Gregoire Chamayou

Dans la tête de la NSA

Une histoire philosophique du renseignement américain

En exposant les secrets de la NSA, Edward Snowden a révélé les méthodes du renseignement américain. Il restait cependant à en montrer les motivations réelles et l'idéologie sous-jacente. Bienvenue dans un monde où nous sommes tous devenus des sous-marins soviétiques, mais où le fantasme d'une NSA capable de tout collecter et surtout de tout analyser est tout simplement faux.

SURVEILLANCE
DRONE
PARANOIA
ANTI-TERRORISME
USA
ALGORITHMES
TECHNOLOGIES
LIBERTES

Prix Libre

sedition.noblogs.org

S·ÉDITION

Gregoire Chamayou

Dans la tête de la NSA

Une histoire philosophique du renseignement américain

En exposant les secrets de la NSA, Edward Snowden a révélé les méthodes du renseignement américain. Il restait cependant à en montrer les motivations réelles et l'idéologie sous-jacente. Bienvenue dans un monde où nous sommes tous devenus des sous-marins soviétiques, mais où le fantasme d'une NSA capable de tout collecter et surtout de tout analyser est tout simplement faux.

SURVEILLANCE
DRONE
PARANOIA
ANTI-TERRORISME
USA
ALGORITHMES
TECHNOLOGIES
LIBERTES

Prix Libre

sedition.noblogs.org

S·ÉDITION

D'autres textes

A lire ou télécharger sur sedition.noblogs.org

- Gunter Anders – La fin du Pacifisme
- Peter Gelderloos – La non-violence est inéfficace
- Que faire pour empêcher la police de tuer ?
- Comme un chien enragé – lettre d'un prisonniers
- Violence de la Légitimité Légitimité de la Violence
- Elsa Dorlin – Ce que peut un corps
- Ballast – Comprendre la « violence judiciaire »
- Mathieu Rigouste - L'ordre sécuritaire et le soulèvement des quartiers populaires
- Quadrupppani et Floch - Pourquoi les flics sont-ils tous des bâtards ?
- Techique De Pouvoir Pastoral
- Maré Almani – Qu'est-ce que le terrorisme ?

s-edition@riseup.net

Vers « l'âge d'or du renseignement électromagnétique »....2
L'utopie du datamining antiterroriste....5
« Collect it all »....14
Surveillance programmatique et machines à remonter le temps....19
Une question de pouvoir....23
Les yeux et les oreilles de la machine de guerre....25
L'écusson de Geocell....28
À la recherche des « inconnus inconnus »....31
Notes....41

D'autres textes....45

D'autres textes

A lire ou télécharger sur sedition.noblogs.org

- Gunter Anders – La fin du Pacifisme
- Peter Gelderloos – La non-violence est inéfficace
- Que faire pour empêcher la police de tuer ?
- Comme un chien enragé – lettre d'un prisonniers
- Violence de la Légitimité Légitimité de la Violence
- Elsa Dorlin – Ce que peut un corps
- Ballast – Comprendre la « violence judiciaire »
- Mathieu Rigouste - L'ordre sécuritaire et le soulèvement des quartiers populaires
- Quadrupppani et Floch - Pourquoi les flics sont-ils tous des bâtards ?
- Techique De Pouvoir Pastoral
- Maré Almani – Qu'est-ce que le terrorisme ?

s-edition@riseup.net

[63] « Activity Based Intelligence ». Les grands axes de cette méthodologie émergente furent posés en 2010 dans une série de documents stratégiques confidentiels rédigés par Robert Arbetter, un ancien cadre de la NGA devenu directeur pour les stratégies et les concepts de collection auprès du sous-secrétaire d'État à la Défense en charge du renseignement.
[64] G. Treverton, « Creatively disrupting the intelligence paradigm », ISN, 13/08/11.
[65] E. Tse, « Activity based intelligence challenges », IMSC Retreat, 07/03/13.
[66] Cf. M. Phillips, « A brief overview of ABI », Trajectory Magazine, 2012.
[67] « From data to decisions III », IBM Center for the Business of Government, 2013, p. 32.
[68] K. Streib, M. Nedrich, K. Sankaranarayanan, J. Davis « Interactive visualization and behavior analysis for video surveillance », SIAM Data Mining Conference, 2010.
[69] Cf. B. Borghetti, « Anomaly detection through behavior signatures », ISRCS Briefing, 10/08/10.
[70] R. Lane, K. Copsey, « Track anomaly detection », FUSION 2012 Conference.
[71] Georges Canguilhem, « Le normal et le pathologique », in La Connaissance de la vie, Vrin, Paris, 1992, p. 208.
[72] Ibid., p. 205.
[73] Cf. J. Llinas, J. Scrofani, Foundational technologies for ABI. A review of the literature, Naval Postgraduate School, Monterey, 2014.
[74] Cf. J. Crampton, S. Roberts, A. Poorthuis, « The new political economy of geographical intelligence », Annals of the AAG, 104/1, 2014.
[75] D. Gauthier, « ABI : NGA initiatives », Next Generation ISR Symposium 10/12/13.
[76] Gauthier cite ici K. Cukier, V. Mayer-Schoenberger, « The rise of big data », Foreign Affairs, mai-juin 2013.
[77] M. Kelley, G. Ingersoll, « Purported NSA slides refer To iPhone owners as "zombies" », Business Insider, 10/09/13.
[78] C'était le Millennium Challenge 2002 ; cf. J. Borger, « Wake-up call », Guardian, 06/09/02.
[79] Comité invisible, À nos amis, La Fabrique, Paris, 2014, p. 117.
[80] V. Serge, Ce que tout révolutionnaire doit savoir de la répression, Zones/ La Découverte, Paris, 2009, p. 62.

Texte initialement publié en 2015
dans la *Revue du Crieur*.

6 juillet 1962, base NAVFAC, île de la Barbade.

Dans un bâtiment gris planté au pied d'un phare en pierre surplombant la mer des Caraïbes, un militaire scrute les lignes que trace face à lui, sur un énorme rouleau de papier, le stylet d'une sorte d'électrocardiogramme géant. Nous sommes dans l'une des bases secrètes du réseau SOSUS (SOund SUrveillance System) mis en place par l'US Navy dans les années 1950. Ce que l'homme cherche, dans cet embrouillamini de hachures où il a appris à lire le son des océans, c'est une « signature ». Ce jour-là, il repère pour la première fois le signal d'un sous-marin nucléaire soviétique[1].

Le problème de la guerre sous-marine était que les engins ennemis se dérobaient aux regards. Mais ce que l'on ne pouvait pas voir, on pouvait l'entendre : l'eau dans laquelle se cachaient les sous-marins propageait au loin les sons de leurs moteurs. C'est ainsi que la mer fut mise sur écoute. Les ondes sonores captées par des hydrophones étaient transmises par câble à des stations côtières où des machines les transcrivaient en graphes. Les « techniciens des

[63] « Activity Based Intelligence ». Les grands axes de cette méthodologie émergente furent posés en 2010 dans une série de documents stratégiques confidentiels rédigés par Robert Arbetter, un ancien cadre de la NGA devenu directeur pour les stratégies et les concepts de collection auprès du sous-secrétaire d'État à la Défense en charge du renseignement.
[64] G. Treverton, « Creatively disrupting the intelligence paradigm », ISN, 13/08/11.
[65] E. Tse, « Activity based intelligence challenges », IMSC Retreat, 07/03/13.
[66] Cf. M. Phillips, « A brief overview of ABI », Trajectory Magazine, 2012.
[67] « From data to decisions III », IBM Center for the Business of Government, 2013, p. 32.
[68] K. Streib, M. Nedrich, K. Sankaranarayanan, J. Davis « Interactive visualization and behavior analysis for video surveillance », SIAM Data Mining Conference, 2010.
[69] Cf. B. Borghetti, « Anomaly detection through behavior signatures », ISRCS Briefing, 10/08/10.
[70] R. Lane, K. Copsey, « Track anomaly detection », FUSION 2012 Conference.
[71] Georges Canguilhem, « Le normal et le pathologique », in La Connaissance de la vie, Vrin, Paris, 1992, p. 208.
[72] Ibid., p. 205.
[73] Cf. J. Llinas, J. Scrofani, Foundational technologies for ABI. A review of the literature, Naval Postgraduate School, Monterey, 2014.
[74] Cf. J. Crampton, S. Roberts, A. Poorthuis, « The new political economy of geographical intelligence », Annals of the AAG, 104/1, 2014.
[75] D. Gauthier, « ABI : NGA initiatives », Next Generation ISR Symposium 10/12/13.
[76] Gauthier cite ici K. Cukier, V. Mayer-Schoenberger, « The rise of big data », Foreign Affairs, mai-juin 2013.
[77] M. Kelley, G. Ingersoll, « Purported NSA slides refer To iPhone owners as "zombies" », Business Insider, 10/09/13.
[78] C'était le Millennium Challenge 2002 ; cf. J. Borger, « Wake-up call », Guardian, 06/09/02.
[79] Comité invisible, À nos amis, La Fabrique, Paris, 2014, p. 117.
[80] V. Serge, Ce que tout révolutionnaire doit savoir de la répression, Zones/ La Découverte, Paris, 2009, p. 62.

44

Texte initialement publié en 2015
dans la *Revue du Crieur*.

6 juillet 1962, base NAVFAC, île de la Barbade.

Dans un bâtiment gris planté au pied d'un phare en pierre surplombant la mer des Caraïbes, un militaire scrute les lignes que trace face à lui, sur un énorme rouleau de papier, le stylet d'une sorte d'électrocardiogramme géant. Nous sommes dans l'une des bases secrètes du réseau SOSUS (SOund SUrveillance System) mis en place par l'US Navy dans les années 1950. Ce que l'homme cherche, dans cet embrouillamini de hachures où il a appris à lire le son des océans, c'est une « signature ». Ce jour-là, il repère pour la première fois le signal d'un sous-marin nucléaire soviétique[1].

Le problème de la guerre sous-marine était que les engins ennemis se dérobaient aux regards. Mais ce que l'on ne pouvait pas voir, on pouvait l'entendre : l'eau dans laquelle se cachaient les sous-marins propageait au loin les sons de leurs moteurs. C'est ainsi que la mer fut mise sur écoute. Les ondes sonores captées par des hydrophones étaient transmises par câble à des stations côtières où des machines les transcrivaient en graphes. Les « techniciens des

1

océans » qui les déchiffraient étaient capables de « *discerner les subtiles nuances de signaux sonores dont l'intensité, la coloration, les formes ou les ombrés font toute la différence entre un banc de poissons et un sous-marin vus par lofargramme* [nom du graphique que tracent ces machines, dites « LOFAR » (Low Frequency Analysis and Recording)] *interposé* [2] ». Ils entendaient avec les yeux.

Les motifs caractéristiques correspondant à des entités connues étaient appelés des « signatures ». On saisit la métaphore : là comme ailleurs, l'identité s'atteste par certains traits inscrits sur du papier. Les cibles, dénoncées par leurs propres signaux, pouvaient alors être identifiées avant d'être localisées. Tout cela allait connaître une fortune très imprévue. Quelques décennies plus tard, ce modèle combinant système d'écoute globale, collecte massive de signaux et télédétection par reconnaissance de signatures allait servir de matrice conceptuelle pour un tout autre dispositif de surveillance.

Vers « l'âge d'or du renseignement électromagnétique »

À la fin des années 1990, la National Security Agency (NSA) avait compris que quelque chose de

[37] E. Snowden, « An open letter to the people of Brazil », Folha de S. Paulo, 16/12/13.
[38]
[39] M. Flynn, R. Juergens, T. Cantrell, « Employing ISR », Joint Forces Quarterly, n° 50, été 2008, p. 57. Cf. aussi D. Houff, « Antisubmarine warfare concepts offer promise for counterterrorism », Signal, mai 2010.
[40] OUSDAT, Report on Defense Intelligence COIN ISR Operations, février 2011, p. 28.
[41] R. Wood, T. McPherson, « Video track screening using syntactic activity-based methods », AIPR Workshop, IEEE, 2012.
[42] Cf. J. Scahill, G. Greenwald, « The NSA's secret role in the US assassination program », The Intercept, 10/02/14.
[43] B. Woodward, Obama's Wars, Simon & Schuster, New York, 2010, p. 7.
[44] « Change Agent », Defense News, 08/10/10.
[45] T. Lash, « Integrated persistent ISR », Geospatial Intelligence Forum, 08/04/10.
[46] D. Priest, « NSA growth fueled by need to target terrorists », Washington Post, 21/07/13.
[47] B. Drogin, « Two agencies melding minds on intelligence », LA Times, 31/12/04.
[48] Cf. « Training the corps », Military Intelligence, 31/1, janvier 2005, p. 54.
[49] [50] D. Gregory, « Lines of descent », Open democracy, 08/11/11.
[51] Flynn, Juergens, Cantrell, « Employing ISR », loc. cit., p. 1.
[52] S. McChrystal, « It takes a network », Foreign Policy, 21/02/11.
[53] S. McChrystal, « Generation kill », Foreign Affairs, mars 2013.
[54] Ibid.
[55] John Inglis, Remarks at GEOINT Symposium, 04/11/10.
[56] G. Porter, « How McChrystal and Petraeus built an indiscriminate "Killing Machine" », Truthout, 26/09/11.
[57] Ibid.
[58] Taipale, « The privacy implications… », loc. cit., p. 3.
[59] J. Foust, « Unaccountable killing machines », Atlantic, 30/12/11. Cf. aussi J. Scahill, Dirty Wars, Lux, Montréal, 2014.
[60] Voir The Civilian Impact of Drones, septembre 2012, p. 8. Mais, comme le précise Gregory, « ceux qui pensent que les "frappes de personnalité" seraient moins fatales devraient aussi lire le dernier rapport de l'ONG Reprieve : "You never die twice" ».
[61] Cité par G. Miller, « Activity-based intelligence », Defense News, 08/07/13.
[62] L. Long, « Activity based intelligence understanding the unknown », The Intelligencer, 20/2/13, p. 7.

océans » qui les déchiffraient étaient capables de « *discerner les subtiles nuances de signaux sonores dont l'intensité, la coloration, les formes ou les ombrés font toute la différence entre un banc de poissons et un sous-marin vus par lofargramme* [nom du graphique que tracent ces machines, dites « LOFAR » (Low Frequency Analysis and Recording)] *interposé* [2] ». Ils entendaient avec les yeux.

Les motifs caractéristiques correspondant à des entités connues étaient appelés des « signatures ». On saisit la métaphore : là comme ailleurs, l'identité s'atteste par certains traits inscrits sur du papier. Les cibles, dénoncées par leurs propres signaux, pouvaient alors être identifiées avant d'être localisées. Tout cela allait connaître une fortune très imprévue. Quelques décennies plus tard, ce modèle combinant système d'écoute globale, collecte massive de signaux et télédétection par reconnaissance de signatures allait servir de matrice conceptuelle pour un tout autre dispositif de surveillance.

Vers « l'âge d'or du renseignement électromagnétique »

À la fin des années 1990, la National Security Agency (NSA) avait compris que quelque chose de

2

[37] E. Snowden, « An open letter to the people of Brazil », Folha de S. Paulo, 16/12/13.
[38]
[39] M. Flynn, R. Juergens, T. Cantrell, « Employing ISR », Joint Forces Quarterly, n° 50, été 2008, p. 57. Cf. aussi D. Houff, « Antisubmarine warfare concepts offer promise for counterterrorism », Signal, mai 2010.
[40] OUSDAT, Report on Defense Intelligence COIN ISR Operations, février 2011, p. 28.
[41] R. Wood, T. McPherson, « Video track screening using syntactic activity-based methods », AIPR Workshop, IEEE, 2012.
[42] Cf. J. Scahill, G. Greenwald, « The NSA's secret role in the US assassination program », The Intercept, 10/02/14.
[43] B. Woodward, Obama's Wars, Simon & Schuster, New York, 2010, p. 7.
[44] « Change Agent », Defense News, 08/10/10.
[45] T. Lash, « Integrated persistent ISR », Geospatial Intelligence Forum, 08/04/10.
[46] D. Priest, « NSA growth fueled by need to target terrorists », Washington Post, 21/07/13.
[47] B. Drogin, « Two agencies melding minds on intelligence », LA Times, 31/12/04.
[48] Cf. « Training the corps », Military Intelligence, 31/1, janvier 2005, p. 54.
[49] [50] D. Gregory, « Lines of descent », Open democracy, 08/11/11.
[51] Flynn, Juergens, Cantrell, « Employing ISR », loc. cit., p. 1.
[52] S. McChrystal, « It takes a network », Foreign Policy, 21/02/11.
[53] S. McChrystal, « Generation kill », Foreign Affairs, mars 2013.
[54] Ibid.
[55] John Inglis, Remarks at GEOINT Symposium, 04/11/10.
[56] G. Porter, « How McChrystal and Petraeus built an indiscriminate "Killing Machine" », Truthout, 26/09/11.
[57] Ibid.
[58] Taipale, « The privacy implications… », loc. cit., p. 3.
[59] J. Foust, « Unaccountable killing machines », Atlantic, 30/12/11. Cf. aussi J. Scahill, Dirty Wars, Lux, Montréal, 2014.
[60] Voir The Civilian Impact of Drones, septembre 2012, p. 8. Mais, comme le précise Gregory, « ceux qui pensent que les "frappes de personnalité" seraient moins fatales devraient aussi lire le dernier rapport de l'ONG Reprieve : "You never die twice" ».
[61] Cité par G. Miller, « Activity-based intelligence », Defense News, 08/07/13.
[62] L. Long, « Activity based intelligence understanding the unknown », The Intelligencer, 20/2/13, p. 7.

43

the Constitution », Mich. Telecommunications and Technology Law Review, mai 2015.

[20] B. Gellman, A. Soltani, « NSA infiltrates links to Yahoo, Google data centers », Washington Post, 30/10/13.

[21]

[22] La logique sous-jacente est la suivante, exposée dans un document de l'agence : « Comment trouver une cellule terroriste n'ayant pas de connexion avec des sélecteurs identifiés ? Réponse : cherchez des événements anormaux. Par exemple quelqu'un qui utilise une langue décalée par rapport à la région où il se trouve. Quelqu'un qui utilise des logiciels de cryptage. Quelqu'un qui cherche des trucs suspects sur le net », cf. A. Davidson, « Presenting XKeyscore », The New Yorker, 31/06/13.

[23] Office of the Inspector General, ST-09-000, 24/03/09, p. 13.

[24] NAS, PPD-28 Report : Bulk Collection of Signals Intelligence, 2015, 3-3.

[25] PCLOB, Report on the Telephone Records Program, op cit., p. 29.

[26] C'est la Foreign Intelligence Surveillance Court (FISC). Cf. W. Banks, « Programmatic Surveillance and FISA », Texas Law Review, 88/7, juin 2010.

[27] K. Tummarello, « NSA's work is like "stop and frisk" », The Hill, 11/04/13.

[28] B. Gellman, A. Soltani, « NSA surveillance program reaches "into the past" », Washington Post, 18/03/14.

[29]

[30] R. Devereaux, G. Greenwald, L. Poitras, « Data pirates of the Caribbeans », Intercept, 19/05/14.

[31] Gellman et Soltani, « NSA surveillance program reaches… », loc. cit.

[32] Ibid.

[33] S. Ackerman, « Senators challenge NSA's claim », Guardian, 13/06/13.

[34] S. Waterman, « NSA chief's admission of misleading numbers », Washington Times, 02/10/13. Cf. aussi B. Schneier, « How the NSA Threatens National Security », Atlantic, 06/01/14.

[35] La commission qui a examiné le programme de métadonnées aboutit au même genre de conclusion : « Nous n'avons trouvé trace d'aucun cas de menace envers les États-Unis où ce programme ait eu le moindre apport concret pour les investigations antiterroristes. En outre, à notre connaissance, il n'y a aucun cas où ce programme ait directement contribué à la découverte d'un complot terroriste jusque-là inconnu », PCLOB, Report on the Telephone Records Program, 23/01/14, p. 11.

[36] « Stabilizing Transatlantic relations after the NSA revelations », loc. cit.

nouveau était en train de se produire et qui promettait, à la condition de triompher de certains obstacles, une extension inouïe de son empire. L'agence était historiquement chargée de l'interception des signaux électromagnétiques pour le renseignement extérieur – câbles diplomatiques, communications militaires, faisceaux satellitaires… Mais, en cette fin de millénaire, les populations civiles se mettaient à leur tour à devenir des émetteurs de signaux. Un monde se connectait, où chacun d'entre nous allait bientôt produire davantage de données qu'aucune ambassade soviétique par le passé. Alors que les utilisateurs découvraient le son strident du modem analogique et les couleurs flashy des portables Nokia, les grandes oreilles du renseignement y voyaient un grand défi, un nouvel espace à conquérir.

Se souvenant de l'état d'esprit qui régnait à cette époque – une époque de pionniers –, l'ancien directeur de la NSA Michael Hayden confie benoîtement aujourd'hui : « *Alors que nous assistions au développement des moyens de télécommunication modernes, nous nous disions que nous avions un problème, […] les télécommunications étaient en train d'exploser en volume et en variété, et de muer à toute vitesse. Mais nous savions aussi que l'humanité était […]*

the Constitution », Mich. Telecommunications and Technology Law Review, mai 2015.

[20] B. Gellman, A. Soltani, « NSA infiltrates links to Yahoo, Google data centers », Washington Post, 30/10/13.

[21]

[22] La logique sous-jacente est la suivante, exposée dans un document de l'agence : « Comment trouver une cellule terroriste n'ayant pas de connexion avec des sélecteurs identifiés ? Réponse : cherchez des événements anormaux. Par exemple quelqu'un qui utilise une langue décalée par rapport à la région où il se trouve. Quelqu'un qui utilise des logiciels de cryptage. Quelqu'un qui cherche des trucs suspects sur le net », cf. A. Davidson, « Presenting XKeyscore », The New Yorker, 31/06/13.

[23] Office of the Inspector General, ST-09-000, 24/03/09, p. 13.

[24] NAS, PPD-28 Report : Bulk Collection of Signals Intelligence, 2015, 3-3.

[25] PCLOB, Report on the Telephone Records Program, op cit., p. 29.

[26] C'est la Foreign Intelligence Surveillance Court (FISC). Cf. W. Banks, « Programmatic Surveillance and FISA », Texas Law Review, 88/7, juin 2010.

[27] K. Tummarello, « NSA's work is like "stop and frisk" », The Hill, 11/04/13.

[28] B. Gellman, A. Soltani, « NSA surveillance program reaches "into the past" », Washington Post, 18/03/14.

[29]

[30] R. Devereaux, G. Greenwald, L. Poitras, « Data pirates of the Caribbeans », Intercept, 19/05/14.

[31] Gellman et Soltani, « NSA surveillance program reaches… », loc. cit.

[32] Ibid.

[33] S. Ackerman, « Senators challenge NSA's claim », Guardian, 13/06/13.

[34] S. Waterman, « NSA chief's admission of misleading numbers », Washington Times, 02/10/13. Cf. aussi B. Schneier, « How the NSA Threatens National Security », Atlantic, 06/01/14.

[35] La commission qui a examiné le programme de métadonnées aboutit au même genre de conclusion : « Nous n'avons trouvé trace d'aucun cas de menace envers les États-Unis où ce programme ait eu le moindre apport concret pour les investigations antiterroristes. En outre, à notre connaissance, il n'y a aucun cas où ce programme ait directement contribué à la découverte d'un complot terroriste jusque-là inconnu », PCLOB, Report on the Telephone Records Program, 23/01/14, p. 11.

[36] « Stabilizing Transatlantic relations after the NSA revelations », loc. cit.

42

nouveau était en train de se produire et qui promettait, à la condition de triompher de certains obstacles, une extension inouïe de son empire. L'agence était historiquement chargée de l'interception des signaux électromagnétiques pour le renseignement extérieur – câbles diplomatiques, communications militaires, faisceaux satellitaires… Mais, en cette fin de millénaire, les populations civiles se mettaient à leur tour à devenir des émetteurs de signaux. Un monde se connectait, où chacun d'entre nous allait bientôt produire davantage de données qu'aucune ambassade soviétique par le passé. Alors que les utilisateurs découvraient le son strident du modem analogique et les couleurs flashy des portables Nokia, les grandes oreilles du renseignement y voyaient un grand défi, un nouvel espace à conquérir.

Se souvenant de l'état d'esprit qui régnait à cette époque – une époque de pionniers –, l'ancien directeur de la NSA Michael Hayden confie benoîtement aujourd'hui : « *Alors que nous assistions au développement des moyens de télécommunication modernes, nous nous disions que nous avions un problème, […] les télécommunications étaient en train d'exploser en volume et en variété, et de muer à toute vitesse. Mais nous savions aussi que l'humanité était […]*

3

en train de placer l'ensemble de sa connaissance sous une forme susceptible d'être interceptée par le renseignement électromagnétique. Donc, pour être francs, notre vision des choses, même avant le 11 Septembre, était que si nous parvenions à maîtriser ne serait-ce que la moitié de cette révolution dans les télécommunications mondiales, nous entrerions dans l'âge d'or du renseignement électromagnétique. Très franchement, c'est cela que la NSA comptait faire[3]. »

Puis les deux avions percutèrent les Tours. Avec eux, les débats sur les « *failles du système de renseignement* », sur « *l'équilibre entre liberté et sécurité* », et leurs suites prévisibles. Le 4 octobre 2001, George Bush autorisa temporairement de nouveaux dispositifs secrets de surveillance électronique, regroupés sous l'appellation de Programme de surveillance du président (PSP). Ces mesures d'exception furent indéfiniment reconduites. On ne tarda pas à comprendre, comme le rapporte un rapport déclassifié sur le PSP, qu'il s'agissait « *moins d'une réponse provisoire aux attentats terroristes du 11 Septembre que d'un instrument de surveillance permanente* ».

Notes

[1] O. Cote, *The Third Battle*, Naval War College Papers 16, Newport, 2003, p. 39.
[2] *Cf.* G. Weir, « The American sound surveillance system », *Int. Journal of Naval History*, 5/2/06.
[3] « Stabilizing Transatlantic relations after the NSA revelations », Atlantic Council, 08/11/13.
[4] S. Greenblatt, T. Coffman, S. Marcus, « Behavioral network analysis for terrorist detection », *in* R. Popp, J. Yen, *Emergent Information Technologies*, Wiley-IEEE, Hoboken, 2006, p. 334.
[5] *House Hearing*, « Can the use of factual data strengthen national security ? », 20/05/03, p. 85. *Cf.* aussi S. Harris, *The Watchers*, Penguin, New York, 2010.
[6] Cité par S. Harris, *The Watchers, op. cit.*
[7] J. Jonas, J. Harper, « Effective counterterrorism », *Policy Analysis*, n° 584, Cato Institute, 11/01/06, p. 8. *Cf.* aussi J. Rosen, *The Naked Crowd*, Random House, New York, 2004.
[8] K. Taipale, « The privacy implications of government data mining program », *Testimony*, 10/01/07, p. 3. *Cf.* aussi D. Jensen, M. Rattigen, H. Blau, « Information awareness », *Proceedings of the ACM Conference*, 2003.
[9] G. Greenwald, M. Hussain, « Meet the Muslim-American leaders », *The Intercept*, 7/09/14.
[10] Jensen, Rattigen, Blau, « Information awareness », *loc. cit.*
[11] Plusieurs modules du programme furent transférés à la NSA (*Cf.* S. Harris, « TIA lives on », *National Journal,* 23/02/06).
[12] *Cf.* K. Alexander, J. Heath, *et al.*, « Automating markup of intelligence community data », *Defense Intelligence Journal,* 12/02/03, p. 84.
[13] *Cf.* Harris, *The Watchers, op. cit.*
[14] S. Harris, « The cowboy of the NSA », *Foreign Policy*, 9/09/13.
[15] E. Nakashima, J. Warrick, « For NSA chief, terrorist threat drives passion to "collect it all" », *Washington Post,* 14/07/13.
[16] PCLOB, *Report on the Telephone Records Program*, 23/01/14, p. 8.
[17] ODNI, *Report Regarding use of National Security Authorities*, 26/06/14, p. 2.
[18] Cf. PCLOB, Report on the Surveillance Program, 02/07/14, p. 124. Cf. aussi B. Gellman, J. Tate, A. Soltani, « In NSA-intercepted data », Washington Post, 05/07/14.
[19] Cf. J. Napier Tye, « Meet Executive Order 12333 », Washington Post, 18/07/14. Cf. aussi A. Arnbak, S. Goldberg, « Loopholes for Circumventing

en train de placer l'ensemble de sa connaissance sous une forme susceptible d'être interceptée par le renseignement électromagnétique. Donc, pour être francs, notre vision des choses, même avant le 11 Septembre, était que si nous parvenions à maîtriser ne serait-ce que la moitié de cette révolution dans les télécommunications mondiales, nous entrerions dans l'âge d'or du renseignement électromagnétique. Très franchement, c'est cela que la NSA comptait faire[3]. »

Puis les deux avions percutèrent les Tours. Avec eux, les débats sur les « *failles du système de renseignement* », sur « *l'équilibre entre liberté et sécurité* », et leurs suites prévisibles. Le 4 octobre 2001, George Bush autorisa temporairement de nouveaux dispositifs secrets de surveillance électronique, regroupés sous l'appellation de Programme de surveillance du président (PSP). Ces mesures d'exception furent indéfiniment reconduites. On ne tarda pas à comprendre, comme le rapporte un rapport déclassifié sur le PSP, qu'il s'agissait « *moins d'une réponse provisoire aux attentats terroristes du 11 Septembre que d'un instrument de surveillance permanente* ».

Notes

[1] O. Cote, *The Third Battle*, Naval War College Papers 16, Newport, 2003, p. 39.
[2] *Cf.* G. Weir, « The American sound surveillance system », *Int. Journal of Naval History*, 5/2/06.
[3] « Stabilizing Transatlantic relations after the NSA revelations », Atlantic Council, 08/11/13.
[4] S. Greenblatt, T. Coffman, S. Marcus, « Behavioral network analysis for terrorist detection », *in* R. Popp, J. Yen, *Emergent Information Technologies*, Wiley-IEEE, Hoboken, 2006, p. 334.
[5] *House Hearing*, « Can the use of factual data strengthen national security ? », 20/05/03, p. 85. *Cf.* aussi S. Harris, *The Watchers*, Penguin, New York, 2010.
[6] Cité par S. Harris, *The Watchers, op. cit.*
[7] J. Jonas, J. Harper, « Effective counterterrorism », *Policy Analysis*, n° 584, Cato Institute, 11/01/06, p. 8. *Cf.* aussi J. Rosen, *The Naked Crowd*, Random House, New York, 2004.
[8] K. Taipale, « The privacy implications of government data mining program », *Testimony*, 10/01/07, p. 3. *Cf.* aussi D. Jensen, M. Rattigen, H. Blau, « Information awareness », *Proceedings of the ACM Conference*, 2003.
[9] G. Greenwald, M. Hussain, « Meet the Muslim-American leaders », *The Intercept*, 7/09/14.
[10] Jensen, Rattigen, Blau, « Information awareness », *loc. cit.*
[11] Plusieurs modules du programme furent transférés à la NSA (*Cf.* S. Harris, « TIA lives on », *National Journal,* 23/02/06).
[12] *Cf.* K. Alexander, J. Heath, *et al.*, « Automating markup of intelligence community data », *Defense Intelligence Journal,* 12/02/03, p. 84.
[13] *Cf.* Harris, *The Watchers, op. cit.*
[14] S. Harris, « The cowboy of the NSA », *Foreign Policy*, 9/09/13.
[15] E. Nakashima, J. Warrick, « For NSA chief, terrorist threat drives passion to "collect it all" », *Washington Post,* 14/07/13.
[16] PCLOB, *Report on the Telephone Records Program*, 23/01/14, p. 8.
[17] ODNI, *Report Regarding use of National Security Authorities*, 26/06/14, p. 2.
[18] Cf. PCLOB, Report on the Surveillance Program, 02/07/14, p. 124. Cf. aussi B. Gellman, J. Tate, A. Soltani, « In NSA-intercepted data », Washington Post, 05/07/14.
[19] Cf. J. Napier Tye, « Meet Executive Order 12333 », Washington Post, 18/07/14. Cf. aussi A. Arnbak, S. Goldberg, « Loopholes for Circumventing

Facebook que l'individu censé se cacher derrière [79] », se rend aussi très vulnérable.

Dans une autre perspective, l'avenir dira peut-être si les lignes suivantes, écrites au début d'un siècle révolu, auront conservé leur pertinence. Victor Serge y évoquait les moyens déployés par la police politique tsariste contre les mouvements révolutionnaires : « *Quelle que soit la perfection des méthodes mises en œuvre pour les surveiller, n'y aura-t-il pas toujours, dans leurs faits et gestes, une inconnue irréductible ? N'y aura-t-il pas toujours, dans les équations le plus laborieusement élaborées par leur ennemi, un grand X redoutable ? [...] les milliers de dossiers de l'_Okhrana, _les millions de fiches du service de renseignement, les merveilleux graphiques de ses techniciens, les ouvrages de ses savants – tout ce mirifique arsenal est aujourd'hui entre les mains des communistes russes. Les "flics", un jour d'émeute, se sont sauvés sous les huées de la foule* [80]*. »*

L'appareil d'État était aux abois. Si une telle chose avait pu se produire, c'est que les services de renseignement avaient failli. Leurs responsables le savaient : des têtes allaient tomber. On leur demandait des solutions. Et ils n'en avaient pas, pas réellement. Certains, cependant, nourrissaient des projets extravagants ; et c'était le moment de les mettre en œuvre, pensaient-ils, car une nation ébranlée est prête à tout. À la suite du 11 Septembre, les docteurs Folamour du renseignement se sentirent pousser des ailes.

L'UTOPIE DU *DATAMINING* ANTITERRORISTE

Le logo montrait une pyramide surmontée d'un œil qui voit tout, façon *Illuminati*, flottant dans l'espace et bombardant la terre de rayons lumineux. C'était l'emblème d'un programme de recherche lancé par la DARPA (la grande agence de recherche militaire américaine), un projet de surveillance électronique intitulé « Total Information Awareness ». Ce dessin imbécile, qu'on aurait dit fait exprès pour alimenter des délires conspirationnistes, était rehaussé d'une maxime latine qui, en un sens, sauvait l'ensemble : « *Scientia est potentia* », le savoir, c'est du pouvoir. Il ne s'agissait, effectivement, que de cela.

Facebook que l'individu censé se cacher derrière [79] », se rend aussi très vulnérable.

Dans une autre perspective, l'avenir dira peut-être si les lignes suivantes, écrites au début d'un siècle révolu, auront conservé leur pertinence. Victor Serge y évoquait les moyens déployés par la police politique tsariste contre les mouvements révolutionnaires : « *Quelle que soit la perfection des méthodes mises en œuvre pour les surveiller, n'y aura-t-il pas toujours, dans leurs faits et gestes, une inconnue irréductible ? N'y aura-t-il pas toujours, dans les équations le plus laborieusement élaborées par leur ennemi, un grand X redoutable ? [...] les milliers de dossiers de l'_Okhrana, _les millions de fiches du service de renseignement, les merveilleux graphiques de ses techniciens, les ouvrages de ses savants – tout ce mirifique arsenal est aujourd'hui entre les mains des communistes russes. Les "flics", un jour d'émeute, se sont sauvés sous les huées de la foule* [80]*. »*

40

L'appareil d'État était aux abois. Si une telle chose avait pu se produire, c'est que les services de renseignement avaient failli. Leurs responsables le savaient : des têtes allaient tomber. On leur demandait des solutions. Et ils n'en avaient pas, pas réellement. Certains, cependant, nourrissaient des projets extravagants ; et c'était le moment de les mettre en œuvre, pensaient-ils, car une nation ébranlée est prête à tout. À la suite du 11 Septembre, les docteurs Folamour du renseignement se sentirent pousser des ailes.

L'UTOPIE DU *DATAMINING* ANTITERRORISTE

Le logo montrait une pyramide surmontée d'un œil qui voit tout, façon *Illuminati*, flottant dans l'espace et bombardant la terre de rayons lumineux. C'était l'emblème d'un programme de recherche lancé par la DARPA (la grande agence de recherche militaire américaine), un projet de surveillance électronique intitulé « Total Information Awareness ». Ce dessin imbécile, qu'on aurait dit fait exprès pour alimenter des délires conspirationnistes, était rehaussé d'une maxime latine qui, en un sens, sauvait l'ensemble : « *Scientia est potentia* », le savoir, c'est du pouvoir. Il ne s'agissait, effectivement, que de cela.

5

En août 2002, le directeur du programme, John Poindexter, le présenta en grande pompe à la conférence DARPATech, qui se tenait à Anaheim en Californie. La question qui nous occupe, commença-t-il, est « *dans une certaine mesure analogue au problème de la guerre sous-marine consistant à trouver des sous-marins dans un océan de bruit : il nous faut trouver des terroristes dans un monde de bruit ».* L'analogie océanique n'était pas là par hasard. L'amiral avait commencé sa carrière dans la Navy à la fin des années 1950 au sein d'une unité en charge de la traque des sous-marins soviétiques. Il ajouta, parlant des « terroristes » : « *Ils laissent nécessairement des signatures dans l'espace informationnel. »*

Le parallèle était clair : ce que l'on avait fait avec l'océan, on allait le faire avec l'« océan de l'information ». En lieu et place des anciens lofargrammes, des ordinateurs passeraient au crible une immense masse de données hétérogènes – télécommunications, relevés bancaires, registres administratifs, etc. – à la recherche de « signatures de comportement terroriste ». Une « red team » serait chargée de répertorier les scénarios d'attentats et d'en préciser les préparatifs nécessaires. Comme le dit Pointdexter dans un rapport au Congrès de mars

Van Riper, qui commandait les « rouges », adopta une stratégie de guerre asymétrique : afin de neutraliser l'appareil de renseignement sophistiqué des « bleus », qui représentaient les États-Unis, il eut recours à des moyens de communication rudimentaires, qui échappaient aux capacités d'interception adverses : plutôt que d'utiliser des téléphones portables ou des transmissions radio, il employa des courriers à moto pour acheminer les ordres ; il fit passer des messages codés dans les appels à la prière, ensuite relayés sur tout le territoire du haut des minarets. Les bleus, devenus sourds, furent incapables de détecter les offensives rouges. Aux premiers jours, une partie de la flotte américaine sombra. Face à une telle débâcle, le Haut-commandement décida de suspendre l'exercice et ordonna à Van Riper d'utiliser des canaux de communication interceptables par le renseignement électromagnétique. Il refusa et quitta la partie.

La stratégie états-unienne, dans le style hyper-technologique qui la caractérise, fait le pari de la « suprématie informationnelle ». Mais un régime qui mise de façon prépondérante sur des systèmes de télédétection électronique, et dont, en définitive, « *les services de sécurité en viennent à considérer comme plus crédible un profil*

En août 2002, le directeur du programme, John Poindexter, le présenta en grande pompe à la conférence DARPATech, qui se tenait à Anaheim en Californie. La question qui nous occupe, commença-t-il, est « *dans une certaine mesure analogue au problème de la guerre sous-marine consistant à trouver des sous-marins dans un océan de bruit : il nous faut trouver des terroristes dans un monde de bruit ».* L'analogie océanique n'était pas là par hasard. L'amiral avait commencé sa carrière dans la Navy à la fin des années 1950 au sein d'une unité en charge de la traque des sous-marins soviétiques. Il ajouta, parlant des « terroristes » : « *Ils laissent nécessairement des signatures dans l'espace informationnel. »*

Le parallèle était clair : ce que l'on avait fait avec l'océan, on allait le faire avec l'« océan de l'information ». En lieu et place des anciens lofargrammes, des ordinateurs passeraient au crible une immense masse de données hétérogènes – télécommunications, relevés bancaires, registres administratifs, etc. – à la recherche de « signatures de comportement terroriste ». Une « red team » serait chargée de répertorier les scénarios d'attentats et d'en préciser les préparatifs nécessaires. Comme le dit Pointdexter dans un rapport au Congrès de mars

6

Van Riper, qui commandait les « rouges », adopta une stratégie de guerre asymétrique : afin de neutraliser l'appareil de renseignement sophistiqué des « bleus », qui représentaient les États-Unis, il eut recours à des moyens de communication rudimentaires, qui échappaient aux capacités d'interception adverses : plutôt que d'utiliser des téléphones portables ou des transmissions radio, il employa des courriers à moto pour acheminer les ordres ; il fit passer des messages codés dans les appels à la prière, ensuite relayés sur tout le territoire du haut des minarets. Les bleus, devenus sourds, furent incapables de détecter les offensives rouges. Aux premiers jours, une partie de la flotte américaine sombra. Face à une telle débâcle, le Haut-commandement décida de suspendre l'exercice et ordonna à Van Riper d'utiliser des canaux de communication interceptables par le renseignement électromagnétique. Il refusa et quitta la partie.

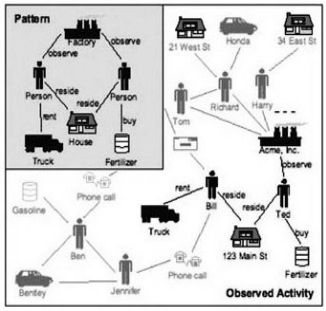
La stratégie états-unienne, dans le style hyper-technologique qui la caractérise, fait le pari de la « suprématie informationnelle ». Mais un régime qui mise de façon prépondérante sur des systèmes de télédétection électronique, et dont, en définitive, « *les services de sécurité en viennent à considérer comme plus crédible un profil*

39

les développements de l'« informatique ubiquitaire » et de l'« Internet des objets ». David Gauthier, l'un des théoriciens du « renseignement fondé sur l'activité » à la NGA, souligne les potentialités qu'ouvre la « *révolution dataculturelle* » en cours : « *prendre tous les aspects de la vie et les convertir en données* [76] ». La notion centrale est celle d'« autodocumentation » : à la limite, pourquoi développer des techniques de surveillance directe alors que les personnes s'équipent elles-mêmes d'une myriade de mouchards électroniques qui capturent en continu leurs moindres faits et gestes ? On n'aurait plus qu'à coller son oreille sur la coquille électronique et à écouter le son de l'océan des données. C'est aussi ce que dit, mais à sa manière, avec un cynisme consommé, l'un des Powerpoint de la NSA divulgués par Snowden. Première diapositive : « *Qui aurait cru, en 1984, que Big Brother ressemblerait à cela…* » – image de Steve Jobs un iPhone à la main. Deuxième vignette : «*… et que les zombies seraient des clients prêts à payer pour cela* » [77] – images de clients d'Apple posant, l'air ravi, avec leur appareil flambant neuf à la sortie d'un iStore.

En 2002, l'armée américaine lança un grand exercice, un wargame combinant forces réelles et simulation informatique [78]. Le lieutenant général

2003, « *ces transactions formeraient un schéma [« pattern »] que l'on pourrait repérer dans des bases de données* ».



Repérage d'un « schéma terroriste » dans un graphe d'activité [4]

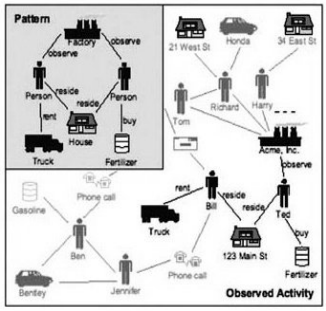
Exemple : si Bill et Ted habitent à la même adresse, louent un camion, se rendent sur un lieu sensible et achètent de l'engrais à base de nitrate d'ammonium (dont on sait qu'il peut servir à faire pousser des patates mais aussi à confectionner une bombe artisanale), alors ils se mettent à présenter un motif comportemental isomorphe à celui d'une signature terroriste, poussant l'algorithme chargé de traiter ces données à sonner l'alerte. L'un des soucis, cependant, comme le fit remarquer un expert dubitatif lors d'une audition parlementaire, c'est qu'un profil ainsi défini aboutirait *illico* à placer

les développements de l'« informatique ubiquitaire » et de l'« Internet des objets ». David Gauthier, l'un des théoriciens du « renseignement fondé sur l'activité » à la NGA, souligne les potentialités qu'ouvre la « *révolution dataculturelle* » en cours : « *prendre tous les aspects de la vie et les convertir en données* [76] ». La notion centrale est celle d'« autodocumentation » : à la limite, pourquoi développer des techniques de surveillance directe alors que les personnes s'équipent elles-mêmes d'une myriade de mouchards électroniques qui capturent en continu leurs moindres faits et gestes ? On n'aurait plus qu'à coller son oreille sur la coquille électronique et à écouter le son de l'océan des données. C'est aussi ce que dit, mais à sa manière, avec un cynisme consommé, l'un des Powerpoint de la NSA divulgués par Snowden. Première diapositive : « *Qui aurait cru, en 1984, que Big Brother ressemblerait à cela…* » – image de Steve Jobs un iPhone à la main. Deuxième vignette : «*… et que les zombies seraient des clients prêts à payer pour cela* » [77] – images de clients d'Apple posant, l'air ravi, avec leur appareil flambant neuf à la sortie d'un iStore.

En 2002, l'armée américaine lança un grand exercice, un wargame combinant forces réelles et simulation informatique [78]. Le lieutenant général

38

2003, « *ces transactions formeraient un schéma [« pattern »] que l'on pourrait repérer dans des bases de données* ».



Repérage d'un « schéma terroriste » dans un graphe d'activité [4]

Exemple : si Bill et Ted habitent à la même adresse, louent un camion, se rendent sur un lieu sensible et achètent de l'engrais à base de nitrate d'ammonium (dont on sait qu'il peut servir à faire pousser des patates mais aussi à confectionner une bombe artisanale), alors ils se mettent à présenter un motif comportemental isomorphe à celui d'une signature terroriste, poussant l'algorithme chargé de traiter ces données à sonner l'alerte. L'un des soucis, cependant, comme le fit remarquer un expert dubitatif lors d'une audition parlementaire, c'est qu'un profil ainsi défini aboutirait *illico* à placer

7

sur une liste des suspects non seulement de possibles émules de Timothy McVeigh (militant d'extrême droite qui fit exploser un camion piégé à Oklahoma City le 19 avril 1995), mais aussi la plupart des agriculteurs du Nebraska qui, eux aussi, assez souvent, habitent une même ferme, achètent de l'engrais et louent des camions [5].

Même à supposer que le « terrorisme » présente des signatures repérables par *datamining* – ce qui est une hypothèse pour le moins hasardeuse –, pareil système allait nécessairement engendrer pléthore de suspects, dont une écrasante majorité de fausses pistes – et ceci, estimait-on, par dizaines de millions : selon Bruce Schneier, qui a fait le calcul suivant pour le magazine *Wired* en octobre 2006, *« si le système a un taux de faux positifs de 1 sur 100 [...] [s'il y a] mille milliards d'indicateurs potentiels à passer au crible – un nombre qui correspond à dix événements (emails, achats, navigation web...) par Américain et par jour. [S'il y en a] dix parmi eux qui correspondent effectivement à des préparatifs terroristes. [Alors] un tel système, alors même qu'il serait, avec les paramètres que nous admettons ici, d'une précision parfaitement irréaliste, n'en générerait pas moins un milliard de fausses alarmes pour chaque complot terroriste effectivement découvert. Chaque jour de chaque année, la police*

capacité opérationnelle aboutie que d'une série de problèmes irrésolus [73]. Cela n'empêche pourtant pas cette vaste usine à gaz, dont les contrats pèsent plusieurs millions de dollars [74], de faire des plans sur l'avenir. Les capacités de collecte excédant largement les capacités d'analyse, le salut viendra de l'automatisation de cette dernière : « *Le problème, c'est le big data, et la solution révolutionnaire,* claironne-t-on sur le site de BAE Systems, *c'est le renseignement fondé sur l'activité.* » On voudrait par exemple des logiciels de reconnaissance vidéo capables d'interpréter la danse des pixels comme un observateur humain sait le faire, c'est-à-dire de façon sémantique et contextuelle. Idéalement, on voudrait que les données se mettent à se décrire elles-mêmes. Mais, entre le désir et sa réalisation, des obstacles se présentent. Et parmi eux des défis d'ordre ontologique : automatiser la reconnaissance des activités supposerait en effet au préalable d'être parvenu à construire une taxonomie et une syntaxe de l'action à même de *« modéliser les milliers d'objets qui constituent un système de comportement dans le temps* » – rien de moins que de bâtir un « *modèle analytique du monde* » [75].

Les apôtres du renseignement 2.0 lorgnent en attendant avec une convoitise non dissimulée sur

sur une liste des suspects non seulement de possibles émules de Timothy McVeigh (militant d'extrême droite qui fit exploser un camion piégé à Oklahoma City le 19 avril 1995), mais aussi la plupart des agriculteurs du Nebraska qui, eux aussi, assez souvent, habitent une même ferme, achètent de l'engrais et louent des camions [5].

Même à supposer que le « terrorisme » présente des signatures repérables par *datamining* – ce qui est une hypothèse pour le moins hasardeuse –, pareil système allait nécessairement engendrer pléthore de suspects, dont une écrasante majorité de fausses pistes – et ceci, estimait-on, par dizaines de millions : selon Bruce Schneier, qui a fait le calcul suivant pour le magazine *Wired* en octobre 2006, *« si le système a un taux de faux positifs de 1 sur 100 [...] [s'il y a] mille milliards d'indicateurs potentiels à passer au crible – un nombre qui correspond à dix événements (emails, achats, navigation web...) par Américain et par jour. [S'il y en a] dix parmi eux qui correspondent effectivement à des préparatifs terroristes. [Alors] un tel système, alors même qu'il serait, avec les paramètres que nous admettons ici, d'une précision parfaitement irréaliste, n'en générerait pas moins un milliard de fausses alarmes pour chaque complot terroriste effectivement découvert. Chaque jour de chaque année, la police*

8

capacité opérationnelle aboutie que d'une série de problèmes irrésolus [73]. Cela n'empêche pourtant pas cette vaste usine à gaz, dont les contrats pèsent plusieurs millions de dollars [74], de faire des plans sur l'avenir. Les capacités de collecte excédant largement les capacités d'analyse, le salut viendra de l'automatisation de cette dernière : « *Le problème, c'est le big data, et la solution révolutionnaire,* claironne-t-on sur le site de BAE Systems, *c'est le renseignement fondé sur l'activité.* » On voudrait par exemple des logiciels de reconnaissance vidéo capables d'interpréter la danse des pixels comme un observateur humain sait le faire, c'est-à-dire de façon sémantique et contextuelle. Idéalement, on voudrait que les données se mettent à se décrire elles-mêmes. Mais, entre le désir et sa réalisation, des obstacles se présentent. Et parmi eux des défis d'ordre ontologique : automatiser la reconnaissance des activités supposerait en effet au préalable d'être parvenu à construire une taxonomie et une syntaxe de l'action à même de *« modéliser les milliers d'objets qui constituent un système de comportement dans le temps* » – rien de moins que de bâtir un « *modèle analytique du monde* » [75].

Les apôtres du renseignement 2.0 lorgnent en attendant avec une convoitise non dissimulée sur

37

dire aberrant par rapport à un type statistiquement défini [71] ». Alors qu'un écart singulier peut être interprété de diverses manières, par exemple « *comme un échec ou comme un essai, comme une faute ou comme une aventure* [72] », ce genre de dispositif paranoïaque va se mettre à le signaler comme une menace potentielle : « ALERTE ».

De façon assez ironique, c'est au sein même de sociétés dont l'idéologie dominante avait érigé en valeur sacrée la liberté individuelle de suivre sa propre « *way of life* » que la singularité d'un tel cheminement va finir par se signaler automatiquement comme suspecte. Mais il faut souligner que ceci ne repose plus, en l'occurrence, sur une logique *disciplinaire.* En utilisant des schémas chronospatiaux pour filtrer des comportements, ces dispositifs-là n'ont par eux-mêmes aucun modèle de conduite déterminé à imposer aux diverses vies qu'ils scrutent. Leur normativité sans norme est animée par une autre visée, par un autre genre d'appétit dévorant : repérer des écarts afin d'« *acquérir des cibles* », et ceci dans un mode de pensée où, les cibles étant inconnues, c'est l'inconnu qui devient cible.

Le « renseignement fondé sur l'activité » est cependant moins aujourd'hui le nom d'une

aurait à mener l'enquête sur 27 millions de complots potentiels afin de découvrir l'unique complot terroriste réel par mois ». Tout cela sans compter qu'il y a bien peu de chances pour que les attentats de demain présentent les mêmes modes opératoires que ceux d'hier.

L'autre problème de fond tenait à la notion même de « terrorisme », trop floue pour que l'on puisse en donner une description opérationnelle suffisante. Qu'est-ce que le terrorisme ? Admettons la définition officielle suivante émanant du département de la Défense américain : « *tout usage illégal et calculé de la violence ou de la menace visant à produire un sentiment de terreur à des fins politiques ».* Cette notion ne se définit pas par certains modes opératoires, mais par une intention visant à produire un effet subjectif, une émotion, la peur. Quel sera l'algorithme capable de repérer les indices comportementaux trahissant une telle intentionnalité ? Il y a mille et une manières de vouloir terroriser. Sans compter qu'avec une telle définition, il y a aussi un risque à ne pas écarter : un jour que Poindexter – qui comptait au nombre de ses faits d'arme d'avoir officié comme barbouze de l'administration Reagan, mouillé jusqu'au cou dans l'affaire des ventes d'armes à l'Iran au profit des escadrons de la mort des « Contras »

dire aberrant par rapport à un type statistiquement défini [71] ». Alors qu'un écart singulier peut être interprété de diverses manières, par exemple « *comme un échec ou comme un essai, comme une faute ou comme une aventure* [72] », ce genre de dispositif paranoïaque va se mettre à le signaler comme une menace potentielle : « ALERTE ».

De façon assez ironique, c'est au sein même de sociétés dont l'idéologie dominante avait érigé en valeur sacrée la liberté individuelle de suivre sa propre « *way of life* » que la singularité d'un tel cheminement va finir par se signaler automatiquement comme suspecte. Mais il faut souligner que ceci ne repose plus, en l'occurrence, sur une logique *disciplinaire.* En utilisant des schémas chronospatiaux pour filtrer des comportements, ces dispositifs-là n'ont par eux-mêmes aucun modèle de conduite déterminé à imposer aux diverses vies qu'ils scrutent. Leur normativité sans norme est animée par une autre visée, par un autre genre d'appétit dévorant : repérer des écarts afin d'« *acquérir des cibles* », et ceci dans un mode de pensée où, les cibles étant inconnues, c'est l'inconnu qui devient cible.

Le « renseignement fondé sur l'activité » est cependant moins aujourd'hui le nom d'une

36

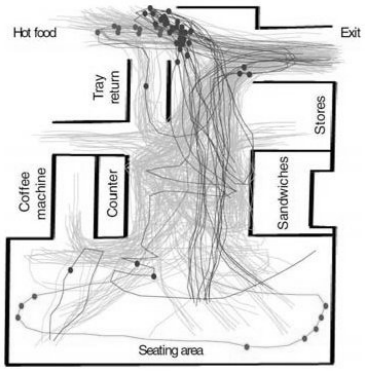
aurait à mener l'enquête sur 27 millions de complots potentiels afin de découvrir l'unique complot terroriste réel par mois ». Tout cela sans compter qu'il y a bien peu de chances pour que les attentats de demain présentent les mêmes modes opératoires que ceux d'hier.

L'autre problème de fond tenait à la notion même de « terrorisme », trop floue pour que l'on puisse en donner une description opérationnelle suffisante. Qu'est-ce que le terrorisme ? Admettons la définition officielle suivante émanant du département de la Défense américain : « *tout usage illégal et calculé de la violence ou de la menace visant à produire un sentiment de terreur à des fins politiques ».* Cette notion ne se définit pas par certains modes opératoires, mais par une intention visant à produire un effet subjectif, une émotion, la peur. Quel sera l'algorithme capable de repérer les indices comportementaux trahissant une telle intentionnalité ? Il y a mille et une manières de vouloir terroriser. Sans compter qu'avec une telle définition, il y a aussi un risque à ne pas écarter : un jour que Poindexter – qui comptait au nombre de ses faits d'arme d'avoir officié comme barbouze de l'administration Reagan, mouillé jusqu'au cou dans l'affaire des ventes d'armes à l'Iran au profit des escadrons de la mort des « Contras »

9

nicaraguayens – donnait une conférence dans une université américaine, un jeune homme du public se leva et lui demanda : *« Amiral Poindexter, si votre système est si performant que cela pour détecter des terroristes, combien de temps cela va-t-il lui prendre pour vous trouver vous-même*[6] ? »

Par fausse analogie, des cerveaux formés durant la guerre froide plaquaient ainsi du mécanique (le signal d'un moteur de sous-marin, nécessaire et constant) sur du vivant (une intentionnalité politique, polymorphe et adaptative). Tout le projet reposait sur le postulat qu'il existait des « *signatures terroristes* ». Or cette prémisse ne tenait pas. La conclusion était inévitable : « *La seule chose prévisible au sujet du* datamining *antiterroriste est son échec permanent*[7]. » Aux critiques qui pointaient les limites épistémologiques d'un tel programme, ses concepteurs répondaient par des procédés destinés à en mitiger les effets d'engorgement. Confrontés à un problème d'explosion du nombre de « *faux positifs* », lui-même lié au faible taux de prévalence du phénomène recherché dans la masse considérée, ils empruntaient leurs solutions au *screening* médical : découper, au sein de la population générale, des sous-populations à risque.



Modélisation des trajets normaux et détection des conduites anormales dans une cantine [70]

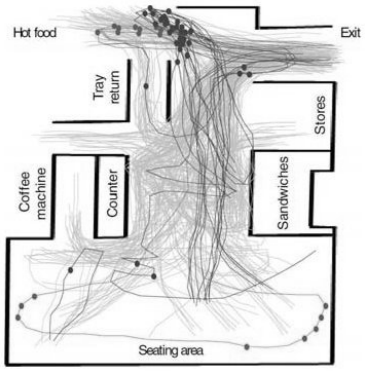
La définition du « normal » dont ces systèmes disposent est purement empirique : elle est *apprise* par la machine sur la base de relevés de fréquences et de répétitions. Et c'est un écart avec de tels motifs de régularité – une anomalie plutôt qu'une anormalité – qui déclenchera des « *alertes de comportement anormal* » s'affichant en teinte rouge-orangé sur l'écran de l'analyste.

Mais l'un des problèmes classiques, avec ce genre de conception de la normalité, c'est que l'« *on devra nécessairement,* comme l'expliquait en son temps Georges Canguilhem, *tenir pour anormal – c'est-à-dire, croit-on, pathologique – tout individu anomal (porteur d'anomalies), c'est-à-*

nicaraguayens – donnait une conférence dans une université américaine, un jeune homme du public se leva et lui demanda : *« Amiral Poindexter, si votre système est si performant que cela pour détecter des terroristes, combien de temps cela va-t-il lui prendre pour vous trouver vous-même*[6] ? »

Par fausse analogie, des cerveaux formés durant la guerre froide plaquaient ainsi du mécanique (le signal d'un moteur de sous-marin, nécessaire et constant) sur du vivant (une intentionnalité politique, polymorphe et adaptative). Tout le projet reposait sur le postulat qu'il existait des « *signatures terroristes* ». Or cette prémisse ne tenait pas. La conclusion était inévitable : « *La seule chose prévisible au sujet du* datamining *antiterroriste est son échec permanent*[7]. » Aux critiques qui pointaient les limites épistémologiques d'un tel programme, ses concepteurs répondaient par des procédés destinés à en mitiger les effets d'engorgement. Confrontés à un problème d'explosion du nombre de « *faux positifs* », lui-même lié au faible taux de prévalence du phénomène recherché dans la masse considérée, ils empruntaient leurs solutions au *screening* médical : découper, au sein de la population générale, des sous-populations à risque.

10



Modélisation des trajets normaux et détection des conduites anormales dans une cantine [70]

La définition du « normal » dont ces systèmes disposent est purement empirique : elle est *apprise* par la machine sur la base de relevés de fréquences et de répétitions. Et c'est un écart avec de tels motifs de régularité – une anomalie plutôt qu'une anormalité – qui déclenchera des « *alertes de comportement anormal* » s'affichant en teinte rouge-orangé sur l'écran de l'analyste.

Mais l'un des problèmes classiques, avec ce genre de conception de la normalité, c'est que l'« *on devra nécessairement,* comme l'expliquait en son temps Georges Canguilhem, *tenir pour anormal – c'est-à-dire, croit-on, pathologique – tout individu anomal (porteur d'anomalies), c'est-à-*

35

La stratégie qui oriente les recherches entreprises en ce domaine consiste à modéliser des *« formes de vie permettant d'identifier les activités normales et les activités anormales* [67] ». En « *accumulant des tracés dans le temps »,* on peut *« modéliser les motifs de déplacements de piétons et détecter des anomalies par rapport à des tendances comportementales apprises par la machine »* [68]. Une fois que l'on a par exemple identifié les itinéraires « normaux » d'un porteur de plateau-repas dans une cantine, on peut voir émerger par contraste un certain nombre de trajectoires aberrantes. Au-delà des tests en espace confiné, l'objectif est ensuite de déployer ces méthodologies de tri comportemental au sein de programmes de « *détection des anomalies à grande échelle* [69] ».

Comme l'expliquaient les partisans de ces méthodes, il allait en fait s'agir de *« détecter des liens relationnels rares mais significatifs [...] au sein de populations ajustées selon le risque* [8] ». L'idée était de combiner les approches du « *datamining* propositionnel » (fondé sur des requêtes du type : « trouver toutes les entités présentant les propriétés x et y ») et du « *datamining* relationnel » (fondé sur des recherches du type : « trouver toutes les entités liées à une entité A »). On allait ainsi cibler des groupes d'individus en fonction de leurs relations, un peu comme dans un dépistage médical, où l'on commence par repérer les antécédents familiaux dans l'espoir de débusquer une maladie rare. On affinerait ensuite la masse par filtres successifs. Enfin, plutôt que de répartir les résultats de l'analyse suivant des classificateurs binaires en « suspects » ou « non-suspects », on leur attribuerait des scores de suspicion. Bref, il y aurait toujours des fausses pistes, mais, en spécifiant ainsi les degrés d'alerte, on espérait prioriser le travail d'investigation.

L'une des implications de cette « solution » apparaissait peu dans les débats, alors même qu'elle était politiquement centrale : dans le contexte ambiant, lesdites « populations à risque » risquaient fort d'être définies selon une

La stratégie qui oriente les recherches entreprises en ce domaine consiste à modéliser des *« formes de vie permettant d'identifier les activités normales et les activités anormales* [67] ». En « *accumulant des tracés dans le temps »,* on peut *« modéliser les motifs de déplacements de piétons et détecter des anomalies par rapport à des tendances comportementales apprises par la machine »* [68]. Une fois que l'on a par exemple identifié les itinéraires « normaux » d'un porteur de plateau-repas dans une cantine, on peut voir émerger par contraste un certain nombre de trajectoires aberrantes. Au-delà des tests en espace confiné, l'objectif est ensuite de déployer ces méthodologies de tri comportemental au sein de programmes de « *détection des anomalies à grande échelle* [69] ».

34

Comme l'expliquaient les partisans de ces méthodes, il allait en fait s'agir de *« détecter des liens relationnels rares mais significatifs [...] au sein de populations ajustées selon le risque* [8] ». L'idée était de combiner les approches du « *datamining* propositionnel » (fondé sur des requêtes du type : « trouver toutes les entités présentant les propriétés x et y ») et du « *datamining* relationnel » (fondé sur des recherches du type : « trouver toutes les entités liées à une entité A »). On allait ainsi cibler des groupes d'individus en fonction de leurs relations, un peu comme dans un dépistage médical, où l'on commence par repérer les antécédents familiaux dans l'espoir de débusquer une maladie rare. On affinerait ensuite la masse par filtres successifs. Enfin, plutôt que de répartir les résultats de l'analyse suivant des classificateurs binaires en « suspects » ou « non-suspects », on leur attribuerait des scores de suspicion. Bref, il y aurait toujours des fausses pistes, mais, en spécifiant ainsi les degrés d'alerte, on espérait prioriser le travail d'investigation.

L'une des implications de cette « solution » apparaissait peu dans les débats, alors même qu'elle était politiquement centrale : dans le contexte ambiant, lesdites « populations à risque » risquaient fort d'être définies selon une

34

11

logique de profilage racial à peine déguisée. Viser par exemple préférentiellement les individus ayant des relations régulières avec des personnes situées au Proche et au Moyen-Orient équivalait à constituer la population arabe américaine en groupe cible. Sous la « *colour blindness* » apparente de l'analyse informatisée, une vieille vision raciste ne tarde pas à refaire surface. Dans certains documents de la NSA, la cible-type a un sobriquet révélateur : « Mohammed Raghead [9] » – terme d'argot qui signifie littéralement « enturbanné », mais dont l'équivalent français serait plutôt : « Mohammed le Bougnoule ».

De l'aveu même de ses concepteurs, ce modèle de « datamining *relationnel* » comportait en outre une série de « *failles manifestes* » au plan tactique : *« Certains types de données relationnelles ne sont clairement pas résistants aux contre-conduites. Par exemple, un individu terroriste pourrait s'abstenir d'émettre ou de recevoir des messages électroniques, des appels téléphoniques ou des transactions financières avec d'autres terroristes. Une autre possibilité est qu'un individu s'efforce consciemment de réduire son degré d'homophilie sociale, de sorte à produire du "bruit" dans les relevés électroniques afin d'escamoter l'existence d'un groupe déterminé. Ils pourraient également utiliser de*

Et c'est cette tâche-là – établir la distinction entre ami et ennemi – que l'on espère derechef pouvoir confier à des algorithmes. Contrairement cependant aux espoirs initiaux du *datamining* prédictif à la Poindexter, on part désormais du principe que les nouvelles cibles sont généralement dépourvues de signature claire permettant leur détection directe.

Dans les discours de la méthode que rédigent les spécialistes du renseignement, le problème revêt des formulations quasi métaphysiques : comment découvrir des « *inconnus inconnus* [66] » ? Un inconnu connu est un individu dont on ignore l'identité singulière, l'état civil, mais dont les attributs repérables correspondent à un type répertorié. Un inconnu inconnu est celui qui échappe à la fois à une identification singulière et à une identification générique : on ne sait ni *qui* il est (on ignore son nom, voire son visage) ni *ce* qu'il est (son profil d'activité ne correspond pas à ceux déjà catalogués). La solution vers laquelle on se tourne alors est en un sens précomprise dans l'énoncé du problème : pour pouvoir repérer des formes inconnues, il faut disposer d'un répertoire de formes connues. Cerner le typique pour repérer l'atypique.

logique de profilage racial à peine déguisée. Viser par exemple préférentiellement les individus ayant des relations régulières avec des personnes situées au Proche et au Moyen-Orient équivalait à constituer la population arabe américaine en groupe cible. Sous la « *colour blindness* » apparente de l'analyse informatisée, une vieille vision raciste ne tarde pas à refaire surface. Dans certains documents de la NSA, la cible-type a un sobriquet révélateur : « Mohammed Raghead [9] » – terme d'argot qui signifie littéralement « enturbanné », mais dont l'équivalent français serait plutôt : « Mohammed le Bougnoule ».

De l'aveu même de ses concepteurs, ce modèle de « datamining *relationnel* » comportait en outre une série de « *failles manifestes* » au plan tactique : *« Certains types de données relationnelles ne sont clairement pas résistants aux contre-conduites. Par exemple, un individu terroriste pourrait s'abstenir d'émettre ou de recevoir des messages électroniques, des appels téléphoniques ou des transactions financières avec d'autres terroristes. Une autre possibilité est qu'un individu s'efforce consciemment de réduire son degré d'homophilie sociale, de sorte à produire du "bruit" dans les relevés électroniques afin d'escamoter l'existence d'un groupe déterminé. Ils pourraient également utiliser de*

Et c'est cette tâche-là – établir la distinction entre ami et ennemi – que l'on espère derechef pouvoir confier à des algorithmes. Contrairement cependant aux espoirs initiaux du *datamining* prédictif à la Poindexter, on part désormais du principe que les nouvelles cibles sont généralement dépourvues de signature claire permettant leur détection directe.

Dans les discours de la méthode que rédigent les spécialistes du renseignement, le problème revêt des formulations quasi métaphysiques : comment découvrir des « *inconnus inconnus* [66] » ? Un inconnu connu est un individu dont on ignore l'identité singulière, l'état civil, mais dont les attributs repérables correspondent à un type répertorié. Un inconnu inconnu est celui qui échappe à la fois à une identification singulière et à une identification générique : on ne sait ni *qui* il est (on ignore son nom, voire son visage) ni *ce* qu'il est (son profil d'activité ne correspond pas à ceux déjà catalogués). La solution vers laquelle on se tourne alors est en un sens précomprise dans l'énoncé du problème : pour pouvoir repérer des formes inconnues, il faut disposer d'un répertoire de formes connues. Cerner le typique pour repérer l'atypique.

peut-être pas. À vrai dire, il peut s'agir de n'importe quoi, quelque chose de potentiellement important, mais dont on ne sait même pas pour commencer si ça existe. [...] Cela peut prendre l'aspect d'un banc de poissons organisés ou bien d'éléments sans aucun lien. Mais ce que nous savons, c'est que nous devons le trouver, l'identifier, et – qu'il s'agisse d'un poisson ou d'un oiseau de mer – comprendre ce qui le rattache à d'autres objets importants à nos yeux [62]. » Ce que Laetitia Long tentait ainsi d'exposer à grand renfort de métaphores marines (mais il faut dire que, bien avant de devenir directrice de la NGA, elle aussi avait fait ses armes dans la détection acoustique des sous-marins) est une nouvelle philosophie, un nouveau paradigme édicté depuis 2010 par les plus hautes autorités du renseignement états-unien.

C'est la doctrine du « *renseignement fondé sur l'activité* [63] » : « *Nous avions l'habitude de savoir ce que nous cherchions et nous cherchions des choses ; à présent, nous ne savons pas ce que nous cherchons, et nous ne cherchons pas des choses, mais plutôt des activités* [64]. » Le postulat est le même que précédemment : « *Dans des environnements où il n'existe aucune différence visuelle entre ami et ennemi, c'est par leurs actions que les ennemis se rendent visibles* [65]. »

fausses identités afin de réduire le nombre apparent de relations associées à une identité donnée. Ce problème constitue un obstacle d'importance pour à peu près tout système de surveillance informationnelle, et ce, quelle que soit sa conception[10]. » Or, si de tels systèmes peuvent être mis en échec par des précautions de cet ordre, à la portée de tout groupuscule averti, ceux-ci ne seront, contrairement à l'objectif affiché, paradoxalement mobilisables que contre des individus ou des groupes dont les activités, pour être en partie privées ou discrètes, n'en sont pas pour autant activement clandestines.

Le projet de Poindexter fut un échec politique. Trop maladroit, trop candide dans sa dystopie. En novembre 2002, une tribune incendiaire du chroniqueur William Safire, « You are a suspect », attira l'attention du public sur le programme. On vit le logo. On s'inquiéta. La pression monta, tant et si bien que, le 13 février 2003, le Congrès coupa les crédits. Ce n'était pourtant qu'un rideau de fumée. Le programme continua sa vie ailleurs, sous le sceau du secret [11]. Il faut dire que d'autres personnages, à la même période, caressaient déjà des ambitions similaires.

peut-être pas. À vrai dire, il peut s'agir de n'importe quoi, quelque chose de potentiellement important, mais dont on ne sait même pas pour commencer si ça existe. [...] Cela peut prendre l'aspect d'un banc de poissons organisés ou bien d'éléments sans aucun lien. Mais ce que nous savons, c'est que nous devons le trouver, l'identifier, et – qu'il s'agisse d'un poisson ou d'un oiseau de mer – comprendre ce qui le rattache à d'autres objets importants à nos yeux [62]. » Ce que Laetitia Long tentait ainsi d'exposer à grand renfort de métaphores marines (mais il faut dire que, bien avant de devenir directrice de la NGA, elle aussi avait fait ses armes dans la détection acoustique des sous-marins) est une nouvelle philosophie, un nouveau paradigme édicté depuis 2010 par les plus hautes autorités du renseignement états-unien.

C'est la doctrine du « *renseignement fondé sur l'activité* [63] » : « *Nous avions l'habitude de savoir ce que nous cherchions et nous cherchions des choses ; à présent, nous ne savons pas ce que nous cherchons, et nous ne cherchons pas des choses, mais plutôt des activités* [64]. » Le postulat est le même que précédemment : « *Dans des environnements où il n'existe aucune différence visuelle entre ami et ennemi, c'est par leurs actions que les ennemis se rendent visibles* [65]. »

32

fausses identités afin de réduire le nombre apparent de relations associées à une identité donnée. Ce problème constitue un obstacle d'importance pour à peu près tout système de surveillance informationnelle, et ce, quelle que soit sa conception[10]. » Or, si de tels systèmes peuvent être mis en échec par des précautions de cet ordre, à la portée de tout groupuscule averti, ceux-ci ne seront, contrairement à l'objectif affiché, paradoxalement mobilisables que contre des individus ou des groupes dont les activités, pour être en partie privées ou discrètes, n'en sont pas pour autant activement clandestines.

Le projet de Poindexter fut un échec politique. Trop maladroit, trop candide dans sa dystopie. En novembre 2002, une tribune incendiaire du chroniqueur William Safire, « You are a suspect », attira l'attention du public sur le programme. On vit le logo. On s'inquiéta. La pression monta, tant et si bien que, le 13 février 2003, le Congrès coupa les crédits. Ce n'était pourtant qu'un rideau de fumée. Le programme continua sa vie ailleurs, sous le sceau du secret [11]. Il faut dire que d'autres personnages, à la même période, caressaient déjà des ambitions similaires.

13

« *COLLECT IT ALL* »

Au plus fort de la polémique, Keith Alexander et James Heath, qui allaient deux ans plus tard devenir respectivement directeur et conseiller scientifique de la NSA, prirent ouvertement fait et cause pour le tournant du *big data* en matière de renseignement : « *Beaucoup estiment que le problème est que nous collectons trop d'information, et que la solution [...] serait de réduire ou de filtrer les données, [...] nous pensons le contraire [...] la solution est de continuer à collecter le plus d'information possible tout en révolutionnant nos façons de l'indexer, de la connecter, de l'analyser, de la stocker* [12]. »

Alexander, qui dirigeait à l'époque l'Information Dominance Center (IDC) de l'armée américaine, avait hébergé les recherches de Poindexter à Fort Belvoir, en Virginie [13]. Le décor de ce centre d'opérations aux allures futuristes avait été conçu pour « *imiter l'_Enterprise, _le vaisseau spatial de* Star Trek, *jusque dans ses moindres détails, avec des panneaux chromés, des postes informatiques, un immense écran de télévision au mur et des portes coulissantes qui faisaient "woosh" quand elles s'ouvraient. Des sénateurs, ainsi que d'autres visiteurs politiques de haut rang, rapporte-t-on, s'asseyaient à tour de rôle*

drones tuent « *sans connaître l'identité précise des individus ciblés »,* sur cette seule base que leurs activités, vues du ciel *« correspondent à une "signature" de comportement préidentifiée que les États-Unis associent à une activité militante* [60] ».

Outre les tueries, la désolation et la déstabilisation de régions entières, quel est le bilan de près de quinze ans de « guerre contre la terreur » ? Combien d'aspirants au djihad en 2001 et combien aujourd'hui ? L'un des seuls résultats tangibles de cette politique aura été de démultiplier la menace que l'on prétendait éradiquer, de la faire proliférer à une échelle, effectivement, industrielle.

Pour la NSA et la NGA cependant, ce nouveau modèle de surveillance géospatiale apparaissait comme une innovation géniale, à étendre et à généraliser. La question était à partir de là de savoir, comme le résumait Gregory Treverton, si « *nous pouvions le transposer au-delà de l'antiterrorisme et de la chasse à l'homme* [61] ».

À LA RECHERCHE DES « *INCONNUS INCONNUS* »

« Aujourd'hui, le renseignement, c'est comme chercher quelque chose dans un grand océan, quelque chose qui est peut-être un poisson, ou

« *COLLECT IT ALL* »

Au plus fort de la polémique, Keith Alexander et James Heath, qui allaient deux ans plus tard devenir respectivement directeur et conseiller scientifique de la NSA, prirent ouvertement fait et cause pour le tournant du *big data* en matière de renseignement : « *Beaucoup estiment que le problème est que nous collectons trop d'information, et que la solution [...] serait de réduire ou de filtrer les données, [...] nous pensons le contraire [...] la solution est de continuer à collecter le plus d'information possible tout en révolutionnant nos façons de l'indexer, de la connecter, de l'analyser, de la stocker* [12]. »

Alexander, qui dirigeait à l'époque l'Information Dominance Center (IDC) de l'armée américaine, avait hébergé les recherches de Poindexter à Fort Belvoir, en Virginie [13]. Le décor de ce centre d'opérations aux allures futuristes avait été conçu pour « *imiter l'_Enterprise, _le vaisseau spatial de* Star Trek, *jusque dans ses moindres détails, avec des panneaux chromés, des postes informatiques, un immense écran de télévision au mur et des portes coulissantes qui faisaient "woosh" quand elles s'ouvraient. Des sénateurs, ainsi que d'autres visiteurs politiques de haut rang, rapporte-t-on, s'asseyaient à tour de rôle*

14

drones tuent « *sans connaître l'identité précise des individus ciblés »,* sur cette seule base que leurs activités, vues du ciel *« correspondent à une "signature" de comportement préidentifiée que les États-Unis associent à une activité militante* [60] ».

Outre les tueries, la désolation et la déstabilisation de régions entières, quel est le bilan de près de quinze ans de « guerre contre la terreur » ? Combien d'aspirants au djihad en 2001 et combien aujourd'hui ? L'un des seuls résultats tangibles de cette politique aura été de démultiplier la menace que l'on prétendait éradiquer, de la faire proliférer à une échelle, effectivement, industrielle.

Pour la NSA et la NGA cependant, ce nouveau modèle de surveillance géospatiale apparaissait comme une innovation géniale, à étendre et à généraliser. La question était à partir de là de savoir, comme le résumait Gregory Treverton, si « *nous pouvions le transposer au-delà de l'antiterrorisme et de la chasse à l'homme* [61] ».

À LA RECHERCHE DES « *INCONNUS INCONNUS* »

« Aujourd'hui, le renseignement, c'est comme chercher quelque chose dans un grand océan, quelque chose qui est peut-être un poisson, ou

31

nuit », s'enorgueillit McChrystal [54]. Le directeur adjoint de la NSA, John Inglis, était dithyrambique : Geocell tenait « *presque du miracle* [55] ». John Nagl saluait, avec un enthousiasme similaire, la mise en œuvre d'une « *machine à tuer de dimension industrielle* [56] ».

Le journaliste Gareth Porter a une autre version des choses : « *Ce qu'impliquait la nouvelle méthodologie de renseignement développée par McChrystal et Flynn était que quiconque se rendait dans un lieu surveillé ou communiquait avec un téléphone portable associé à ce lieu pouvait être considéré comme faisant partie d'un réseau d'insurgés* [57]. » On mobilisait les instruments de suspicion réticulaire élaborés par la NSA pour servir de base à des décisions de vie et de mort, ceci en faisant mine d'oublier qu'il s'était toujours agi d'« *instruments d'investigation, mais pas d'outils de preuve* [58] ». Les autorités s'étaient bâti un théâtre d'ombres et des scènes sanglantes s'y enchaînaient à un rythme accéléré : « *Le résultat, beaucoup trop souvent, consistait en un tir aveugle fondé sur des indicateurs de "formes de vie" sans confirmation directe du fait que les cibles sont effectivement celles que nous pensons qu'elles sont* [59]. » C'est sur le même genre de méthodologie que se fondent les frappes dites de « signature », où les

dans le "siège du capitaine", un fauteuil plein cuir trônant au centre de la pièce, pour voir Alexander, grand amateur de science-fiction, leur faire la démonstration sur écran géant de ses logiciels de traitement de données [14] ».

Lorsque Alexander prit la direction de la NSA, en 2005, sa position n'avait pas varié d'un iota : « *Plutôt que de chercher une seule aiguille dans la botte de foin, son approche était la suivante : "collectons toute la botte de foin, [...] collectez tout, indexez et archivez"* [15]. » On a résumé cette philosophie par un slogan : « Tout collecter. » Il faut cependant ajouter qu'un tel principe se mord la queue : pour s'assurer de ne rien rater dans l'analyse, on veut amasser toujours plus de données, sauf que plus on en a, moins on est en capacité de les analyser. C'est la contradiction fondamentale entre capacités de collecte démultipliées et capacités d'analyse bornées. Une collecte massive n'implique cependant pas que tout soit analysé, lu, ou écouté. C'est la différence cruciale entre « surveillance passive » et « surveillance active ».

La collecte peut être effectuée soit en vrac, soit de manière ciblée. Une collecte en vrac amasse sans trier. C'est le cas du « Telephone Record Program », conduit sous l'égide de la section 215

nuit », s'enorgueillit McChrystal [54]. Le directeur adjoint de la NSA, John Inglis, était dithyrambique : Geocell tenait « *presque du miracle* [55] ». John Nagl saluait, avec un enthousiasme similaire, la mise en œuvre d'une « *machine à tuer de dimension industrielle* [56] ».

Le journaliste Gareth Porter a une autre version des choses : « *Ce qu'impliquait la nouvelle méthodologie de renseignement développée par McChrystal et Flynn était que quiconque se rendait dans un lieu surveillé ou communiquait avec un téléphone portable associé à ce lieu pouvait être considéré comme faisant partie d'un réseau d'insurgés* [57]. » On mobilisait les instruments de suspicion réticulaire élaborés par la NSA pour servir de base à des décisions de vie et de mort, ceci en faisant mine d'oublier qu'il s'était toujours agi d'« *instruments d'investigation, mais pas d'outils de preuve* [58] ». Les autorités s'étaient bâti un théâtre d'ombres et des scènes sanglantes s'y enchaînaient à un rythme accéléré : « *Le résultat, beaucoup trop souvent, consistait en un tir aveugle fondé sur des indicateurs de "formes de vie" sans confirmation directe du fait que les cibles sont effectivement celles que nous pensons qu'elles sont* [59]. » C'est sur le même genre de méthodologie que se fondent les frappes dites de « signature », où les

30

dans le "siège du capitaine", un fauteuil plein cuir trônant au centre de la pièce, pour voir Alexander, grand amateur de science-fiction, leur faire la démonstration sur écran géant de ses logiciels de traitement de données [14] ».

Lorsque Alexander prit la direction de la NSA, en 2005, sa position n'avait pas varié d'un iota : « *Plutôt que de chercher une seule aiguille dans la botte de foin, son approche était la suivante : "collectons toute la botte de foin, [...] collectez tout, indexez et archivez"* [15]. » On a résumé cette philosophie par un slogan : « Tout collecter. » Il faut cependant ajouter qu'un tel principe se mord la queue : pour s'assurer de ne rien rater dans l'analyse, on veut amasser toujours plus de données, sauf que plus on en a, moins on est en capacité de les analyser. C'est la contradiction fondamentale entre capacités de collecte démultipliées et capacités d'analyse bornées. Une collecte massive n'implique cependant pas que tout soit analysé, lu, ou écouté. C'est la différence cruciale entre « surveillance passive » et « surveillance active ».

La collecte peut être effectuée soit en vrac, soit de manière ciblée. Une collecte en vrac amasse sans trier. C'est le cas du « Telephone Record Program », conduit sous l'égide de la section 215

15

du *Patriot Act*, où la NSA « *collecte à peu près tous les relevés d'appels générés par certaines compagnies téléphoniques aux États-Unis* [16] ». Une collecte ciblée se concentre sur des « sélecteurs forts » (numéro de téléphone, adresse email, adresse IP, etc.), mais qu'elle soit « ciblée » ne l'empêche pas d'être très fournie : 89 138 identifiants auraient ainsi été visés par la NSA en 2013 sous la houlette de la section 702 du *Foreign Intelligence Surveillance Act*, dont relève entre autres le programme de collecte des données Internet PRISM [17]. Une « collecte ciblée » – tout comme, au demeurant, une « frappe ciblée » – peut aussi avoir ses « dommages collatéraux » : certains modes d'interception vont ainsi « accidentellement », « par inadvertance » – mais en réalité de façon tout à fait providentielle – aspirer tous les paquets de données transitant au voisinage des sélecteurs officiellement visés [18].

Parce que le débat américain se polarise à peu près exclusivement sur la question des écoutes domestiques et de la vie privée des citoyens des États-Unis, ces deux premiers programmes (métadonnées et PRISM) ont été largement médiatisés. Mais cette focalisation tend à déformer le tableau, car une grande partie du ratissage de données s'effectue, autant qu'on puisse le savoir, à l'ombre d'une autre subtilité

Traditionnellement, le renseignement intervenait surtout dans les phases préparatoires de reconnaissance. Il s'incorpore désormais en temps réel à la phase opérationnelle : « *Aujourd'hui, le renseignement est opération* [51]. » Ce déplacement est lié à une profonde réforme du « cycle de ciblage » impulsée en Irak par le Joint Special Operations Command (JSOC). L'idée, expose le général McChrystal, « *était de combiner les analystes qui trouvent l'ennemi, [...] les opérateurs de drones qui ferrent la cible, les unités combattantes qui la terminent [...], les spécialistes qui exploitent les renseignements obtenus dans le raid – dont les téléphones portables. [...] En faisant cela, nous avons réussi à accélérer le cycle* [52] ». Tandis qu'au début de la guerre, l'analyse des renseignements collectés lors d'une opération pouvait prendre des semaines, la mise en place de ce cycle agressif permit de faire tourner la « *kill chain* » à plein régime et de multiplier les raids nocturnes, chaque nouvelle opération permettant de trouver, par chaînage de contacts, de nouveaux suspects que l'on ciblait sur-le-champ et de remonter ainsi de proche en proche jusqu'à « *des gens dont on ignorait même l'existence au début de la nuit* [53] » : on passa ainsi de dix-huit raids par mois en aout 2004 à trois cents raids par mois en 2006 – « *dix chaque*

du *Patriot Act*, où la NSA « *collecte à peu près tous les relevés d'appels générés par certaines compagnies téléphoniques aux États-Unis* [16] ». Une collecte ciblée se concentre sur des « sélecteurs forts » (numéro de téléphone, adresse email, adresse IP, etc.), mais qu'elle soit « ciblée » ne l'empêche pas d'être très fournie : 89 138 identifiants auraient ainsi été visés par la NSA en 2013 sous la houlette de la section 702 du *Foreign Intelligence Surveillance Act*, dont relève entre autres le programme de collecte des données Internet PRISM [17]. Une « collecte ciblée » – tout comme, au demeurant, une « frappe ciblée » – peut aussi avoir ses « dommages collatéraux » : certains modes d'interception vont ainsi « accidentellement », « par inadvertance » – mais en réalité de façon tout à fait providentielle – aspirer tous les paquets de données transitant au voisinage des sélecteurs officiellement visés [18].

Parce que le débat américain se polarise à peu près exclusivement sur la question des écoutes domestiques et de la vie privée des citoyens des États-Unis, ces deux premiers programmes (métadonnées et PRISM) ont été largement médiatisés. Mais cette focalisation tend à déformer le tableau, car une grande partie du ratissage de données s'effectue, autant qu'on puisse le savoir, à l'ombre d'une autre subtilité

Traditionnellement, le renseignement intervenait surtout dans les phases préparatoires de reconnaissance. Il s'incorpore désormais en temps réel à la phase opérationnelle : « *Aujourd'hui, le renseignement est opération* [51]. » Ce déplacement est lié à une profonde réforme du « cycle de ciblage » impulsée en Irak par le Joint Special Operations Command (JSOC). L'idée, expose le général McChrystal, « *était de combiner les analystes qui trouvent l'ennemi, [...] les opérateurs de drones qui ferrent la cible, les unités combattantes qui la terminent [...], les spécialistes qui exploitent les renseignements obtenus dans le raid – dont les téléphones portables. [...] En faisant cela, nous avons réussi à accélérer le cycle* [52] ». Tandis qu'au début de la guerre, l'analyse des renseignements collectés lors d'une opération pouvait prendre des semaines, la mise en place de ce cycle agressif permit de faire tourner la « *kill chain* » à plein régime et de multiplier les raids nocturnes, chaque nouvelle opération permettant de trouver, par chaînage de contacts, de nouveaux suspects que l'on ciblait sur-le-champ et de remonter ainsi de proche en proche jusqu'à « *des gens dont on ignorait même l'existence au début de la nuit* [53] » : on passa ainsi de dix-huit raids par mois en aout 2004 à trois cents raids par mois en 2006 – « *dix chaque*

L'écusson de Geocell

Ce partenariat entre la NGA et la NSA a été décrit comme un « *basculement décisif* [47] ». La révolution consistait en une synthèse perceptive : voir ce que l'on écoute et regarder ce que l'on entend. Réunir « les yeux et les oreilles » de la machine de guerre, fusionner ce que l'on appelle, également dans ce jargon, deux « phénoménologies ». Dans le processus, les deux agences hybridaient aussi leurs savoir-faire. Il en résulta une nouvelle discipline, l'« analyse géospatiale du renseignement électromagnétique ». Pour former les analystes à cette spécialité émergente, on mit en place un cursus spécial, le Geocell bootcamp, sur la base de Goodfellow (Texas) [48]. Divers outils informatiques furent également développés, dont le logiciel Analyst Notebook, qui permet, souligne la notice d'IBM, de présenter presque toutes les données disponibles « *en une seule image analytique combinant l'analyse géospatiale, associative et temporelle* [49] ». Équipés de telles interfaces de visualisation, les analystes, explique Derek Gregory, s'occupent de « *suivre plusieurs individus à travers différents réseaux sociaux afin d'établir une forme ou un "schéma de vie" ["pattern of life"]* [50] ».

juridique, l'autorisation exécutive 12333, héritée de l'administration Reagan [19]. Cette disposition négligée et pourtant capitale recouvre entre autres le programme MUSCULAR, utilisé pour piller les *data centers* de Google à travers le monde [20]. Le programme DANCINGOASIS, qui siphonne pour sa part les câbles de fibre optique situés entre l'Europe et le Moyen-Orient, est l'une des plus importantes sources de ce genre, avec plus de 57 milliards d'entrées en un mois fin 2012 [21]. Il faudrait aussi évoquer les partenariats de la NSA avec les services de pays « amis », dont son équivalent britannique, le GCHQ. Quoi qu'il en soit, pour faire face à cette avalanche numérique, la NSA – l'une des plus importantes agences de renseignement au monde, avec un budget de plus de 10 milliards de dollars et des dizaines de milliers d'employés – a fait construire un gigantesque *data center* en plein pays mormon, dans l'Utah, capable de stocker plusieurs exabits (1 exabit = 1 milliard de gigabits) de données.

Pour analyser les données collectées, on mobilise notamment deux grands types de méthodes. Dans une première catégorie, XKEYSCORE fonctionne comme un moteur de recherche par « sélecteurs faibles », c'est-à-dire des mots clés ou des requêtes du type « montre-moi tous les individus qui parlent en allemand au Pakistan [22] ». Si l'on

L'écusson de Geocell

Ce partenariat entre la NGA et la NSA a été décrit comme un « *basculement décisif* [47] ». La révolution consistait en une synthèse perceptive : voir ce que l'on écoute et regarder ce que l'on entend. Réunir « les yeux et les oreilles » de la machine de guerre, fusionner ce que l'on appelle, également dans ce jargon, deux « phénoménologies ». Dans le processus, les deux agences hybridaient aussi leurs savoir-faire. Il en résulta une nouvelle discipline, l'« analyse géospatiale du renseignement électromagnétique ». Pour former les analystes à cette spécialité émergente, on mit en place un cursus spécial, le Geocell bootcamp, sur la base de Goodfellow (Texas) [48]. Divers outils informatiques furent également développés, dont le logiciel Analyst Notebook, qui permet, souligne la notice d'IBM, de présenter presque toutes les données disponibles « *en une seule image analytique combinant l'analyse géospatiale, associative et temporelle* [49] ». Équipés de telles interfaces de visualisation, les analystes, explique Derek Gregory, s'occupent de « *suivre plusieurs individus à travers différents réseaux sociaux afin d'établir une forme ou un "schéma de vie" ["pattern of life"]* [50] ».

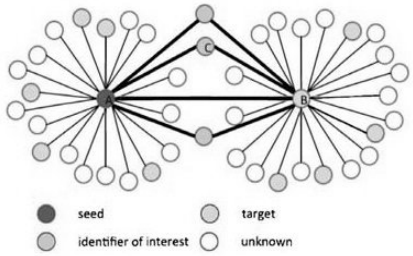
28

juridique, l'autorisation exécutive 12333, héritée de l'administration Reagan [19]. Cette disposition négligée et pourtant capitale recouvre entre autres le programme MUSCULAR, utilisé pour piller les *data centers* de Google à travers le monde [20]. Le programme DANCINGOASIS, qui siphonne pour sa part les câbles de fibre optique situés entre l'Europe et le Moyen-Orient, est l'une des plus importantes sources de ce genre, avec plus de 57 milliards d'entrées en un mois fin 2012 [21]. Il faudrait aussi évoquer les partenariats de la NSA avec les services de pays « amis », dont son équivalent britannique, le GCHQ. Quoi qu'il en soit, pour faire face à cette avalanche numérique, la NSA – l'une des plus importantes agences de renseignement au monde, avec un budget de plus de 10 milliards de dollars et des dizaines de milliers d'employés – a fait construire un gigantesque *data center* en plein pays mormon, dans l'Utah, capable de stocker plusieurs exabits (1 exabit = 1 milliard de gigabits) de données.

Pour analyser les données collectées, on mobilise notamment deux grands types de méthodes. Dans une première catégorie, XKEYSCORE fonctionne comme un moteur de recherche par « sélecteurs faibles », c'est-à-dire des mots clés ou des requêtes du type « montre-moi tous les individus qui parlent en allemand au Pakistan [22] ». Si l'on

17

découvre, par ce biais ou par un autre, un individu intéressant, on peut passer à un second type de méthode : l'analyse des liens. Le procédé de « chaînage des contacts » (« *contact chaining* ») consiste à « *construire un graphe de réseau qui modélise les schémas communicationnels (email, téléphone, etc.) d'entités ciblées* [23] ». On part d'un identifiant, appelé « graine », et on suit les tiges qui se mettent progressivement à germer. À mesure que les contacts se nouent, on obtient des arborescences bourgeonnantes, en forme de pissenlits. La cible se conçoit ici fondamentalement comme une individualité réticulaire. Ce que l'on cherche à connaître, par effraction dans la vie privée, c'est la *vie sociale*.



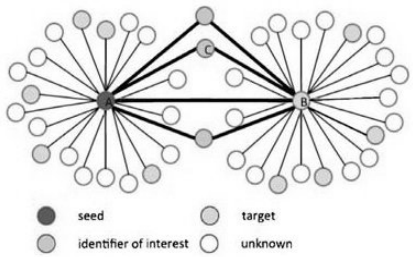
Le « chainage des contacts »

Mais, à nouveau, que cette analyse soit « ciblée » ne lui interdit pas d'être proliférante. Dans le cas

guerre contre-insurrectionnelle. En 2007, l'agence déploya en Irak un nouvel outil informatique appelé « Real Time Regional Gateway ». Il permettait de « *capturer toutes les données, de les archiver et de les rendre immédiatement disponibles pour les analystes* [43] ». Mais l'apport crucial de ce réseau, soulignait Pete Rustan, était sa capacité « *d'intégrer et de géolocaliser les signaux* [44] ». Tout l'enjeu, en effet, était de « *convertir les métadonnées en renseignements actionnables* [45] », c'est-à-dire en cibles. Ce travail fut confié à des équipes spéciales. Leur écusson montrait un personnage d'espion tout droit tiré d'une bande dessinée de *MAD Magazine,* armé d'une loupe-viseur dirigée sur des empreintes de pas rouge sang au sommet d'une dune. Le slogan rendait les choses explicites : « *Nous les traquons, vous les buttez.* »

Cette devise était celle des équipes Geocell, nées d'une collaboration inédite initiée au début des années 2000, entre la NSA et sa sœur siamoise, encore méconnue, la National Geospatial Agency (NGA). La finalité de ces « cellules de géolocalisation » était, par l'analyse combinée des signaux et de l'imagerie, de « *traquer géographiquement les individus en temps réel* [46] ».

découvre, par ce biais ou par un autre, un individu intéressant, on peut passer à un second type de méthode : l'analyse des liens. Le procédé de « chaînage des contacts » (« *contact chaining* ») consiste à « *construire un graphe de réseau qui modélise les schémas communicationnels (email, téléphone, etc.) d'entités ciblées* [23] ». On part d'un identifiant, appelé « graine », et on suit les tiges qui se mettent progressivement à germer. À mesure que les contacts se nouent, on obtient des arborescences bourgeonnantes, en forme de pissenlits. La cible se conçoit ici fondamentalement comme une individualité réticulaire. Ce que l'on cherche à connaître, par effraction dans la vie privée, c'est la *vie sociale*.



Le « chainage des contacts »

Mais, à nouveau, que cette analyse soit « ciblée » ne lui interdit pas d'être proliférante. Dans le cas

guerre contre-insurrectionnelle. En 2007, l'agence déploya en Irak un nouvel outil informatique appelé « Real Time Regional Gateway ». Il permettait de « *capturer toutes les données, de les archiver et de les rendre immédiatement disponibles pour les analystes* [43] ». Mais l'apport crucial de ce réseau, soulignait Pete Rustan, était sa capacité « *d'intégrer et de géolocaliser les signaux* [44] ». Tout l'enjeu, en effet, était de « *convertir les métadonnées en renseignements actionnables* [45] », c'est-à-dire en cibles. Ce travail fut confié à des équipes spéciales. Leur écusson montrait un personnage d'espion tout droit tiré d'une bande dessinée de *MAD Magazine,* armé d'une loupe-viseur dirigée sur des empreintes de pas rouge sang au sommet d'une dune. Le slogan rendait les choses explicites : « *Nous les traquons, vous les buttez.* »

Cette devise était celle des équipes Geocell, nées d'une collaboration inédite initiée au début des années 2000, entre la NSA et sa sœur siamoise, encore méconnue, la National Geospatial Agency (NGA). La finalité de ces « cellules de géolocalisation » était, par l'analyse combinée des signaux et de l'imagerie, de « *traquer géographiquement les individus en temps réel* [46] ».

si l'adversaire « *ne peut plus être identifié par ce qu'il est, théorise-t-on, il peut en revanche l'être par ce qu'il fait* [41] ». Surveiller l'activité pour en induire l'identité.

À cette fin, l'outil technologique décisif fut le drone. L'engin, capable de demeurer en l'air pendant des heures, rend possible une « surveillance persistante ». On parle d'un œil qui ne cligne jamais. Traditionnellement, le renseignement géographique s'était focalisé sur les éléments plus ou moins statiques du terrain. Le regard persistant de la caméra changeait la donne : l'imagerie pouvait désormais capturer les activités mouvantes des populations. *Via* des moyens high-tech, les analystes héritaient d'anciennes tâches de planque et de filature policières transposées en contexte militaire. Les drones n'avaient pas seulement des caméras à leur bord, mais aussi d'autres types de capteurs, dont de petits boîtiers capables d'intercepter les signaux des téléphones portables en contrebas [42]. Cet élément était capital : combiner imagerie vidéo et interception des signaux allait former le creuset pour une refonte des éléments constitutifs de la surveillance armée.

En parallèle, la NSA, avec Alexander à sa tête, appliquait son principe de collecte totale à la

des métadonnées téléphoniques, étant donné la règle dite des « trois degrés de séparation », « *un analyste qui fait une requête à propos d'un numéro de téléphone suspect peut voir des relevés d'appels impliquant les numéros de téléphone qui ont eu un contact avec un numéro de téléphone qui a eu un contact avec un numéro de téléphone qui a eu un contact avec la cible de départ. Si une "graine" a par exemple 75 contacts directs et si chacun de ces contacts en a lui aussi 75, chaque requête fournit [...] les relevés complets de 5 625 numéros de téléphone. Et si chacun de ces numéros situés à deux degrés de séparation a lui-même 75 nouveaux contacts, une seule requête aboutit à une masse de relevés téléphoniques impliquant plus de 420 000 numéros* [25] ».

Surveillance programmatique et machines à remonter le temps

Dans le sillage des révélations de Snowden, on a beaucoup dit que les programmes de la NSA opéraient une « surveillance totale » – Big Brother ou panoptique. Il faut sans doute préciser le diagnostic. La thèse d'une NSA capable *de tout collecter et de tout analyser,* outre le fait qu'elle est empiriquement fausse, a aussi le tort, en véhiculant l'image incapacitante d'un pouvoir à l'emprise absolue, d'être politiquement contre-

si l'adversaire « *ne peut plus être identifié par ce qu'il est, théorise-t-on, il peut en revanche l'être par ce qu'il fait* [41] ». Surveiller l'activité pour en induire l'identité.

À cette fin, l'outil technologique décisif fut le drone. L'engin, capable de demeurer en l'air pendant des heures, rend possible une « surveillance persistante ». On parle d'un œil qui ne cligne jamais. Traditionnellement, le renseignement géographique s'était focalisé sur les éléments plus ou moins statiques du terrain. Le regard persistant de la caméra changeait la donne : l'imagerie pouvait désormais capturer les activités mouvantes des populations. *Via* des moyens high-tech, les analystes héritaient d'anciennes tâches de planque et de filature policières transposées en contexte militaire. Les drones n'avaient pas seulement des caméras à leur bord, mais aussi d'autres types de capteurs, dont de petits boîtiers capables d'intercepter les signaux des téléphones portables en contrebas [42]. Cet élément était capital : combiner imagerie vidéo et interception des signaux allait former le creuset pour une refonte des éléments constitutifs de la surveillance armée.

En parallèle, la NSA, avec Alexander à sa tête, appliquait son principe de collecte totale à la

26

des métadonnées téléphoniques, étant donné la règle dite des « trois degrés de séparation », « *un analyste qui fait une requête à propos d'un numéro de téléphone suspect peut voir des relevés d'appels impliquant les numéros de téléphone qui ont eu un contact avec un numéro de téléphone qui a eu un contact avec un numéro de téléphone qui a eu un contact avec la cible de départ. Si une "graine" a par exemple 75 contacts directs et si chacun de ces contacts en a lui aussi 75, chaque requête fournit [...] les relevés complets de 5 625 numéros de téléphone. Et si chacun de ces numéros situés à deux degrés de séparation a lui-même 75 nouveaux contacts, une seule requête aboutit à une masse de relevés téléphoniques impliquant plus de 420 000 numéros* [25] ».

Surveillance programmatique et machines à remonter le temps

Dans le sillage des révélations de Snowden, on a beaucoup dit que les programmes de la NSA opéraient une « surveillance totale » – Big Brother ou panoptique. Il faut sans doute préciser le diagnostic. La thèse d'une NSA capable *de tout collecter et de tout analyser,* outre le fait qu'elle est empiriquement fausse, a aussi le tort, en véhiculant l'image incapacitante d'un pouvoir à l'emprise absolue, d'être politiquement contre-

19

productive. Ces dispositifs n'ont en fait ni la capacité ni même la volonté de surveiller *activement tout le monde.* Cela ne veut bien sûr pas dire qu'ils ne sont pas dangereux.

Pour caractériser plus distinctement la chose, on peut recourir au concept de « surveillance programmatique ». Cette notion renvoie à une expression juridique précise : l'« approbation programmatique », octroyée à la NSA par la cour secrète qui chapeaute une partie de ses activités [26]. Traditionnellement, on autorisait *individuellement* par mandat judiciaire la mise sur écoute de tel ou tel suspect. Les pouvoirs spéciaux mis en place à la suite du 11 Septembre ont fait sauter ce verrou, pourtant déjà mince : la cour autorise désormais en bloc certains *programmes* de surveillance, laissant ainsi à la NSA le pouvoir de choisir elle-même ses cibles. Interrogé sur ce que recouvrait le critère de « suspicion raisonnable et articulable » censé encadrer en interne l'exercice de cette prérogative, le directeur juridique de la NSA lâcha un jour, en pleine audition officielle : *« En fait, c'est exactement la même norme que pour le "stop and frisk"* [27] » – c'est-à-dire la pratique policière pour le moins controversée du « contrôle au faciès ».

L'antiterrorisme n'est que l'une des multiples missions de la NSA, dont la panoplie comporte des préoccupations aussi variées que surveiller les activités politiques internes de pays dont on veut protéger le régime, dont l'Arabie saoudite, suivre des processus politiques représentant une menace pour les intérêts américains, dont l'« é_volution des mouvements bolivariens en Amérique du Sud_ [38] », ou espionner les activités technologiques de puissances étrangères. D'où la surveillance de la chancelière Merkel, de Dilma Rousseff, ou d'industriels chinois…

Les yeux et les oreilles de la machine de guerre

Mais la NSA, ça sert, avant tout, à faire la guerre. Les champs de bataille d'Afghanistan et d'Irak ont été de grands laboratoires, de vastes aires d'expérimentation à ciel ouvert pour de nouvelles armes. Les agences de renseignement américaines y ont élaboré un nouveau modèle de « renseignement, de surveillance et de reconnaissance » [« Intelligence Surveillance and Reconnaissance »]. Le premier problème de la guerre contre-insurrectionnelle est de repérer les « *ennemis à contraste faible* [39] » – qui se fondent dans le paysage, qui n'émettent plus « *de signatures militaires de type soviétique* [40] ». Or,

productive. Ces dispositifs n'ont en fait ni la capacité ni même la volonté de surveiller *activement tout le monde.* Cela ne veut bien sûr pas dire qu'ils ne sont pas dangereux.

Pour caractériser plus distinctement la chose, on peut recourir au concept de « surveillance programmatique ». Cette notion renvoie à une expression juridique précise : l'« approbation programmatique », octroyée à la NSA par la cour secrète qui chapeaute une partie de ses activités [26]. Traditionnellement, on autorisait *individuellement* par mandat judiciaire la mise sur écoute de tel ou tel suspect. Les pouvoirs spéciaux mis en place à la suite du 11 Septembre ont fait sauter ce verrou, pourtant déjà mince : la cour autorise désormais en bloc certains *programmes* de surveillance, laissant ainsi à la NSA le pouvoir de choisir elle-même ses cibles. Interrogé sur ce que recouvrait le critère de « suspicion raisonnable et articulable » censé encadrer en interne l'exercice de cette prérogative, le directeur juridique de la NSA lâcha un jour, en pleine audition officielle : *« En fait, c'est exactement la même norme que pour le "stop and frisk"* [27] » – c'est-à-dire la pratique policière pour le moins controversée du « contrôle au faciès ».

L'antiterrorisme n'est que l'une des multiples missions de la NSA, dont la panoplie comporte des préoccupations aussi variées que surveiller les activités politiques internes de pays dont on veut protéger le régime, dont l'Arabie saoudite, suivre des processus politiques représentant une menace pour les intérêts américains, dont l'« é_volution des mouvements bolivariens en Amérique du Sud_ [38] », ou espionner les activités technologiques de puissances étrangères. D'où la surveillance de la chancelière Merkel, de Dilma Rousseff, ou d'industriels chinois…

Les yeux et les oreilles de la machine de guerre

Mais la NSA, ça sert, avant tout, à faire la guerre. Les champs de bataille d'Afghanistan et d'Irak ont été de grands laboratoires, de vastes aires d'expérimentation à ciel ouvert pour de nouvelles armes. Les agences de renseignement américaines y ont élaboré un nouveau modèle de « renseignement, de surveillance et de reconnaissance » [« Intelligence Surveillance and Reconnaissance »]. Le premier problème de la guerre contre-insurrectionnelle est de repérer les « *ennemis à contraste faible* [39] » – qui se fondent dans le paysage, qui n'émettent plus « *de signatures militaires de type soviétique* [40] ». Or,

contre rien. Mais cette manière de dire les choses est encore incorrecte. Ce que l'on perdait, au prétexte d'un gain en sécurité, était en fait une part supplémentaire de *sûreté,* au sens classique que cette notion revêt depuis les Lumières, à savoir la protection contre l'arbitraire d'un pouvoir d'État, et plus particulièrement d'un pouvoir de police.

Contrairement au discours officiel qui les a légitimés, ces instruments se révèlent de piètres moyens de détection antiterroriste : leur fonction réelle est ailleurs. C'est à cette lumière qu'il faut lire la confidence suivante, glissée par l'ancien directeur de la NSA Michael Hayden dans l'entre-soi d'un *think tank* de Washington : « *Je crois que nos dirigeants ont beaucoup trop cherché à justifier les activités de la NSA sur une base étroitement antiterroriste. Une telle justification est tout simplement inadéquate au regard de ce que font les États-Unis. Nous avons beaucoup d'autres motivations [...] liées à la souveraineté étatique* [36]. » Edward Snowden, de son côté, ne dit pas non plus autre chose : « *Ces programmes n'ont jamais été conçus en réaction au terrorisme : il s'agit d'espionnage économique, de contrôle social et de manipulation diplomatique. C'est une question de pouvoir* [37]. »

Qualifier ces programmes de « surveillance programmatique » *au sens large* permet de comprendre ceci : il ne s'agit pas tant pour la NSA de surveiller activement tout le monde que de se doter des capacités de cibler *n'importe qui* – ou plutôt *qui bon lui semble.* Les cibles de la surveillance active seront définies selon les priorités inscrites à l'ordre du jour, c'est-à-dire en fonction du « programme », pris cette fois au sens de l'ensemble des « actions que l'on se propose d'accomplir ». Ce programme, faut-il le préciser, n'est autre que celui de la raison d'État.

Un dispositif récemment révélé par Edward Snowden permet de se faire une idée des projets de l'agence à plus longue échéance. MYSTIC est un « *système de surveillance capable d'enregistrer 100 % des appels téléphoniques d'un pays* [28] ». Il a été testé par la NSA aux Bahamas et déployé dans un autre pays non identifié, vraisemblablement l'Afghanistan [29]. Le dispositif de stockage associé, SOMALGET, est aujourd'hui capable de conserver les enregistrements de toutes les conversations durant un mois [30]. On peut ainsi « *repasser les voix enregistrées de n'importe quel appel téléphonique sans qu'il ait été besoin d'identifier au préalable la personne comme étant une cible à surveiller* [31] ». Collecte totale et surveillance

contre rien. Mais cette manière de dire les choses est encore incorrecte. Ce que l'on perdait, au prétexte d'un gain en sécurité, était en fait une part supplémentaire de *sûreté,* au sens classique que cette notion revêt depuis les Lumières, à savoir la protection contre l'arbitraire d'un pouvoir d'État, et plus particulièrement d'un pouvoir de police.

Contrairement au discours officiel qui les a légitimés, ces instruments se révèlent de piètres moyens de détection antiterroriste : leur fonction réelle est ailleurs. C'est à cette lumière qu'il faut lire la confidence suivante, glissée par l'ancien directeur de la NSA Michael Hayden dans l'entre-soi d'un *think tank* de Washington : « *Je crois que nos dirigeants ont beaucoup trop cherché à justifier les activités de la NSA sur une base étroitement antiterroriste. Une telle justification est tout simplement inadéquate au regard de ce que font les États-Unis. Nous avons beaucoup d'autres motivations [...] liées à la souveraineté étatique* [36]. » Edward Snowden, de son côté, ne dit pas non plus autre chose : « *Ces programmes n'ont jamais été conçus en réaction au terrorisme : il s'agit d'espionnage économique, de contrôle social et de manipulation diplomatique. C'est une question de pouvoir* [37]. »

24

Qualifier ces programmes de « surveillance programmatique » *au sens large* permet de comprendre ceci : il ne s'agit pas tant pour la NSA de surveiller activement tout le monde que de se doter des capacités de cibler *n'importe qui* – ou plutôt *qui bon lui semble.* Les cibles de la surveillance active seront définies selon les priorités inscrites à l'ordre du jour, c'est-à-dire en fonction du « programme », pris cette fois au sens de l'ensemble des « actions que l'on se propose d'accomplir ». Ce programme, faut-il le préciser, n'est autre que celui de la raison d'État.

Un dispositif récemment révélé par Edward Snowden permet de se faire une idée des projets de l'agence à plus longue échéance. MYSTIC est un « *système de surveillance capable d'enregistrer 100 % des appels téléphoniques d'un pays* [28] ». Il a été testé par la NSA aux Bahamas et déployé dans un autre pays non identifié, vraisemblablement l'Afghanistan [29]. Le dispositif de stockage associé, SOMALGET, est aujourd'hui capable de conserver les enregistrements de toutes les conversations durant un mois [30]. On peut ainsi « *repasser les voix enregistrées de n'importe quel appel téléphonique sans qu'il ait été besoin d'identifier au préalable la personne comme étant une cible à surveiller* [31] ». Collecte totale et surveillance

21

ciblée ne s'opposent pas : elles se combinent parfaitement sur le double mode de l'archivage provisionnel et de l'analyse rétrospective. Ce qui a été construit là, se félicite-t-on, c'est une petite « *machine à remonter le temps* [32] ».

Cette capacité de « récupération rétrospective » – ici au stade embryonnaire, sur une durée encore limitée – est essentielle pour saisir les visées de l'agence à plus long terme. L'objectif n'est pas seulement de surveiller certaines cibles en temps réel, mais aussi de pouvoir retracer l'itinéraire relationnel de n'importe quelle individualité devenue entre-temps intéressante. On rêve de constituer, sur chacun et par collecte automatique, des dossiers dormants. Un tel dispositif archivistique constituerait l'instrument d'un *pouvoir biographique* fondé sur la capture informationnelle généralisée des micro-histoires de vies.

Alors que l'ambition du *datamining* prédictif était de déceler dans le présent des traces de l'avenir, ici, la perspective s'inverse : recueillir dans le présent les archives d'un passé futur. N'importe qui pouvant un jour devenir une cible, on voudrait anticiper l'actualisation de ce devenir-cible en archivant les vies de tous. Parce qu'elle a pour objet l'indétermination du devenir, cette

rationalité tend elle-même à devenir, en sa dynamique, illimitée.

Une question de pouvoir

En juin 2013, Alexander affirma que les programmes de surveillance de la NSA avaient permis de déjouer des douzaines de « *complots terroristes* » [33]. En octobre de la même année, le général révisa son estimation à la baisse, évoquant treize « *événements* » en rapport avec le territoire américain, avant d'admettre que le nombre de menaces étouffées dans l'œuf par le programme de collecte des métadonnées téléphoniques se montait à une, ou peut-être deux [34]. En fin de compte, ne resta qu'un seul « *complot* » à avoir été déjoué par plus de dix ans de collecte massive des fadettes téléphoniques états-uniennes : un habitant de San Diego arrêté pour avoir envoyé 8 500 dollars à un groupe militant somalien [35].

Alors que l'on se creusait depuis un certain temps les méninges pour disserter en mauvais philosophes sur le moins injuste compromis entre sécurité et liberté, ce qui s'était produit en pratique ne correspondait en rien à l'intitulé choisi, qui s'avérait parfaitement hors sujet. On n'échangeait pas une portion de liberté contre une dose de sécurité. On échangeait une part de liberté

ciblée ne s'opposent pas : elles se combinent parfaitement sur le double mode de l'archivage provisionnel et de l'analyse rétrospective. Ce qui a été construit là, se félicite-t-on, c'est une petite « *machine à remonter le temps* [32] ».

Cette capacité de « récupération rétrospective » – ici au stade embryonnaire, sur une durée encore limitée – est essentielle pour saisir les visées de l'agence à plus long terme. L'objectif n'est pas seulement de surveiller certaines cibles en temps réel, mais aussi de pouvoir retracer l'itinéraire relationnel de n'importe quelle individualité devenue entre-temps intéressante. On rêve de constituer, sur chacun et par collecte automatique, des dossiers dormants. Un tel dispositif archivistique constituerait l'instrument d'un *pouvoir biographique* fondé sur la capture informationnelle généralisée des micro-histoires de vies.

Alors que l'ambition du *datamining* prédictif était de déceler dans le présent des traces de l'avenir, ici, la perspective s'inverse : recueillir dans le présent les archives d'un passé futur. N'importe qui pouvant un jour devenir une cible, on voudrait anticiper l'actualisation de ce devenir-cible en archivant les vies de tous. Parce qu'elle a pour objet l'indétermination du devenir, cette

22

rationalité tend elle-même à devenir, en sa dynamique, illimitée.

Une question de pouvoir

En juin 2013, Alexander affirma que les programmes de surveillance de la NSA avaient permis de déjouer des douzaines de « *complots terroristes* » [33]. En octobre de la même année, le général révisa son estimation à la baisse, évoquant treize « *événements* » en rapport avec le territoire américain, avant d'admettre que le nombre de menaces étouffées dans l'œuf par le programme de collecte des métadonnées téléphoniques se montait à une, ou peut-être deux [34]. En fin de compte, ne resta qu'un seul « *complot* » à avoir été déjoué par plus de dix ans de collecte massive des fadettes téléphoniques états-uniennes : un habitant de San Diego arrêté pour avoir envoyé 8 500 dollars à un groupe militant somalien [35].

Alors que l'on se creusait depuis un certain temps les méninges pour disserter en mauvais philosophes sur le moins injuste compromis entre sécurité et liberté, ce qui s'était produit en pratique ne correspondait en rien à l'intitulé choisi, qui s'avérait parfaitement hors sujet. On n'échangeait pas une portion de liberté contre une dose de sécurité. On échangeait une part de liberté

23