Décadrages

Cinéma, à travers champs

26-27 | 2014

Drones, cartographie et images automatisées

Vision (prédatrice) alpha

Joël Vacheron

Édition électronique

URL : <https://journals.openedition.org/decadrages/746>

DOI : 10.4000/decadrages.746

ISSN : 2297-5977

Éditeur

Association Décadrages

Édition imprimée

Date de publication : 10 avril 2014

Pagination : 111-128

ISBN : 978-2-9700668-8-0

ISSN : 2235-7823

Référence électronique

Joël Vacheron, « Vision (prédatrice) alpha », *Décadrages* [En ligne], 26-27 | 2014, mis en ligne le 14 décembre 2015, consulté le 03 avril 2022. URL : <http://journals.openedition.org/decadrages/746> ; DOI : <https://doi.org/10.4000/decadrages.746>

Joël Vacheron

Vision (prédatrice) alpha

Le contrôle ne peut s'exercer sans notre complicité.

Mark Fisher¹

Pas de répit

Avant de connaître un large succès commercial avec leurs scénarios pour *Wild Wild West* (1999) ou *Mission to Mars* (2000), Jim et John Thomas s'étaient fait la main en signant *Hard Time on Planet Earth* (1989). Au fil de 13 épisodes insipides, ils exprimaient leur penchant pour une approche candide de la science-fiction. Le héros de la série est un officier de race extraterrestre, condamné à séjourner sur Terre sous les traits d'un être humain. Le synopsis s'échafaude autour des surprises et autres quiproquos jalonnant la difficile acculturation de Jesse. Le résultat n'a pas convaincu, et la série a pris fin au terme de sa première saison. Reléguée aux oubliettes, il est difficile aujourd'hui encore de trouver un quelconque intérêt à raviver le souvenir de cette saga.

Hard Time on Planet Earth présente toutefois un élément remarquable. En effet, le héros principal est accompagné d'une sorte d'amibe bionique virevoltant continuellement à ses côtés. Ce compagnon observe, suit et commente les faits et gestes de l'apprenti terrien, le prévenant de sa voix métallique des décisions et à des actions à prendre. Dans certaines situations, il tente vainement de communiquer avec des feux de signalisation ou une tondeuse à gazon. Dans d'autres, son écran sert à diffuser des extraits de films ou de programmes télévisés susceptibles d'apporter des solutions à chaque problème rencontré. Lorsqu'il n'est pas engagé dans un de ses monologues pataphysiques, il réfère les écarts de Jesse à travers cette formule récurrente: «*Negative Outcome. Not Good*»². Résultat bâtard de la fusion entre une coque d'iMac G3 et d'un dispositif CCTV, cet œil unique porte le nom de *Control*. Sa mission sur Terre consiste par conséquent à assister Jesse à traiter la masse d'informations extraordinaire qu'il est amené à gérer. Assistant personnel,

¹ Mark Fisher, *Capitalist Realism: Is There No Alternative?*, Winchester, Zero Books, 2009, p. 22. Traduction de l'auteur.

² Traduit par «Agressivité, pas bon» dans l'adaptation française de la série.

3 Comme le souligne Nicolas Nova : « A l'époque, je le trouvais à la fois effrayant et fascinant [...] et je pense qu'il peut être considéré en puissance comme un indicateur / un signal faible de potentiels «drones personnels». Ceux-ci peuvent apparaître comme la dernière actualisation de moyens d'assistance de surveillance à domicile, ou comme une espèce d'assistant personnel. » Voir <http://betaknowledge.tumblr.com/post/29025433750/hard-time-on-planet-earth-is-an-american-science> (dernière consultation le 1^{er} avril 2014). Traduction de l'auteur.

Martin Kove et *Control*, les deux protagonistes principaux de « Hard Time on Planet Earth » (1989). La série a été diffusée pour la première fois sur une chaîne française au début des années 1990 sous le nom de « Pas de répit sur la planète Terre ». La série laissera une impression mitigée ; à son propos, un critique notait : « Il n'y a pas eu de séries aussi outrageusement stupides et absolument dénuées d'intérêt depuis *Misfits of Science* » (Jicha, Tom, « « Hard Time » Clunker Really Hard to Stomach », *Sun Sentinel*, 1^{er} mars 1989).

caméra de surveillance, bracelet électronique et drone personnalisé, *Control* serait un agent idéal dans une période où les aides décisionnelles sont devenues indispensables pour gérer les flux de Big datas. A la fois réconfortant et inquiétant, il constitue un prototype pour interroger la présence ambivalente et intrigante des agents intelligents dans notre quotidien³.

Pour Foucault, les sociétés disciplinaires étaient historiquement organisées à partir de lieux physiques clos tels que la prison et, par extension, les usines ou les écoles. Au centre de ce modèle de société, les dispositifs panoptiques devaient permettre à l'observateur de tout voir et de tout entendre sans pour autant être visible. A partir de ce modèle architectural, Foucault a largement contribué à définir la manière dont le pouvoir peut influencer sur l'intimité des individus. Dans *Surveiller et punir*,

il mentionne à quel point cette technologie d'Etat opère essentiellement de manière intestine⁴. Avec l'essor des systèmes de communication, en particulier l'usage de la vidéosurveillance, les modalités d'action du contrôle se sont énormément diversifiées. Désormais, ces dispositifs sont à tel point banalisés que même des émissions de TV jouent sur leurs effets de réalité et la persistance de l'auto-discipline. «*Le contrôle ne peut s'exercer sans notre complicité*»⁵, affirme Mark Fisher dans son analyse des mutations récentes du modèle capitaliste. Les atteintes répétées exercées actuellement à l'encontre des libertés individuelles témoignent du fait que, même si nous ne sommes pas tous devenus complices, nous faisons preuve d'une passivité douteuse par rapport aux décisions de *Control*.

Notre intention n'est pas de détailler directement les avancées technologiques dans le domaine, ni même de dresser un inventaire des innombrables questions éthiques ou philosophiques actuellement mises en jeu. Nous proposons plutôt d'interroger quelques *modulations* et *hallucinations* que les êtres computationnels parviennent à introduire dans nos manières de voir. A ce titre, nous porterons une attention particulière au couplage entre des dispositifs biométriques dits «doux» (Soft biometrics⁶) et les drones (Unmanned Aerial System) – même si, à l'heure actuelle, les résultats sont peu probants. Les avatars de *Control* à venir seront essentiellement conçus pour identifier, localiser, voire même intercepter des acteurs humains ou non-humains. L'énergie déployée de toutes parts pour accélérer cette synergie ne manque pas de soulever quelques interrogations. Quel est l'horizon d'attente des stratégies mises en œuvre en matière de politique sécuritaire? Quelles sont les techniques développées en matière d'identification biométrique? Comment s'opère la distinction entre des recherches à des fins commerciales et les agendas politiques? Au-delà des inquiétudes légitimes sur les dérives liberticides occasionnées par ces agents autopilotés, c'est la nature (prédatrice) de la vision qui peut être questionnée.

Des yeux dans le ciel

Les avatars contemporains les plus spectaculaires de *Control* sont certainement à classer dans la catégorie Lethal Autonomous Robotics (LARs): à savoir le matériel de guerre qui peut opérer sans assistance humaine. Dans une série d'interventions présentées devant la Chambre des

⁴ «*Nous ne sommes ni sur les gradins ni sur la scène, mais dans la machine panoptique, investis par ses effets de pouvoir que nous reconduisons nous-mêmes, puisque nous en sommes un rouage.*» (Michel Foucault, *Surveiller et punir: Naissance de la prison*, Paris, Folio, 1993, p. 238).

⁵ «Control only works if you are complicit with it.» (Mark Fisher, *op. cit.*).

⁶ Antitza Dantcheva et al., «Bag of Soft Biometrics for Person Identification: New Trends and Challenges», *Multimedia Tools and Applications*, octobre 2010, pp. 1-39.

représentants en mai 2013, des experts étaient invités à interroger les dérives potentielles de ce type d'automatisation. Le rapport, intitulé « Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems », présente un tableau particulièrement précis de l'impact de ces dispositifs sur les libertés individuelles :

« Comme vous le savez, les drones peuvent être équipés d'appareils de prises de vues sophistiqués, de caméras à vision nocturne, de lecteurs de plaques d'immatriculation et de systèmes de radar laser. Suivant un récent article du Service de recherche du Congrès, les drones seront bientôt capables d'opérer avec des systèmes de reconnaissance faciale et biométrique qui peuvent reconnaître et traquer des individus selon leurs attributs physiques, tels que la taille, l'âge, le sexe et la couleur de peau. En regard de la technologie avancée désormais disponible, comparer un drone à un avion ou un hélicoptère traditionnels revient à comparer une fouille exercée par un officier de police à une machine moderne à rayons-x qui peut voir à travers les habits et représenter graphiquement les traits physiques d'une personne. »⁷

7 « Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems, Hearing before the Subcommittee on Crime, Terrorism, Homeland Security and Investigation », mai 2013.

A l'instar du Professeur Tracey Maclin, qui s'inquiète des conséquences de cette évolution sur le quatrième amendement de la Constitution des Etats-Unis, l'ensemble des commentaires évoque le changement profond qui s'opère actuellement.

8 Voir Eyal Weizman, *Mengele's Skull: The Advent of a Forensic Aesthetics*, Berlin, Sternberg Press, 2012.

Dans le prolongement de la tradition phrénologique, en particulier des travaux touchant à la science forensique⁸, le visage reste encore le modèle privilégié. Toutefois, la tendance actuelle tend vers l'élaboration de techniques permettant de reconnaître des individus à partir de signes périphériques, tels que d'autres traits physiologiques, des comportements dans l'espace ou des éléments vestimentaires. Le principe de la biométrie douce vise à définir de manière automatique les traits anatomiques qui rendent unique un être humain ou un objet, en s'inspirant des intuitions naturelles propres à tout processus de reconnaissance.

9 Selon la terminologie développée par Michel Callon et Bruno Latour, les faits sociologiques peuvent être saisis à travers les associations qui s'opèrent entre acteurs humains et non-humains. Un animal, un objet, une procédure ou un agencement sont autant de choses qui agissent activement dans la définition de la réalité. Parmi les nombreuses répercussions épistémologiques qu'il occasionne, ce principe d'équivalence influe sur la dualité entre nature et culture.

Dans le cadre de programmes de surveillance, ces technologies permettent déjà de produire automatiquement des données statistiques basées sur la couleur de la peau, la taille, l'âge ou le sexe. Même si elles ne permettent pas encore d'identifier expressément une personne, ces informations sont utiles pour observer des mouvements de foules ou d'autres formes d'actions de masse. Le but est ainsi de pouvoir repérer des acteurs, humains ou non-humains⁹, dans leur « environnement na-

Des entreprises comme Progeny développent des systèmes extrêmement performants destinés à des fins militaires ou commerciales. Surveillance, Persistent Observation, and Target Recognition (SPOTR™) est une solution développée par la firme Progeny qui vise à « détecter, traquer et identifier des cibles non coopératives » à partir d'un réseau de capteurs placés dans différents environnements. Les systèmes sont capables de reconnaître de manière toujours plus précise des objets ou des individus à partir des critères suivants : grandeur, âge, genre, ethnicité, couleur des vêtements, couleur de peau, couleur des cheveux, présence ou absence de pilosité faciale. SPOTR™ permet également de recréer automatiquement des visages en 3D et d'utiliser des caméras thermiques (source : www.spotrtech.com/).

turel»; et des bureaux ou un magasin seront bientôt capables de reconnaître toutes les personnes à peine le pas de porte franchi. Ces capacités de reconnaissance sont généralement évoquées comme des atouts pour améliorer le service à la clientèle¹⁰ ou offrir de nouveaux angles d'attaque aux départements des relations publiques ou de marketing. Les études actuelles dans le domaine projettent que des panneaux publicitaires munis de capteurs seront capables d'établir un profil des passants comprenant des informations quant aux goûts et aux achats récemment réalisés¹¹.

La communication faite autour de ces dispositifs se concentre encore, pour l'instant, sur des capteurs fixes. Toutefois, on comprend très vite quels sont les avantages de munir des UAS de systèmes tels

¹⁰ « En fin de compte, le but est d'identifier une personne en mouvement dans n'importe quelle situation », déclarait un dirigeant de CyberExtruder à propos de leurs recherches en biométrie douce. « Ne serait-il pas merveilleux d'entrer et de recevoir le service désiré sans n'avoir à prononcer un seul mot ? » (Hal Hodson, « «Soft» biometrics is the new way to monitor people », *New Scientist*, 28 décembre 2013).

¹¹ Sarah Freishtat, « Just a face in a crowd? Scans pick up ID, personal data », *The Washington Times*, 26 juillet 2013.

SPOTR™. A plus ou moins long terme, le fantasme de ces recherches est de créer des agents computationnels capables d'intuition. De telle sorte qu'ils puissent anticiper un *scénario* afin d'être toujours au bon endroit, au bon moment.

Après plus d'une dizaine d'années de recherche dans le domaine, Animetrics est devenu une des références en matière de reconnaissance faciale. En utilisant des images 2D provenant de sources diverses, ForensicGPS™ parvient à reconstituer des modélisations 3D très réalistes en une ou deux secondes (source: www.youtube.com/watch?v=hHp-FDfDQCw).

Dans le jargon militaire, ces stratégies sont regroupées dans la rubrique dite «Long Range, Non-cooperative, Biometric Tagging, Tracking and Location». De nombreux documents, accessibles sur internet, décrivent précisément les finalités *prédatrices* de tels projets. Voici par exemple un extrait d'un document précisant les objectifs de l'armée américaine dans ce domaine:

- «1) Biométrie de longue portée – la capacité de biométrie de longue portée sera fondée sur les techniques de reconnaissance faciale qui utilisent des algorithmes optimisés capables de fournir un pourcentage élevé d'identifications faciales à partir d'un capteur d'images de longue portée qui ne dispose, en retour, que d'informations réduites.
- 2) Algorithmes de données en réseau sporadiques – les algorithmes de données en réseau sporadiques seront capables de compléter des données, non reçues par le capteur d'images, en prolongeant les données reçues et en extrapolant les données réelles à partir de données simulées comme si elles avaient été transmises.
- 3) Algorithmes de lieux prédictifs – il s'agit à nouveau d'une technique algorithmique qui partira du «dernier lieu connu», de méthodes de comportement et/ou de marqueurs de lieux, et qui calculera l'espace au moment où la cible d'intérêt n'est pas acquise de sorte à prédire où la cible se situera probablement après la perte de sa trace à cause du mauvais temps, de l'obstruction de la cible (par exemple lorsqu'elle entre dans un immeuble ou une cave), ou de sa mise temporaire hors de portée du capteur d'images.»¹²

¹² «Long Range, Non-cooperative, Biometric Tagging, Tracking and Location», SBIR Source (dernière consultation le 3 avril 2014).

Dans les faits, ce type de projections est encore souvent relégué au statut de légende urbaine. En décembre 2013, une information selon laquelle la ville de Montréal se serait équipée de drones capables de «neutraliser des suspects» s'est révélée être un canular¹³. Cependant, la progression de ces technologies est tellement rapide et impérieuse qu'il ne fait aucun doute que ces types d'opérations dessinent l'horizon de ces prochaines années en matière de politiques sécuritaires.

¹³ Dominic Gover, *Montreal Armed Police Drones Story Exposed as Hoax*, 4 décembre 2013.

Faces hallucinées

Les diverses innovations dans le domaine, en particulier celle touchant à la reconnaissance faciale, continuent d'avoir bonne presse dans le contexte sécuritaire ambiant. Même si les résultats n'étaient pas véritablement probants, les discours postulant la nécessité de ces dispositifs ont été consolidés à la suite des attentats de Boston. Le CyLab

Images diffusées par le FBI montrant les frères Tsarnaev dans le public du marathon de Boston. La large diffusion des séquences les montrant a sensibilisé l'opinion publique sur l'actualité des recherches en matière de biométrie douce. Ceci malgré l'aveu du FBI que ces technologies n'avaient pas permis de reconnaître les suspects dont les visages étaient déjà enregistrés dans leur banque de données (source : ABC, 18 avril 2013).

Biometrics Center, affilié à la Carnegie Mellon University, a largement profité de cette plateforme pour influencer l'actualité et communiquer les besoins en matière d'identification biométrique. La particularité des attentats de Boston était notamment liée au fait que les clichés du « Suspect N° 2 » étaient de très basse qualité. Ils étaient par conséquent illisibles par les dispositifs de reconnaissance habituels. C'est précisément sur ce cas de figure que les experts en biométrie douce concentrent leurs recherches.

Obscurité, mouvement, longue distance, conditions climatiques, etc. : les images sont souvent loin d'être optimales. L'enjeu repose donc essentiellement sur cette aptitude à décoder le plus précisément possible des visages à partir d'images de mauvaise qualité. Les efforts se concentrent actuellement sur la construction de programmes susceptibles de déchiffrer ces données avec un minimum d'informations disponibles. Le logiciel utilisé pendant la traque des frères Tsarnaev fait partie de cette nouvelle génération de *robots* « entraînés » à identifier des

images de résolutions différentes. Il est déjà possible de recomposer un œil avec seulement 6 pixels, et il suffit d'une image de 50 pixels pour modéliser un portrait en 3D.

« Dans l'espoir de contribuer à appliquer la loi, l'équipe de Savvides a pris la photo du site web du FBI et l'a passée à travers une ancienne version d'un logiciel de retouche d'images. Le logiciel repose sur un système de reconnaissance automatique comprenant une base de données de 30 000 visages présentés à travers des résolutions multiples. Les algorithmes générés reposaient sur la mémoire du système et permettaient de reconstituer approximativement un visage à partir de modèles d'images faciales, avec pas plus de six pixels entre les yeux du suspect. Résultat de cette opération, le logiciel peut reconstituer dans l'essentiel un visage à partir de la relation entre les pixels et l'identification assistée humainement de repères faciaux, générant ce que Savvides désigne comme une « hallucination » du visage de l'individu à partir d'une quantité négligeable de données visuelles. »¹⁴

¹⁴ Sean Gallagher, « *Hallucinating* » a face, new software could have ID'd Boston bomber, 29 mai 2013.

Les attentats de Boston ont également permis de révéler les travaux réalisés dans le cadre de BOSS (Biometric Optical Surveillance System): un projet mené par Electronic Warfare Associates, et financé par des fonds publics, spécialisé dans le « crowd scanning », dont le but est de pouvoir isoler automatiquement des personnes suspectes dans une foule (source: FBI/Salon).

Selon les termes utilisés par Mario Savvides, le directeur du centre, il est ainsi possible de créer une «hallucination» de visage à partir d'une quantité négligeable de données. Dans le futur, le CyLab espère développer des méthodes biométriques encore plus poussées en créant une «hallucination» d'un visage entier à partir d'un profil de visage ou en se fondant uniquement sur les contours des yeux et des sourcils.

Même si les résultats n'ont pas été véritablement concluants dans le cas des attentats de Boston, la plupart des experts dans ce domaine sont convaincus que, dans peu de temps, tous les ordinateurs seront capables

Dans sa communication à propos de DeepFace en mars 2014, Facebook a utilisé le portrait de Sylvester Stallone afin de montrer les différentes étapes du processus. La compagnie présentait ses intentions dans une brève introduction, intitulée «DeepFace: Closing the Gap to Human-Level Performance in Face Verification»: « Dans la reconnaissance faciale moderne, la procédure conventionnelle s'articule en quatre étapes: détecter → ajuster → représenter → classifier. Nous reconfigurons la phase d'ajustement et la phase de représentation en utilisant des modelages en 3D du visage en vue de pratiquer une transformation fine d'un morceau, et de déduire une représentation de visage à partir d'un vaste réseau neuronal de neuf niveaux. Ce vaste réseau implique plus de 120 millions de paramètres en exploitant plusieurs niveaux

de relier n'importe quel portrait avec des sports pratiqués, des liens familiaux ou amicaux et toute une gamme d'informations plus ou moins personnelles¹⁵. Malgré leur aspect encore rudimentaire, ces modélisations pourraient rapidement fournir beaucoup plus d'informations que des empreintes digitales¹⁶.

Never say never

Le réel enjeu de ces recherches se situe dans l'accès aux banques de données, car l'efficacité de ces systèmes *auto-apprenant* dépend de la quantité

¹⁵ « Online photos can reveal our private data say experts », BBC (3 août 2011).

¹⁶ Le programme Janus, lancé en 2013 par l'Intelligence Advanced Research Projects Activity (IARPA), a constitué un signal fort de cette volonté de précision (voir www.iarpa.gov/index.php/research-programs/janus/baa).

connectés localement sans supporter leur poids, à la différence des niveaux à convolution habituels. Nous l'avons expérimenté sur la base de données faciales à ce jour la plus large, composée de 4 millions d'images faciales appartenant à plus de 4000 identités, où chacune comprend plus d'un millier d'exemplaires. Les représentations reconnues, associées avec précision à l'affiliation modélisée avec la base de données faciales, correspondent remarquablement bien avec les visages dans un environnement non contraint, même avec un simple système de classement. Notre méthode avoisine un taux de réussite de 97,25 % dans la base de données Labeled Faces in the Wild (LFW), réduisant la marge d'erreur de plus de 25 % par rapport à l'état courant de l'art, s'approchant de la performance humaine » (source : Facebook).

¹⁷ « Personal computing device control using face detection and recognition, United States Patent 860012 », décembre 2013 (dernière consultation le 1^{er} avril 2014).

d'images à disposition. Plus les barèmes d'évaluation sont vastes, plus ils parviennent à affiner les critères de comparaison et de sélection. Sans surprise, le perfectionnement de ces techniques biométriques est également devenu un des impératifs des titans de la Silicon Valley. Apple a notamment déposé une patente¹⁷ en décembre 2013 pour un dispositif de

Le réseau Domain Awareness System, une collaboration entre Microsoft et le NYPD [voir Joe Coscarelli, *The NYPD's Domain Awareness System Is Watching You*, 9 août 2012], ambitionne de superviser en temps réel les actes criminels dans le quartier financier de Lower Manhattan. Même si les technologies de reconnaissance faciale ne sont pas officiellement utilisées, il est d'ores et déjà possible de repérer et de traquer des objets ou des individus suspects en l'espace de quelques secondes. Ceci à partir d'informations aussi lacunaires que la couleur d'un t-shirt ou la forme d'un colis (source: NYT, 2012).

reconnaissance faciale destiné, notamment, à contrôler tout usage non désiré d'un appareil. Le dispositif est présenté avant tout sous des traits sécurisants. A savoir, autoriser ou refuser l'accès d'un iPhone ou d'un ordinateur en fonction du visage de l'utilisateur. Toutefois, il est évident que ces potentialités apportées par les systèmes de reconnaissance faciale ne se limiteront pas à cette simple fonction.

Les réseaux sociaux vont jouer un rôle particulièrement crucial. En effet, les nouvelles habitudes photographiques apparues ces dernières années, en particulier la généralisation des selfies, offrent un nombre toujours plus important d'angles de vue et d'expressions de visages humains. A ce titre, les récentes initiatives entreprises par Facebook, qui possède la plus grande archive photographique du monde, sont instructives. Après un premier essai peu concluant en 2011, la société se targuait en mars 2014 d'avoir résolu les principaux obstacles en matière d'identification des visages grâce à DeepFace. Cette technologie permet de comparer deux photographies de la même personne avec un taux de reconnaissance avoisinant 100 %. Même si ces firmes se défendent d'utiliser ces technologies à des fins sécuritaires, il subsiste des doutes réels quant à la manière dont ces informations seront traitées à l'avenir. D'ailleurs, Le PDG de Google, Eric Schmidt, entretient l'équivocité lorsqu'il évoque l'éventualité de permettre aux agents de la NYPD d'activer des systèmes de reconnaissance biométriques sur leurs Google Glasses : « Well, never say never, but we have said we wouldn't do it »¹⁸. Comme de nombreuses innovations et déclarations corrodant les libertés individuelles élémentaires, ces différentes prises de position passent pratiquement inaperçues. Sous couvert de lutte antiterroriste, maints projets indiquent déjà clairement dans quelle mesure gouvernements et entreprises privées vont être amenés à collaborer dans ce domaine. Il est décisif de rester attentif à l'impact occasionné par l'utilisation de ces diverses ressources dans les agendas politiques à venir.

De tels projets ne cessent de rendre poreuses les frontières à partir desquelles il est possible de circonscrire nos libertés dans l'espace public. Opérations commerciales ou programmes sécuritaires, le but n'est plus uniquement de recueillir des informations, ni même de surveiller. Selon un accord tacite, nous avons délégué aux machines le pouvoir de traiter la masse exponentielle d'informations produites. De plus en plus d'agents intelligents seront ainsi amenés à effectuer toute une gamme

¹⁸ « Bon, il ne faut jamais dire jamais, mais nous avons dit que nous ne le ferons pas. » (Jemima Kiss, *Worried about Your Privacy? Wait until the drones start stalking you*, 9 février 2014).

d'actions et d'analyses qui dépassent l'entendement humain. En grande partie grâce à l'indistinction des juridictions, des champs gigantesques ont été ouverts grâce à cette rencontre entre UAV, dispositifs de visualisation et banques de données.

Le but est explicitement de rendre fluide le passage de l'*aide* à la décision à la *prise* de décision. A terme, l'idée serait de construire des drones biométriques capables de se souvenir d'un visage et, en fonction de l'estimation des risques encourus, d'intervenir dans des contextes très divers. La question se concentre déjà sur le degré de fiabilité de ces machines de vision, afin d'en légitimer l'utilisation. Dans un rapport du Human Rights Council, Christof Heyns formulait une sévère mise en garde quant aux limites à apporter au développement des LARS :

« Ils érigent des critères d'une portée considérable pour protéger la vie en temps de guerre et de paix. Ceux-ci incluent la question de l'étendue avec laquelle ils peuvent être programmés pour répondre aux exigences de la loi humanitaire internationale et aux principes qui protègent la vie selon la loi internationale des droits humains. Ceci dit, leur déploiement peut être inacceptable car aucun système adéquat de responsabilité légale ne peut être conçu, car les robots ne devraient pas avoir le pouvoir de vie ou de mort sur des êtres humains. Le Rapporteur spécial recommande que les Etats établissent des moratoires nationaux sur ces aspects des LARS, et appellent à la mise en place d'un panel de haut niveau sur les LARS afin d'instituer une politique générale pour la communauté internationale à ce sujet. »¹⁹

La grande différence avec les nombreuses projections de la science-fiction²⁰ tient au fait qu'il ne s'agira pas d'avatars anthropomorphiques. Ces nouvelles espèces de « robots clairvoyants » prendront des formes essentiellement immatérielles et algorithmiques. Dans son essai sur *L'Humanité augmentée*, Eric Sadin s'interroge sur la nature de ces nouvelles entités :

« Comment nommer ces puissances brusquement surgies ? Sortes de créatures non pas dotées de conscience, mais d'une sorte de « vie autonome », appelées à déambuler sans fin au sein d'environnements artificiels, à « apprendre des décisions » en fonction des événements « vécus ». « Individus » s'apparentant à des entités organiques, humaines ou animales, à la nuance décisive près qu'ils ne revêtent aucun contour reconnaissable, ou encore moins localisable en quelque zone identifiée. »²¹

¹⁹ « Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns, United Nations » (dernière consultation le 2 avril 2014).

²⁰ Voir à ce propos l'article d'Alain Boillat, « Le héros hollywoodien dans les mailles de la télésurveillance et dans la ligne de mire du drone », dans le présent dossier.

²¹ Eric Sadin, *L'Humanité augmentée*, Paris, L'Echappée, 2014.

Les compétences quasi instinctives accordées à des automates, polymorphes et ubiquitaires, révèlent les propriétés prédatrices de la vision contemporaine.

Vision prédatrice alpha

Ces différentes remarques nous permettent de revenir aux frères Thomas. En effet, peu de temps avant *Hard Time on Planet Earth*, ils signaient leur premier succès avec leur scénario pour *Predator* (John McTiernan, 1987). Comme dans la série, ils exploitent les ressorts de la présence extra-terrestre, en créant un personnage doté d'armes inédites. Hormis le monstre lui-même – mutation improbable entre une araignée géante et une hyène à dreadlocks –, cette traque aliénante n'apporte rien de très original par rapport aux productions qui, sur une trame plus ou moins similaire, pullulaient durant cette période.

Toutefois, comme le personnage de *Control*, un aspect du film a durablement marqué les esprits. Il s'agit des scènes montrant, en mode

Predator (1987), de John McTiernan, suit un groupe paramilitaire, emmené par Arnold Schwarzenegger et Danny Glover, arpentant la jungle à la recherche d'un ministre kidnappé. Visuellement, le film repose largement sur l'effet graphique de la vision thermique (ou *thermovision*).

subjectif, la vision thermique de ce prédateur (encore) invisible. Saisis dans des faisceaux infrarouges, les membres de l'expédition se transforment en silhouettes polychroïques, errant dans une pénombre bleutée. Le spectre sonore de la bande-son, composée essentiellement de bourdonnements et des échos lointains de voix déformées, se déroule verticalement en bordure de l'image. Les plans s'enchaînent brusquement comme si la bête zappait d'un écran à l'autre ou, plus métaphoriquement, jouissait d'un don d'ubiquité.

Dans un crescendo nerveux, un viseur triangulaire se focalise sur le visage d'un soldat. Dans cette jungle méandreuse et étouffante, aucune présence ne semble pouvoir échapper à l'acuité perceptive du prédateur. En 1987, ces prises de vue réalisées à l'aide de caméras thermographiques étaient encore essentiellement cantonnées à des usages scientifiques et militaires. Près de quinze ans avant les visions nocturnes de la première invasion en Irak, ces rayonnements synthétiques permettaient de fantasmer le rôle capital des simulations informatiques dans les variations contemporaines du modèle panoptique. *Predator* dessinait l'horizon dystopique découlant du couplage entre drones et systèmes de reconnaissance.

Les drones constituent des avatars contemporains d'une volonté toujours plus poussée de perfectionner une vision verticale du monde. Google Earth (2005) et Google Streetview (2007) ont notamment largement participé à «naturaliser» des manières de voir jusqu'alors difficilement accessibles. Toutefois, même si elle tend quelquefois vers l'omniscience, la vision verticale repose sur l'hypothèse de l'existence d'un observateur qui, grâce à la généralisation de dispositifs techniques et rhétoriques à sa disposition, parvient à créer une gamme toujours plus fine de correspondances entre des réalités *a priori* dissociées. À l'instar des dispositifs panoptiques traditionnels, ces technologies stratégiques impliquent toujours la présence d'un observateur ou d'un opérateur tout-puissant. Cet impératif n'est plus envisageable à l'ère de la vision (*prédatrice*) *alpha*²². La furtivité des représentations, l'instantanéité des situations et la surabondance des données dépassent nos facultés cognitives. La vision (*prédatrice*) *alpha* est la vision stratégique du devenir-machine. Elle ne repose plus sur l'autorité de l'œil humain et il est toujours plus difficile de *faire face* à la perte des repères anthropomorphiques engendrée par cette accélération du présent. Comme le soulignait Gilles Deleuze

22 Une référence à la gamme de drones *Predator*, commercialisée par General Atomics Aeronautical Systems, Inc., et au prédateur *alpha* qui, dans le règne animal, n'est *a priori* plus la proie d'autres espèces lorsqu'il a atteint l'âge adulte.

« Il n'y a pas besoin de science-fiction pour concevoir un mécanisme de contrôle qui donne à chaque instant la position d'un élément en milieu ouvert, animal dans une réserve, homme dans une entreprise (collier électronique). [...] Ce qui compte n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle. » Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », 1990 (image : *Predator*).

dans sa contribution sur les sociétés de surveillance²³, il n'y a désormais plus besoin de science-fiction pour saisir cet actuel changement de paradigme. Désormais, plutôt que de parachever des idéaux d'intelligibilité dans notre rapport aux images, la vision verticale du drone désoriente les regards :

« Lorsqu'elle est retournée verticalement, la pyramide visuelle consolide une réalité photographique qui tend plutôt vers la métaphore et l'abstraction. L'aplanissement des perspectives découlant de cette prise d'altitude permet de créer une gamme infinie de correspondances entre des réalités a priori dissociées. »²⁴

Automatisée, dynamique et errante, la vision (prédatrice) alpha consacre le dépassement d'un modèle basé sur l'aptitude du génie humain à créer des correspondances à partir de signes visibles. Elle louvoie plutôt par balayages, combinant des masses monstrueuses de données prédictives. Grâce à sa puissance de calcul, la vision (prédatrice) alpha

²³ Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », *Pourparlers 1972-1990*, Paris, Les Editions de Minuit, 1990.

²⁴ Joël Vacheron, « Photographie et vision omnisciente », dans Nathalie Herschdorfer (éd.), *High Altitude*, Milan, Ed. 5 Continents, 2013, p. 105.

peut isoler, traquer et, potentiellement, neutraliser des individus, des choses ou des idées. Stratégique et tactique, clandestine et souveraine, elle inaugure le stade terminal des sociétés de contrôle.

La vision (prédatrice) alpha ne nécessite plus d'opérateurs *opérant*, car ce regard computationnel est le privilège exclusif d'espèces mutantes. Invisible et atomisé dans des magmas algorithmiques, le contrôle subsiste uniquement grâce aux récits favorisant une adhésion affective à l'autoritarisme ambiant. De la lutte antiterroriste aux reliquats du fantasme anthropomorphique, toute une gamme d'abstractions donne corps à des opérations qui ont déjà quitté le champ de la vision. Il est vain de tenter de regarder, d'interpréter ou d'identifier ce type de représentations. Elles ne constituent que des hallucinations qui se soustraient aux tournures du langage et aux postures habituellement mobilisées pour décrire ce que l'on voit. La vision (prédatrice) alpha est la prothèse ultime d'un réalisme capitaliste qui, à force de modulations, est parvenu à faire basculer la persistance des modèles humanistes dans l'instantanéité de modélisations «hallucinatoires».