « We Are At War » et dans lequel il appelle à une large mobilisation de la communauté du renseignement contre le terrorisme. Mais il prêche dans le désert.

En 1998, empêtrée dans l'affaire Lewinsky, l'administration Clinton ne parvient pas à mobiliser suffisamment contre le terrorisme et, une fois en fonction, le président Bush n'en fait pas une priorité, considérant que la lutte contre la prolifération des armes de destruction massive et la construction d'un bouclier anti-missile sont des objectifs plus importants que la neutralisation d'Al-Qaïda. En outre, comme l'ont amplement démontré les enquêtes menées par le Congrès après le 11-septembre, les agences de renseignement elles-mêmes ont fait preuve de négligence, voire d'incompétence, dans leur gestion du danger terroriste. Après les attentats, en revanche, la mobilisation est désormais totale.

Chacune des seize agences de la communauté du renseignement est sur le pied de guerre, à commencer par le FBI, qui n'a pas brillé par son efficacité avant les attentats. C'est Robert Mueller, nommé directeur le 4 septembre 2001, qui engage les changements nécessaires, forçant l'admiration de James Comey, qui lui succède en 2013 :

> I admired Bob and marveled at the way he had transformed the FBI in the aftermath of 9/11, driving the organization to break down walls, overcome its heritage as solely a detective culture, and become a fully integrated member of the intelligence community. Bob had proven that it would be a mistake to break the FBI into a criminal investigative agency and a counterterrorism agency by making the FBI great at both (122).

Mais bien évidemment la guerre contre le terrorisme ne se joue pas sur le seul territoire national et il convient d'intervenir en amont sur le terrain extérieur afin de

déjouer les menaces. Comme on l'a déjà indiqué, à l'extérieur, la CIA est aux avant-postes avec l'opération *Jawbreaker* qu'elle mène en Afghanistan. Mais la capacité opérationnelle de la CIA n'est pas illimitée.

Selon Jeremy Scahill, au moment du 11-septembre, l'agence dispose de quelque 600 ou 700 hommes formés à l'action paramilitaire, ce qui est insuffisant pour conduire une action de grande envergure (58). Elle n'a donc d'autre choix que de s'appuyer sur les forces spéciales de l'armée américaine, qui comptent alors plusieurs dizaines de milliers d'hommes. Ils sont placés sous l'autorité du *Joint Special Operations Command* (JSOC), une organisation qui depuis 1980 exécute les opérations spéciales pour le compte de l'armée américaine. Ces forces spéciales peuvent également intervenir dans le cadre d'une opération chapeautée par la CIA, ce qui permet ainsi au gouvernement américain d'en nier, théoriquement, l'existence. La porosité toujours croissante entre CIA et JSOC conduira certains membres de la communauté du renseignement à s'inquiéter de cette évolution. Ainsi, Dennis Blair, *Director of National Intelligence* (DNI) de 2009 à 2010, déplore à mots couverts ce recours à l'action clandestine : « We must acknowledge that the context has changed, and that there are more overt tools of national power [where] previously only covert action would have been applicable » (Ambinder). Mais en nommant à la tête de la CIA en 2011 David Petraeus, jusqu'alors commandant en chef des forces armées américaines en Afghanistan, le président Barack Obama apporte un désaveu cinglant à Dennis Blair. La CIA continuera à participer à la « guerre irrégulière » (Tenenbaum 89-112) même si Michael Hayden (329-330), directeur de l'agence de 2006 à 2009, a prévenu Petraeus que la CIA n'est pas supposée ressembler à l'OSS (*Office of Strategic Services*), cette agence mise en place en 1942 et dissoute trois ans plus tard par le président Harry Truman et dont la spécialité était l'action clandestine.

Outre la conduite d'opérations secrètes, la CIA apporte sa contribution à la guerre contre le terrorisme en menant de nombreuses frappes par drones interposés. Elle intervient en Afghanistan, en Somalie, au Yémen et dans les zones tribales au Pakistan où des membres d'Al-Qaïda ont trouvé refuge après le déclenchement des hostilités. Le *Bureau of Investigative Journalism*, qui s'efforce de collecter les données au sujet de ces frappes, en a comptabilisé 51 au Pakistan pour la période allant de 2004 à 2009. Mais avec l'administration du président Obama le recours aux frappes de drones s'intensifie puisque, pour la période couvrant les années 2009-2016, on en

dénombre 373, qui provoquent la mort de 2090 à 3106 personnes, parmi lesquelles entre 167 et 634 civils, dont 66 à 78 enfants[1]. Cette intensification des frappes de drones orchestrées par la CIA est vivement critiquée et, le 23 mai 2013, le président Obama décide de les justifier publiquement :

> Conventional airpower or missiles are far less precise than drones, and are likely to cause more civilian casualties and more local outrage. And invasions of these territories lead us to be viewed as occupying armies, unleash a torrent of unintended consequences, are difficult to contain, result in large numbers of civilian casualties and ultimately empower those who thrive on violent conflict.

Ce qu'Obama omet de dire c'est que les frappes de drones permettaient de ne pas s'encombrer de prisonniers, dont la gestion, comme on le verra plus bas, avait posé de sérieux problèmes à la précédente administration. Par ailleurs, le recours aux drones et autres actions clandestines s'inscrivait dans la démarche dite d'empreinte légère (« light footprint ») de l'administration Obama et elles ont permis au renseignement américain de se régénérer. Mais cette « renaissance » a été accomplie au prix d'une militarisation accrue de la CIA, qui s'est ainsi éloignée de sa mission initiale de collecte et d'analyse du renseignement. En outre, comme le démontre rapidement la vigilance exercée par les médias américains, l'agence a dévoyé cette mission avec le rapport erroné qu'elle fournit en 2002 au sujet de l'existence d'armes de destruction massive en Irak. Cette affaire ne constitue que la première d'une longue liste de révélations.

D'inévitables révélations

En octobre 2004, Charles Duelfer remet, au nom de l'*Iraq Survey Group* (ISG), un rapport de 900 pages dans lequel il conclut que l'Irak ne disposait pas de telles armes lorsque l'administration Bush a pris la décision d'y intervenir militairement en 2002. L'ISG est ce groupe de travail multinational qui est venu remplacer en 2003 la commission d'enquête portant sur les armes de destruction massive en Irak menée conjointement par l'ONU et l'Agence internationale de l'énergie atomique (AIEA). Dans ses mémoires, George Tenet finira également par l'admettre : « We allowed flawed intelligence to be presented to Congress, the President, the United Nations, and the world. That never should have happened » (383). Si le *mea culpa* de Tenet ne saurait l'exonérer, il convient néanmoins de souligner que l'administration Bush a exercé une forte pression pour que la CIA lui fournisse des éléments de preuve lui

[1] Chiffres fournis par *The Bureau of Investigative Journalism*. « Drone Warfare ». [Consulté le 4 mars 2001]. Disponible sur : https://www.thebureauinvestigates.com/projects/drone-war

permettant de lancer son opération militaire en Irak. Mais en acceptant de se soumettre à cette exigence du pouvoir exécutif, la CIA a commis l'un des péchés capitaux qui menace toujours un service de renseignement, celui de la politisation, qui consiste à apporter des renseignements qui servent les intérêts politiques du pouvoir en place. Après le déclenchement des opérations militaires en Irak, l'absence d'armes de destruction massive sur place a été rapidement constatée et les médias américains se sont empressés de relayer cette information, sommant ainsi le renseignement américain de s'expliquer. Malgré la latitude accordée aux agences de renseignement par le pouvoir politique au nom de la guerre contre le terrorisme, elles ne pouvaient espérer échapper durablement à la vigilance de médias avides de révélations.

L'affaire des armes de destruction massive est encore bien vivace lorsque la presse américaine apporte, en mars 2005, un nouveau lot de révélations au sujet du traitement infligé à des prisonniers par la CIA. Un an après les révélations concernant l'armée américaine et les méthodes d'interrogatoire dégradantes qu'elle a utilisées à la prison d'Abu Ghraib en Irak, c'est la CIA qui se trouve maintenant sur la sellette. En la matière, l'agence a une certaine expérience, ayant établi en 1963 à l'attention de ses agents un document, le *Kubark Counterintelligence Interrogation Manual*, qui proposait alors un changement de méthode : « this work then produced a new approach to torture that was psychological, not physical, perhaps best described as "no-touch torture" » (McCoy 7). Mais ce que la presse révèle en 2005, c'est que l'approche de la CIA après le 11-septembre n'a pas été que psychologique, tant s'en faut. Tout d'abord, l'agence ne peut garantir l'intégrité physique des prisonniers parce que, dans le cadre du projet *Greystone*, elle ordonne le transfert de nombreux prisonniers vers des pays tiers, une pratique nommée « rendition ». Dans ce réseau de prisons secrètes, communément appelées « black sites », la survie des prisonniers n'est pas la principale préoccupation. Le 16 mars 2005, le *New York Times* révèle ainsi que, depuis 2002, pas moins de 26 prisonniers sont morts pendant leur détention en Afghanistan ou en Irak, chiffre que Lawrence Di Rita, porte-parole du Pentagone, relativise en indiquant que les troupes américaines ont, pendant cette même période, « traité » quelque 50 000 prisonniers (Jehl). Par ailleurs, la CIA a été dûment autorisée par le ministère de la Justice à recourir à la pratique du « waterboarding » ou simulation de noyade. Les révélations de la presse provoquent une

vive émotion dans le pays, conduisant le Congrès à se saisir tardivement de cette affaire.

Les révélations concernant les interrogatoires menés par l'armée américaine à Abu Ghraib ont mené le Congrès, à l'initiative du sénateur républicain John McCain, à voter en 2005 le *Detainee Treatment Act* mais il faut attendre mars 2009 avant que le *Senate Select Committe on Intelligence* (SSCI) ne décide d'ouvrir une enquête au sujet des pratiques de la CIA vis-à-vis de ses prisonniers. La commission d'enquête, présidée par la sénatrice Dianne Feinstein, remet son rapport, totalisant 6700 pages, en décembre 2012 mais elle n'est autorisée à en rendre publique qu'une version abrégée de 449 pages (Johnson 191-205). Bien que très largement tronqué, ce rapport incite le Sénat à adopter en 2015 une disposition qui proscrit l'utilisation de techniques d'interrogation autres que celles définies par l'*Army Field Manual*.

Malgré cela, John Prados, qui consacre de nombreuses pages à cette question dans son *Histoire de la CIA*, juge que le contrôle exercé par le Congrès sur les agences de renseignement est très insuffisant : « La supervision du Congrès n'est qu'une vaste plaisanterie, quand elle n'est pas purement et simplement ignorée » (501). Il est vrai que la commission d'enquête dirigée par Dianne Feinstein a dû batailler ferme pour obtenir de la CIA les documents dont elle avait besoin et pour les conserver. Ainsi, en mars 2010, les enquêteurs de la commission sénatoriale se rendent compte que 840 documents ont été retirés de la base de données qu'ils avaient mise en place et ils arrivent rapidement à la conclusion qu'ils ont été piratés par des agents de la CIA (460-465). Sans en arriver à la même conclusion que John Prados, on ne peut que constater que l'exercice du contrôle parlementaire des activités de renseignement est une tâche bien difficile à remplir (Le Voguer 2014, 107-136), ce qui explique en partie pourquoi le Congrès semble être passé à côté d'une évolution majeure du renseignement américain en matière de collecte de données.

En décembre 2005, le *New York Times* apprend à ses lecteurs que le président Bush a signé une directive autorisant la *National Security Agency* (NSA), agence chargée depuis 1952 de la protection des secrets d'État et de la collecte du renseignement par moyens techniques interposés, à mener un programme de surveillance et la dispensant de demander au préalable une autorisation judiciaire. Bien qu'embarrassante pour l'administration Bush, cette révélation ne la conduit pas à remettre en question les pratiques de la NSA, qui multiplie les programmes de surveillance massive, comme le révèle huit ans plus tard *The Guardian*. Le 5 juin 2013,

le journal britannique annonce que la NSA a établi, depuis au moins sept ans, une gigantesque base de données contenant des communications téléphoniques effectuées depuis le territoire national. Le lendemain, le même journal révèle que la NSA recueille également des données électroniques auprès de neuf des plus grandes entreprises de la toile, dans le cadre d'un programme nommé *Prism*. Dans les jours et semaines qui suivent, les révélations se multiplient et l'on apprend, par exemple, que la NSA dispose également d'un programme, *Upstream*, qui lui permet de collecter des données directement à partir des flux Internet portés par les câbles de fibre optique. À l'origine de ces révélations il y a un homme : Edward Snowden.

Ce dernier, au moment où le *Guardian* publie son premier article, a trouvé refuge à Hong Kong et, quelques jours plus tard, il dévoile publiquement son identité. Snowden est un jeune informaticien qui travaillait pour la société privée Booz Allen Hamilton, un sous-traitant régulier de la NSA. C'est ainsi qu'il a pu recueillir des montagnes de données appartenant à la communauté du renseignement et les transmettre ensuite à la presse, ayant abouti à la conclusion que la surveillance de masse orchestrée par la NSA est liberticide : « Au terme d'une décennie de surveillance de masse, l'informatique a prouvé qu'elle servait davantage à brider la liberté qu'à lutter contre le terrorisme. » (229) Pour la communauté du renseignement, cette fuite massive de données provoque un véritable séisme. C'est à James Clapper, alors *Director of National Intelligence* (DNI), qu'il incombe d'apprendre la nouvelle au président Obama : « I […] was about to inform the president of the United States that we'd potentially had one of the worst thefts of US secrets in the history of intelligence – and that I couldn't tell him much for certain beyond that fact. This wasn't exactly the Intelligence Community's – or my – finest hour » (229). La fuite de données effectuée par Edward Snowden était en effet d'une ampleur inédite.

En fait, cette fuite, massive, de données était à la mesure de la surveillance, massive elle aussi, opérée par la NSA. Si les agences de renseignement s'adaptent à la nouvelle ère numérique, les pirates informatiques également. James Clapper comprend rapidement que la situation exige tout d'abord que la communauté du renseignement se mette au diapason de la société américaine, qui demande plus de transparence : « By the end of June we'd decided we would respond to the leaks as an integrated community, much as we'd responded to the first round of budget cuts. In doing so we would add a new word to the Intelligence Community lexicon – "transparency"» (236-237). Après avoir reçu le rapport interne qu'il a commandité suite aux

premières fuites, le président Obama promet lui aussi plus de transparence dans un discours prononcé le 17 janvier 2014. Le Congrès s'active également et adopte le USA FREEDOM Act[2]. Parallèlement, les agences prennent des mesures pour mieux protéger leurs données des dangers internes et extérieurs qui guettent le renseignement américain dans le cyberespace, ce territoire nouveau qu'il s'efforce de maîtriser.

Les défis du cyberespace

Avant d'être embauché par Booz Allen Hamilton, Edward Snowden était employé par la société Dell mais, en fait, il travaillait dans les locaux de la NSA, ce qui lui permit de constater que cette agence ne protégeait pas suffisamment ses données : « Il était assez déconcertant de voir que la NSA était à la fois très en avance en matière de cyber-renseignement et très en retard pour tout ce qui touchait à la cybersécurité. » (186) Malgré les mesures prises après les révélations de Snowden, les agences de renseignement américaines demeuraient vulnérables. Ainsi, en août 2016, un groupe de hackers mystérieux, qui opèrent sous le nom de *Shadow Brokers*, met à la disposition des internautes des fichiers subtilisés à la NSA. Ils contiennent des outils informatiques utilisés par cette agence pour procéder à du cyberespionnage et à des cyberattaques. L'annonce est accompagnée du message suivant : « Attention government sponsors of cyber warfare and those who profit from it. » Selon le *New York Times*, le piratage effectué par les *Shadow Brokers* a été encore plus dommageable que celui d'Edward Snowden (Shane). Quelques mois plus tard, en, mars 2017, c'est le site WikiLeaks qui porte à la connaissance de ses lecteurs une série de documents qui émanent du *Center for Cyber Intelligence* (CCI) de la CIA et fournissent eux aussi des informations au sujet des outils de piratage informatique utilisés par l'agence. (Nakashima) Par deux fois, donc, en moins d'un an, la communauté du renseignement a été victime de piratages, ce qui donne raison à Edward Snowden à propos des faiblesses de la communauté du renseignement en matière de cybersécurité. Ce constat nous invite à considérer comment le renseignement américain s'efforce de s'adapter à l'émergence du cyberespace.

[2] Cette loi, dont le titre USA FREEDOM Act rappelle à dessein l'USA PATRIOT Act, est un acronyme signifiant "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection, and Online Monitoring."

La prise de conscience par la communauté du renseignement des dangers inhérents au cyberespace a été progressive, suivant plus ou moins le rythme des cyberattaques qui ont frappé les États-Unis. Déjà, à la fin des années 1990, la NASA, le Pentagone et d'autres agences gouvernementales subissent pendant trois ans une puissante cyberattaque, ainsi que le révèle en 1999 l'enquête *Moonlight Maze* (Sanger 13). Cependant, ce n'est qu'en 2010 que l'armée américaine met en place un commandement interarmées exclusivement consacré au cyberespace, le *U.S. Cyber Command*. La NSA, quant à elle, dispose depuis 1998 d'une unité cyber, d'abord nommée *Tailored Access Operations* puis récemment renommée *Computer Network Operations*. À la CIA, le 11 octobre 2012, Leon Panetta met en garde contre l'éventualité d'un « cyber Pearl Harbor » et plaide pour que l'agence qu'il dirige se dote de son propre service cyber (434). En 2014, la *National Intelligence Strategy of the United States*, formulée par les services de l'*Office of the Director of National Intelligence* (ODNI) dirigé alors par James Clapper, mentionne pour la première fois la question du cyberespace et en fait une priorité. L'année suivante, sous la houlette de John Brennan, qui a succédé à Panetta en 2013, la CIA transforme son *Information Operations Center* (IOC) en une véritable direction, le *Directorate of Digital Innovation* (DDI).

La mise en place du DDI marque l'entrée définitive de la CIA dans le monde cyber et signifie aussi que l'agence commence à se détacher du processus de militarisation qu'elle avait enclenché après le 11-septembre. Bien entendu, avant la création de cette structure, elle avait déjà acquis une certaine expérience en matière de cyber-renseignement, ainsi qu'on l'a vu précédemment avec la collecte massive de données. De même, elle avait déjà investi le domaine de la cyber-conflictualité, comme en témoigne l'opération *Olympic Games* qu'elle a mise au point avec les services de renseignement israéliens en 2010. Cette opération a consisté à activer le virus *Stuxnet* afin non seulement d'infecter le système informatique du centre iranien d'enrichissement d'uranium de Natanz mais également d'en neutraliser définitivement les centrifugeuses (Aid 223-224). Trois ans après cet acte de cybersabotage, des documents dévoilés par Edward Snowden prouvent que la NSA a introduit un logiciel malveillant au cœur du système informatique de la société de télécommunications Belgacom, qui fournit ses services à différentes institutions de l'Union européenne (Delesse 387-388). À partir de 2008, la même agence lance le programme *Quantum*, qui aurait permis d'infiltrer les réseaux informatiques des ar-

mées chinoise et russe (Sanger 73). Ces quelques exemples suffisent à démontrer que le renseignement américain est bien à l'offensive dans le cyberespace, n'hésitant pas à l'occasion à s'en prendre à ses alliés européens. Mais la puissance de feu du cyber-renseignement américain ne saurait dissimuler une vulnérabilité certaine en termes de sécurité.

Quelques semaines après l'opération *Olympic Games*, plusieurs dizaines de sociétés financières américaines, parmi lesquelles JPMorgan Chase, Bank of America et Capital One, sont victimes d'un piratage informatique (Sanger 48-49). Il est revendiqué par un groupe de hackers dénommé « Izz ad-Din al-Qassam Cyber Fighters » mais on comprend rapidement qu'il a été orchestré par Téhéran. Il ne s'agissait pas d'une opération très sophistiquée mais le renseignement américain n'a pas su l'anticiper, mettant ainsi en évidence son impréparation. De même, en 2014, les agences de renseignement ont été incapables de prévenir une opération de piratage conduite par les services chinois et dont la cible était l'*Office of Personnel Management* (OPM), une institution qui recueille et conserve des données confidentielles au sujet des quelques 22 millions de personnes employées par le gouvernement américain. Cette opération de cyber-espionnage, qui a duré environ un an, a suscité l'admiration de James Clapper. En effet, en juin 2015 lors d'un symposium, il déclare : « You know, on one hand, don't take this the wrong way, you have to, kind of, salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute » (296). Sans en minimiser l'impact, le *Director of National Intelligence* indique ainsi à son auditoire que ce piratage s'apparente à une opération classique d'espionnage. Un an plus tard, en revanche, les États-Unis sont confrontés à une cyber-opération d'un autre type, qui ne risque pas d'être jugée admirable.

Le 22 juillet 2016, WikiLeaks place sur son site quelques 20 000 courriers électroniques appartenant au *Democratic National Committee* (DNC), qui font apparaître que le DNC a favorisé la candidate Hillary Clinton au détriment de son adversaire Bernie Sanders. La communauté du renseignement est rapidement convaincue que ce sont des hackers russes qui sont à la manœuvre et, le 4 août, le directeur de la CIA, John Brennan, appelle son homologue russe, Alexander Bortnikov, l'enjoignant d'ordonner à ses agents de mettre un terme à cette opération qui déstabilise l'élection présidentielle américaine qui bat alors son plein. Ce coup de téléphone ne sera pas suivi d'effets puisque, le 7 octobre, WikiLeaks annonce avoir à sa disposition 50 000 courriers électroniques de John Podesta, le directeur de campagne

d'Hillary Clinton. Les enquêtes menées ensuite par le renseignement américain et le Congrès confirmeront l'origine russe des fuites orchestrées par WikiLeaks et dévoileront le rôle joué par l'*Internet Research Agency* (IRA), une officine privée installée à Saint-Pétersbourg. Cette affaire démontre à nouveau la vulnérabilité du renseignement américain, ce que deux affaires récentes confirment.

Le 13 décembre 2020, les médias américains ont annoncé qu'un programme malveillant nommé *Sunburst* avait été introduit dans les réseaux informatiques de plusieurs sociétés privées et de diverses institutions américaines, y compris la NSA. (Perlroth) Ce programme, qui serait d'origine russe, affecte le logiciel de gestion informatique *Orion* de la firme *SolarWinds*, que toutes ces organisations utilisent. Encore plus récemment, le 6 mars 2021, le *New York Times* a informé ses lecteurs que des hackers chinois étaient parvenus à pirater le programme *Exchange* de la firme Microsoft, affectant quelque 30 000 clients de cette société américaine (Conger). L'enjeu de la cyberdéfense est une priorité pour la nouvelle administration américaine et, lors du récent sommet de l'OTAN à Bruxelles le 14 juin 2021, le président Joe Biden a invité les membres de l'organisation à mobiliser leurs forces pour y répondre.

Malgré l'échec du 11-septembre, la communauté du renseignement américaine est rapidement apparue comme un instrument indispensable pour mener la guerre contre le terrorisme, lui permettant ainsi de connaître une certaine renaissance. Mais son zèle l'a conduite à des excès coupables, qui ont été bientôt révélés par les médias et dénoncés par une partie de l'opinion publique et des parlementaires américains. Par ailleurs, en faisant de cette guerre son objectif prioritaire, elle a négligé les nouvelles menaces dans le cyberespace et n'a pas su mettre en place des moyens de cyberdéfense adéquats. La relation conflictuelle (Le Voguer, « Donald Trump ») entretenue par l'administration du président Donald Trump et son effort pour la transformer en un instrument au service de ses intérêts politiques ont retardé cette mise en place. Avril Haines, qui a été nommée *Director of National Intelligence* (DNI) par le président Biden, s'est engagée devant le Congrès à tourner la page de l'ère Trump et celle des dérives liées à la guerre contre le terrorisme, en soulignant que les impératifs de la démocratie américaine s'appliquent également à la communauté du renseignement :

> To safeguard the integrity of our Intelligence Community, the DNI must **insist** that, when it comes to intelligence, there is simply no place for politics – **ever**.
>
> The DNI must prioritize transparency, accountability, analytic rigor, facilitating oversight and diverse thinking […] To be trusted, the DNI must uphold our democratic values and ensure that the work of the Intelligence Community, mostly done in secret, is ethical, wise, lawful, and effective.

L'avenir nous dira s'il s'agit d'un vœu pieux. En attendant, Avril Haines et son service, l'*Office of the Director of National Intelligence* (ODNI), sont à la manœuvre et la cyberdéfense figure en bonne place dans leurs objectifs, tels qu'ils sont définis par l'*Annual Threat Assessment of the US Intelligence Community* qui a été rendu public le 9 avril 2021.

Bibliographie

AID, Matthew M. *Intel Wars: The Secret History of the Fight against Terror*. New York: Bloomsbury Press, 2012.

AMDINDER, Marc. « Intel Director Defends His Job, and the Job ». *The Atlantic*, April 6, 2010, https://www.theatlantic.com/politics/archive/2010/04/intel-director-defends-his-job-and-the-job/38542. Consulté le 4 mars 2021.

BUSH, George W. « The President Thanks the Agency Workforce for Its Efforts Against Terrorism ». *Studies in Intelligence* 11, Fall-Winter 2001, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/index.html. Consulté le 5 mars

CLAPPER, James R. *Facts and Fears : Hard Truths from a Life in Intelligence*. New York : Viking, 2018.

COMEY, James. *A Higher Loyalty : Truth, Lies, and Leadership*. New York : Macmillan, 2018.

CONGER, Kate, Sheera Frenkel. « Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China ». *New York Times*, March 6, 2021, https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html. Consulté le 8 mars 2021.

DELESSE, Claude. *NSA – Histoire de la plus secrète des agences de renseignement*. Paris : Tallandier/Texto, [2016] 2019.

HAINES, Avril. « Statement of Avril Haines ». January 19, 2021. *Senate Select Committee on Intelligence*, https://fas.org/irp/congress/2021_hr/index.html. Consulté le 16 juin 2021.

HAYDEN, Michael V. *Playing to the Edge : American Intelligence in the Age of Terror*. New York : Penguin Press, 2016.

JEHL, Douglas, Eric Schmitt. « U.S. Military Says 26 Inmate Deaths May Be Homicide ». *New York Times*, March 16, 2005, https://www.nytimes.com/2005/03/16/politics/us-military-says-26-inmate-deaths-may-be-homicide.html. Consulté le 16 octobre 2021.

JOHNSON, Lock K. *Spy Watching : Intelligence Accountability in the United States*. New York : Oxford University Press, 2018.

LE VOGUER, Gildas. « Donald Trump et les services de renseignement : une relation sous tension ». *Revue LISA/LISA e-journal* XVI, 2. 2018, https://journals.openedition.org/lisa/10076. Consulté le 23 décembre 2020.

——. *Le renseignement américain : Entre secret et transparence, 1947-2013*. Rennes : Presses Universitaires de Rennes, 2014.

MCCOY, Alfred W. *A Question of Torture: CIA Interrogation, from the Cold War to the War on Terror*. New York : Henry Holt & Co., 2006.

MAKASHIMA, Ellen, Shane Harris. « Elite CIA Unit Developed Hacking Tools Failed To Secure Its Own System, Allowing Massive Leak, an Internal Report Found ». *The Washington Post*, 16 juin 2020, Disponible sur: https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html.Consulté le 9 mars 2021.

OBAMA, Barack. « Remarks by the President at the National Defense University ». Washington D.C., May 23, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university. Consulté le 4 mars 2021.

OFFICE OF THE DIRECTOR OF THE NATIONAL INTELLIGENCE. « Annual Threat Assessment of the US Intelligence Community », April 9, 2021, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community. Consulté le 16 juin 2021.

PANETTA, Leon. *Worthy Fights : A Memoir of Leadership in War and Peace*. New York : Penguin, 2015.

PRADOS, John. *Histoire de la CIA : Les fantômes de Langley*. Paris : Perrin, 2019.

PERLROTH Nicole, David E SANGER, and Julian E. BARNES. « Billions Spent on U.S. Defense Failed to Detect Giant Russian Hack ». *New York Times*, December 16, 2020, https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html. Consulté le 6 janvier 2021.

SANGER, David E. *The Perfect Weapon : War, Sabotage, and Fear in the Cyber Age*. London : Scribe, 2018.

SCAHILL, Jeremy. *Dirty Wars : The World is a Battlefield*. London : Serpent's Tail, 2013.

SHANE, Scott, Nicole PERLROTH, and David E. SANGER. « Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core". *New York Times*, November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html. Consulté le 10 mars 2021.

SNOWDEN, Edward. *Mémoires vives*. Paris : Seuil, 2019.

TENENBAUM, Élie. « Les États-Unis au défi des guerres irrégulières ». *Politique américaine*. Paris : L'Harmattan, 2019/2, p. 89-112.

TENET, George. *At the Center of the Storm : My Years at the CIA*. New York : Harper Collins, 2002.

U.S. DEPARTMENT OF DEFENSE. « The National Security Strategy of the United States », September 2002, https://history.defense.gov/Historical-Sources/National-Security-Strategy. Consulté le 16 janvier 2021.

WOODWARD, Bob. « 'Gloves Are off' as CIA Pursues bin Laden ». *International Herald Tribune*, October 22, 2001.