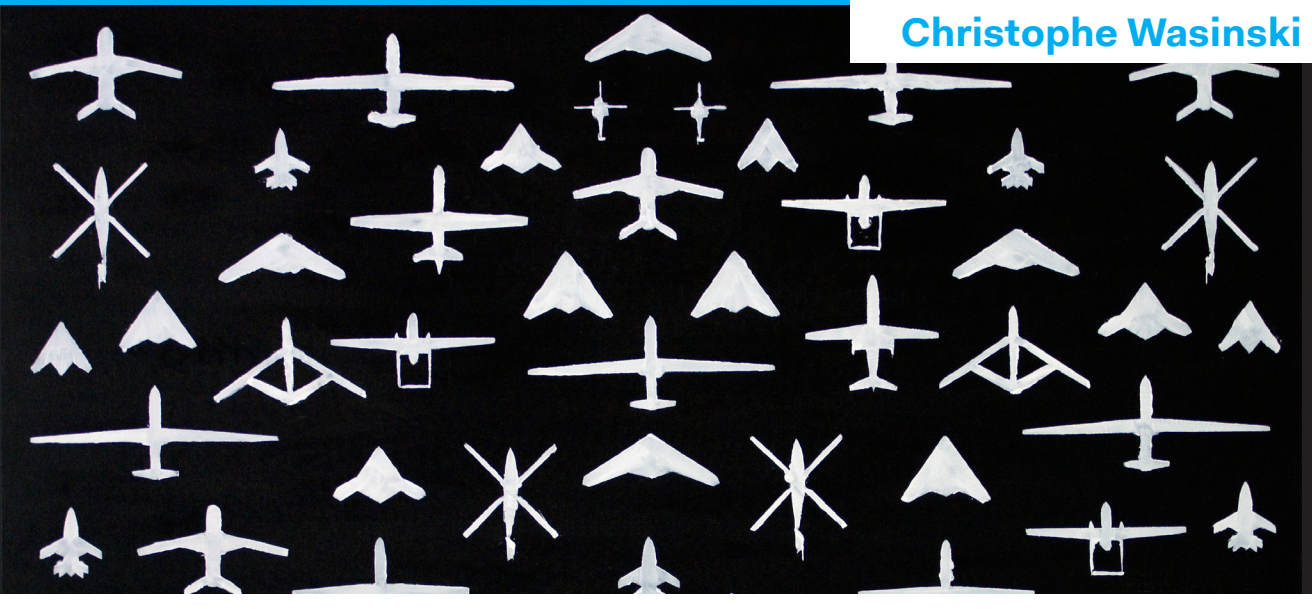
L'intelligence artificielle et le réenchantement de la défense de l'« Occident »

L'IMAGINAIRE « START-UP » DE LA GUERRE

Christophe Wasinski



GRIP

LES RAPPORTS DU GRIP 2025/3

Avenue des Arts 7-8
B-1210 Bruxelles
Tél : 0473 982 820
Courriel: admi@grip.org
Site Internet: www.grip.org
Twitter : @grip_org
Facebook : GRIP.1979

Photos de couverture : **Photo du haut :** Un drone est prêt à l'emploi lors du Blue UAS Refresh Challenge organisé par la Defense Innovation Unit, à Camp Wilson (Marine Corps Air Ground Combat Center), Twentynine Palms, Californie, le 4 novembre 2024.
Crédit : © U.S. Marine Corps / Lance Cpl. Richard PerezGarcia

Photo du bas : Drone Empire Decoration
Crédit : © John Johnston – Flickr.com

Prix : 10 euros

ISSN : 2466-6734
ISBN : 978-2-87291-251-3
ISBN : 978-2-87291-252-0 (version e-pub)

Version PDF: https://grip.org/limaginaire-start-up-de-la-guerre-lintelligence-artificielle-et-le-reenchantement-de-la-

Les Rapports du GRIP sont également diffusés sur www.i6doc.com, l'édition universitaire en ligne.

L'IMAGINAIRE « START-UP » DE LA GUERRE :

L'intelligence artificielle et le réenchantement de la défense de l'« Occident »

LES RAPPORTS DU GRIP 2025 / 3

TABLE DES MATIÈRES

LISTE DES ACRONYMES

AD/A2	*Anti-access/area-denial* / Déni d'accès et interdiction de zone
AUKUS	*Australia, United Kingdom and United States /* Australie, Royaume-Uni et États-Unis
AWCFT	*Algorithmic Warfare Cross-Functional Team* / Équipe interfonctionnelle de la guerre algorithmique
CCAC	Convention sur certaines armes classiques
CIA	*Central Intelligence Agency /* Agence centrale de renseignement
D3	*Dare to Defend Democracy*
DARPA	*Defense Advanced Research Projects Agency* / Agence pour les projets de recherche avancée de Défense
DASA	*Defense and Security Accelerator* / Accélérateur pour la défense et la sécurité
DCGS-A	*Distributed Common Ground System – Army* / Système de terrain commun distribué
DIANA	*Defence Innovation Accelerator for the North Atlantic* / Accélérateur d'innovation en matière de défense pour l'Atlantique nord
DIB	*Defense Innovation Board* / Comité d'innovation en matière de défense
DIUx	*Defense Innovation Unit Experimental* / Unité d'innovation de défense expérimentale
DS&T	*Directorate of Science and Technology* / Direction de la science et de la technologie
DSTL	*Defence Science and Technology Laboratory* / Laboratoire des sciences et technologie de Défense
FED	Fonds européen de la défense
IA	Intelligence artificielle
ICE	*U.S. Immigration and Customs Enforcement* / Services de contrôle de l'immigration et des douanes des États-Unis
ICRAC	*International Committee for Robot Arms Control*

JAIC	*Joint Artificial Intelligence Center* / Centre conjoint d'intelligence artificielle
JEDI	*Joint Enterprises Defense Infrastructure* / Infrastructure d'entreprises communes de défense
JSOC	*Joint Special Operation Command* / Commandement des opérations conjointes
JWCC	*Joint Warfighting Cloud Capability* / Capacité informatique de guerre interarmées
MDR	*Mission Data Repository* / Référentiel des données de la mission
MSS	*Maven Smart System* / Système intelligent Maven
NGA	*National Geospatial-Intelligence Agency* / Agence nationale de renseignements géospatiaux
NSA	*National Security Agency* / Agence nationale de la sécurité
NSCAI	*National Security Commission on Artificial Intelligence* / Commission nationale de sécurité sur l'intelligence artificielle
OTAN	Organisation du traité de l'Atlantique nord
RT-RG	*Real Time Regional Gateway* / Passerelle régionale en temps réel
SAIC	*Science Applications International Corporation*
SBICCT	*Small Business Investment Company Critical Technology initiative*
SSCI	*Select Intelligence Committee on Intelligence* / Comité spécial sur le renseignement du Sénat des États-Unis
UE	Union européenne
URSS	Union des républiques socialistes soviétiques
USDI	*Under Secretary of Defense for Intelligence and Security* / Sous-secrétaire à la Défense pour le renseignement et la sécurité

INTRODUCTION

Le 24 octobre 2024, la Maison-Blanche a rendu public un mémorandum concernant la politique de l'administration Biden en matière d'intelligence artificielle (IA) dans le champ de la sécurité[1]. Ce document précise que les États-Unis doivent devenir un leader dans ce domaine. Pour ce faire, il préconise un soutien du gouvernement à l'écosystème de l'IA. Le mémorandum souligne par ailleurs le fait que le développement de cette technologie doit se faire dans le respect des valeurs démocratiques. Selon le journaliste Gerrit de Vynck du *Washington Post* : « *Ce mémo* [était] *le dernier exemple en date des efforts déployés par l'administration Biden pour répondre aux inquiétudes concernant les inconvénients potentiels de l'IA, tout en encourageant le gouvernement à utiliser cette technologie et en permettant aux entreprises technologiques américaines de continuer à innover dans ce domaine*[2] ». L'arrivée à la Maison-Blanche de Donald Trump n'a pas remis en question ces objectifs. En janvier 2025, Pete Hegseth a été auditionné par le Comité des forces armées du Sénat des États-Unis *(Senate Armed Services Committee)* qui a confirmé sa nomination en tant que nouveau secrétaire à la Défense[3]. Lors de cette audition, il a notamment fait part de sa volonté de moderniser les infrastructures informatiques du Pentagone. Il a également évoqué la nécessité de développer l'IA afin, entre autres, de faire face à la Chine. Selon lui, en matière d'IA, le Département de la Défense se doit de prendre appui sur le secteur commercial étatsunien. Ceux et celles qui s'intéressent aux applications sécuritaires de l'IA ne seront pas surpris par ces déclarations. Depuis une vingtaine d'années, les États-Unis, ainsi que d'autres États, s'intéressent aux usages militaires de l'IA. Les évolutions récentes amènent même à penser que le développement de l'IA à des fins militaires s'est normalisé dans les discours sécuritaires ces dernières années.

Cette normalisation pose cependant de sérieux problèmes, comme l'ont constaté les experts des droits humains[4]. Ceux-ci attirent notamment l'attention sur les problèmes potentiels de biais algorithmiques et à propos de la dilution de la responsabilité humaine dans les décisions d'emploi de la force. De manière plus générale, ils pointent les risques de déshumanisation liés à l'usage de cette nouvelle technologie qui automatise l'exécution des actions létales. Il s'agit sans conteste de problèmes cruciaux. Les experts ne perdent cependant pas non plus de vue un problème moins spécifique, mais tout aussi important : le

[1] « Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence », *The White House*, 24 octobre 2024.

[2] DE VYNCK Gerrit, « White House orders Pentagon and intel agencies to increase use of AI », *Washington Post*, 24 octobre 2024.

[3] BRANDI Vincent, « Trump's defense secretary nominee pledges to prioritize AI investments », *DefenseScoop*, 14 janvier 2025.

[4] Nous nous appuyons ici sur l'argumentaire développé dans le cadre de la campagne « *Stop Killer Robots* » lancée en avril 2023 et soutenue par *Amnesty International* et *Human Rights Watch*. Voir : https://www.stopkillerrobots.org/.

fait que l'IA, même si elle n'a pas l'efficacité militaire vantée par l'industrie, puisse faire baisser le seuil d'acceptabilité du recours à la force et, par ce biais, s'avérer politiquement déstabilisante. À la lumière de ces éléments, les États auraient tout intérêt, par prudence, à s'entendre pour limiter au maximum la militarisation de l'IA. Dans les faits, pourtant, ils sont nombreux à encourager leurs forces armées à se doter d'équipements recourant à cette technologie. Les prédictions, parfois apocalyptiques, des experts paraissent même les pousser à investir dans ce domaine plutôt qu'à les inciter à mettre en œuvre des politiques de lutte contre la prolifération de l'IA militarisée[5].

Ce rapport explique pourquoi, en dépit des risques qui viennent d'être évoqués, l'IA fait l'objet d'un tel engouement dans le champ militaire. À cette fin, il expose le processus par lequel une multitude d'acteurs – services de renseignement, forces armées, grandes entreprises technologiques, fonds de capital-risque et décideurs politiques – ont conféré aux start-ups qui développent des applications militaires de l'IA un rôle toujours plus important depuis la fin de la Guerre froide. Dans une première partie, il expose le rôle joué par les services de renseignement, en particulier dans le cadre de la « *guerre contre le terrorisme* », dans ce processus. Toujours dans ce contexte, il se penche ensuite sur les rapprochements entre les start-ups et le Pentagone. Il souligne, dans cette partie, à quel point le Pentagone est devenu, de fait, un relai de l'industrie. Au surplus, il montre que l'IA est également conçue comme un moyen adapté aux conflits interétatiques. La troisième et dernière partie aborde la circulation transnationale de l'IA, un phénomène en grande partie influencé par les États-Unis. Sont entre autres évoqués dans celle-ci les usages de l'IA en Ukraine et en Palestine, et sa diffusion dans les armées alliées des États-Unis. Cette partie propose aussi une analyse des évolutions étatsuniennes récentes, dans laquelle nous montrons que les liens entre les entreprises et le Pentagone se sont encore resserrés depuis l'investiture de Donald Trump en 2025. De manière générale, ce rapport insiste sur les enjeux économiques qui sont à l'origine du développement de l'IA. Il met aussi en exergue le fait que ces enjeux économiques jouent un rôle déterminant dans la construction d'un imaginaire militariste qui contribue à la re-légitimation de la guerre au nom de la protection de l'« *Occident* ».

[5] PRÉVOST Thibault, *Les prophètes de l'IA. Pourquoi la Silicon Valley nous vend l'apocalypse*, Montréal, Lux, 2024.

1. « LA GUERRE CONTRE LE TERRORISME » COMME PLAN D'ÉMERGENCE

1.1. Anti-diplomatie et start-ups

Lors de la Guerre froide, l'Agence centrale de renseignement (*Central Intelligence Agency* - CIA) a participé au développement de programmes technologiques liés à la collecte de renseignements[6]. C'est dans le cadre de ceux-ci qu'ont notamment été conçus l'avion espion *Lockheed U-2* et des satellites d'observation, du matériel alors essentiellement élaboré pour espionner l'Union des républiques socialistes soviétiques (URSS). Avec le recul, il apparaît que ces technologies n'ont pas contribué à mettre un terme au conflit qui opposait les États-Unis à l'URSS. En définitive, c'est surtout la diplomatie classique, et sa capacité à instaurer un climat de confiance, qui a fait cesser le conflit qui opposait l'Est et l'Ouest et, *a fortiori*, a pacifié les relations internationales. *A contrario*, le matériel d'observation notamment développé par la CIA a contribué à aggraver les tensions entre les grandes puissances. On en voudra pour preuve la crise causée par la destruction d'un appareil *Lockheed U-2* qui survolait l'URSS en 1960. Les satellites, quant à eux, étaient intégrés dans le dispositif nucléaire qui a maintenu le monde au bord du gouffre pendant des décennies. Les programmes soutenus par la CIA ont en fait joué un rôle important dans la mise en place de ce que le chercheur James Der Derian nomme l'« *anti-diplomatie* », c'est-à-dire une vision complotiste et paranoïaque des rapports internationaux qui entretient des liens très forts avec les technologies de surveillance et le secret[7].

La CIA, pur produit de la Guerre froide, n'est pour autant pas dissoute après la chute de l'URSS. L'Agence voit certes sa dotation se réduire, mais elle conserve l'appareillage de surveillance qui fonde l'anti-diplomatie. Ses capacités d'interception de communications se sont même améliorées au cours des années 1990, à tel point que les analystes de l'Agence ont fini noyés sous les informations[8]. L'Agence ne remet cependant pas en cause la logique d'accumulation des informations. Ses membres regrettent plutôt le fait qu'elle ne dispose plus des ressources suffisantes pour impulser le développement d'outils permettant

[6] PRADOS John, *Histoire de la CIA*, Paris, Perrin, 2019, p. 534-535.

[7] DER DERIAN James, *Antidiplomacy. Spies, Terror, Speed, and War*, Cambridge, Blackwell, 1992. À propos des visions complotistes, voir : JAMESON Frédéric, *La totalité comme complot. Conspiration et paranoïa dans l'imaginaire contemporain*, Paris, Amsterdam, 2017.

[8] REINERT John T., « In-Q-Tel: The Central Intelligence Agency as Venture Capitalist », *Northwestern Journal of International Law & Business*, vol. 33, n°3, 2013, p. 686.

d'exploiter systématiquement les informations collectées[9]. La vision des élus politiques au fil des administrations qui se sont succédé durant cette période ne diffère guère de celle des membres de la communauté du renseignement. Ils s'inquiètent des faiblesses techniques de l'Agence et s'interrogent sur sa capacité à soutenir des opérations militaires, tel que cela est notamment attesté par les prises de position de 1998 du Comité spécial sur le renseignement du Sénat des États-Unis (*Senate Select Intelligence Committee on Intelligence* - SSCI). Comme le souligne John Prados : « *Le SSCI [avait] notamment critiqué l'incapacité persistante des systèmes de communication de l'agence et de l'armée à se connecter pour transmettre aux utilisateurs militaires des informations essentielles, telles que des photos prises par satellite*[10] ». Environ un an plus tard, lors de la guerre du Kosovo, les forces étatsuniennes détruisent par erreur l'ambassade de Chine à Belgrade. Le bombardement avait été planifié à partir d'informations communiquées aux militaires par la CIA. La destruction de l'ambassade provoquera la mort de trois personnes. Selon des thèses complotistes, circulant notamment en Chine, les États-Unis auraient délibérément visé le bâtiment. Les relations entre les États-Unis et la Chine s'enveniment suite à cet incident. Une fois de plus, l'infrastructure de l'anti-diplomatie était à l'origine d'une crise internationale[11].

Le rôle de la CIA et de ses technologies n'est cependant pas remis en question après cet incident. Au contraire, la question qui occupe, une fois encore, les espions est celle de savoir comment développer de nouvelles technologies alors que les financements restent, selon eux, trop limités. C'est dans ce contexte que Ruth David, à la tête de la Direction de la science et de la technologie (*Directorate of Science and Technology* - DS&T) de l'Agence, et son adjointe, Joanne Hisham, qui la remplacera ultérieurement en tant que responsable de la même direction, suggèrent au directeur George Tenet de faire appel aux entreprises de la Silicon Valley, en Californie. Des membres de la CIA s'entretiennent ensuite avec des techniciens et des représentants de l'industrie des nouvelles technologies afin de réfléchir à la manière de mettre à exécution la suggestion de Ruth David et de Joanne Hisham. À la suite de cela, la DS&T prend la décision de remplacer son bureau dédié à la recherche et au développement par un bureau qui se spécialise dans les investissements dans des programmes technologiques. Grâce à celui-ci, la CIA se met en position de faire appel à des prestataires extérieurs. Le dispositif évolue rapidement. En 1999, George Tenet, le PDG du géant de l'armement *Lockheed Martin*, Norman Augustine, et Lee A. Ault III fondent *Peleus*, une entreprise à but non-lucratif qui a pour mission de soutenir les sociétés qui élaborent des technologies potentiellement utiles aux services de renseignement[12]. Rapidement, *Peleus* est rebaptisée *In-Q-Tel* – la lettre « Q » est une référence à l'inventeur de gadgets

[9] *Ibid.*, p. 685.

[10] Traduction personnelle. PRADOS John, *Safe for Democracy. The Secret Wars of the CIA*, Chicago, Ivan R. Dee, 2006, p. 624.

[11] DER DERIAN James, *Virtuous War. Mapping the Military-Industrial-Entertainment Network*, New York, Routledge, 2009.

[12] GONZÁLES Roberto J., *War Virtually. The Quest to Automate Conflict, Militarized Data, and Predict the Future*, Oakland, University of California Press, 2022, p. 58. L'auteur indique que l'entreprise n'a pas de but lucratif mais que ses employés ont le droit de mener des activités qui génèrent des profits.

dans les films de James Bond – et devient un fonds de capital-risque ou, dans le jargon des affaires, un « *accélérateur de technologies* » (*« technology accelerator »*).

Avec *In-Q-Tel*, les responsables de la CIA espèrent pouvoir « *endiguer la fuite des cerveaux et répartir les ressources là où elle en a besoin*[13] ». Plus de 500 projets sont soutenus par ce fonds dont le premier directeur est Gilman Louie, un homme qui a travaillé pendant 20 ans dans le secteur des jeux vidéo[14]. *In-Q-Tel* investit notamment dans *Keyhole, Inc*., une entreprise qui développe un système de visualisation en trois dimensions de la Terre (*Earth Viewer*), lequel sera utilisé par les forces étatsuniennes lors de la guerre en Irak en 2003[15]. En 2004, *Keyhole* sera rachetée par *Google* qui la renommera *Google Earth*. Cet exemple ne constitue pas un cas isolé. *In-Q-Tel* financera aussi *Cleversafe*, une société spécialisée dans la « *gestion dispersée des données* » (« *cloud computing* ») qui sera reprise par l'*International Business Machines Corporation* (IBM). Elle financera par ailleurs *MindMeld*, une société qui a développé un système de reconnaissance vocal à l'origine de l'application *Siri* sur *Iphone*. *MindMeld* sera rachetée par *Cisco System*. *Samsung* et *Amazon* acquerront aussi des start-ups qui avaient été financées par *In-Q-Tel* pour développer des logiciels initialement destinés aux services de renseignement. *In-Q-Tel* soutient aussi des start-ups – tels que *Dataminr*, *Geofeedia*, *PathAR*, *Transvoyant* ou encore *Palantir Technologies* – spécialisées dans le développement de logiciels qui exploitent de grandes quantités de « *données accessibles sur les réseaux sociaux* » (« *data mining social media* »). En résumé, à travers *In-Q-Tel*, la CIA délègue le développement de l'infrastructure de l'anti-diplomatie à des start-ups[16]. Également, par l'entremise d'*In-Q-Tel*, l'Agence devient un acteur économique qui finance, avec de l'argent public, des entreprises du secteur privé. En définitive, la CIA a légitimé le rôle des start-ups dans le champ de la sécurité.

1.2. L'*homo contractus* au service de la NSA[17]

Le 11 septembre 2001, *Al Qaeda* frappe les États-Unis. L'attaque résulte, au moins en partie, de la guerre clandestine que les services de renseignement étatsuniens menaient contre le groupe depuis une dizaine d'années[18]. Poussée dans ses retranchements, l'organisation d'Oussama Ben Laden a donc joué la surenchère. S'en est suivie une battue effrénée pour mettre la main sur celui-ci. Peu nombreux sont cependant ceux et celles qui s'interrogent

[13] PRADOS John, *Histoire de la CIA, op. cit.,* p. 235.

[14] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *Costs of War*, Watson Institute, Brown University, 17 avril 2024, p. 12.

[15] *Ibid.*, p. 60-61.

[16] Ajoutons aussi que d'autres institutions s'inspirent de l'initiative de la CIA. C'est le cas de l'*US Army* qui crée *OnPoint Technologies* et de la NASA qui met sur pied *Red Planet Capital*. REINERT John T., « In-Q-Tel: The Central Intelligence Agency as Venture Capitalist », *loc. cit.*

[17] Nous devons le terme *« homo contractus »* à : SNOWDEN Edward, *Mémoires vives*, Paris, Seuil, 2019, p. 150-162.

[18] CLARKE Richard A., *Against All Enemies. Inside America's War on Terror*, New York, Free Pres, 2004 ; COLL Steve, *Ghost Wars. The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001*, New York, Penguin, 2004. Comme le montre par ailleurs Gilbert Achcar, la politique étrangère des Etats-Unis au Proche et Moyen-Orient a contribué à faire émerger l'organisation : ACHCAR Gilbert, *Le choc des barbaries*, Paris, 10/18, 2002.

sur les risques qui peuvent découler de l'adoption d'une stratégie principalement basée sur une chasse à l'homme musclée[19]. La radicalisation de la traque et le renforcement de sa dimension militaire, sont considérés comme devant aller de soi après les attentats du 11 septembre 2001. L'attitude des sécurocrates étasuniens repose en fait sur la conviction rétrospective que les attentats auraient pu être évités si davantage de moyens avaient été dédiés à la lutte contre le « *terrorisme* ». Cette croyance apporte de l'eau au moulin d'un fantasme sécuritaire ancien, celui qui veut que, pour comprendre les intentions de l'ennemi, il faut disposer d'une grande masse d'informations et d'outils techniques capables de « *connecter les points* » (« *connect the dots* ») entre les renseignements[20]. Ce type de fantasme, qui fait fi des principales causes politiques de la violence, relève en fait d'une épistémologie de l'ignorance[21]. Une ignorance qui s'avère néanmoins cruciale pour justifier de nouvelles dépenses pour le développement de moyens d'interception et d'analyse des données au sein de l'Agence nationale de la sécurité (*National Security Agency* - NSA).

Concrètement, les analystes de la NSA, comme ceux de la CIA, sont confrontés à un problème d'accumulation d'informations résultant de l'amélioration des capacités d'interception des communications avant les attentats[22]. Pour autant, il n'est nullement question de remettre en cause cette accumulation après le 11 septembre 2001. L'appareil de sécurité étatsunien, se raccrochant à l'idée qu'il faut « *connecter les points* », choisit la fuite en avant et se met en recherche de solutions technologiques. Pour être plus précis, la question du traitement de vastes quantités d'informations se manifeste surtout au sein de la NSA à travers le dossier des « *métadonnées* ». Le lanceur d'alerte Edward Snowden, qui a notamment travaillé en tant que contractant de *Booz Allen Hamilton* pour la NSA, a bien expliqué l'enjeu relatif à leur collecte et à leur analyse :

> « [Les métadonnées sont] *des informations qui ne sont pas dites ni écrites mais qui permettent néanmoins de révéler un contexte plus large et des modèles de comportements.* [Le] *préfixe "méta", traditionnellement traduit par "au-dessus" ou "au-delà", est ici utilisé dans le sens d'"à propos" : des données à propos d'autres données, un ensemble de marqueurs rendant ces données utiles. La façon la plus simple de se représenter les métadonnées est de les envisager comme des "données d'activité" c'est-à-dire l'enregistrement de toutes les choses que vous faites avec vos appareils et tout ce que ces derniers font d'eux-mêmes. Imaginons que vous téléphoniez à quelqu'un depuis votre portable. Les métadonnées peuvent alors inclure la date et*

[19] Sur cette notion, voir : CHAMAYOU Grégoire, *Les chasses à l'homme*, Paris, La Fabrique, 2010.

[20] CHAMAYOU Grégoire, « Dans la tête de la NSA. Une histoire philosophique du renseignement américain », *Revue du Crieur*, 2015, n°1, p. 20-39 ; HENN Steve, « In-Q-Tel: The CIA's Tax-Funed Player in Silicon Valley », *NPR*, 16 juillet 2012. L'idée selon laquelle les intentions de l'ennemi peuvent être devinées grâce au croisement d'un grand nombre d'informations se retrouve dans les discours sécuritaire coloniaux. Voir par exemple : DASH Mike, *Thug. La confrérie secrète des étrangleurs indiens*, Versailles, Omblage, 2017.

[21] DE SOUSA SANTOS Boaventura, « Colonialism and the Epistemology of Ignorance: A Lesson from Afghanistan », *Critical Legal Thinking*, 30 août 2021.

[22] LEFÉBURE Antoine, *L'affaire Snowden. Comment les Etats-Unis espionnent le monde*, Paris, La Découverte, 2014, p. 103 et p. 112 ; HARRIS Shane, *@War. The Rise of the Military-Internet Complex*, Boston, Mariner Books, 2015, p. 31. Voir aussi : CAMPBELL Duncan, *Surveillance électronique planétaire*, Paris, Allia, 2007.

> *l'heure de votre conversation, la durée de l'appel, le numéro de l'émetteur, celui du récepteur, et l'endroit où l'un et l'autre se trouvent*[23] ».

Michael V. Hayden, qui a dirigé la NSA entre 1999 et 2005, ajoute : « *Si l'on dispose de suffisamment de métadonnées, c'est-à-dire du mode d'utilisation d'un appareil de communication (qui a-t-il appelé, qui l'a appelé, quand, pendant combien de temps), on peut à peu près déterminer ce que fait le propriétaire de l'appareil*[24] ».

La collecte et l'analyse des métadonnées par la NSA vont jouer un rôle important, et polémique, dans la politique étatsunienne de lutte contre le « *terrorisme* ». Dans un premier temps, cette collecte se fait dans le cadre du programme *Stellarwind*. Celui-ci est utilisé pour contrôler des citoyens étatsuniens à travers l'interception de leurs courriels et s'assurer qu'ils ne sont pas potentiellement impliqués dans des activités « *terroristes* ». Considéré comme illicite, un terme sera mis à ce programme en 2004. Dans un second temps, l'Agence de renseignement prendra une place de premier plan dans la collecte des métadonnées destinées à localiser des personnes présumées « *terroristes* » en dehors des frontières étatsuniennes. Le rôle de la NSA en la matière était tout sauf anodin. Comme Antoine Lefébure le soulignait : « [La NSA] *fournit en effet 60 % des renseignements opérationnels (interceptions de messages et géolocalisation) qui alimentent une base de données créée en 2010, dite "Disposition Matrix"*[25] *»*. Cette banque de données listait les personnes suspectées de faire partie d'*Al Qaeda*. Elle était plus populairement connue sous le nom de « *kill list* » car les individus qui figuraient sur ladite liste risquaient d'être éliminés par des attaques de drones.

L'ampleur de l'ambition de la NSA transparaît à la lumière de la construction d'installations à Bluffdale, dans l'Utah – la patrie des Mormons, les spécialistes des données généalogiques. Celles-ci abritent un immense dépôt de données collectées : le Référentiel des données de la mission (*Mission Data Repository* - MDR). Selon Edward Snowden :

> « *Il était prévu que le MDR fasse environ 39 500 m² et soit rempli de serveurs. Il pouvait héberger une quantité phénoménale de données, en gros une sorte d'histoire en perpétuelle évolution des faits et gestes à l'échelle de la planète, dans la mesure où la vie peut être modélisée en connectant des paiements à des individus, des individus à des téléphones, des téléphones à des appels et des appels à des réseaux, le tout avec le tableau synoptique de l'activité d'Internet se déployant le long de ces lignes de réseaux*[26] ».

---

[23] SNOWDEN Edward, *Mémoires vives*, *op. cit.*, p. 237-238. Nous reviendrons sur les *« modèles de comportements* » plus loin.

[24] Italique dans l'original et traduction personnelle. HAYDEN Michael V., *Playing to the Edge. American Intelligence in the Age of Terror*, New York, Penguin, 2016, p. 30. Michael V. Hayden dirigea aussi la CIA entre 2006 et 2009.

[25] LEFÉBURE Antoine, *L'affaire Snowden, op. cit.*, p. 111.

[26] SNOWDEN Edward, *Mémoires vives, op. cit.*, p. 326. Certains commentateurs se sont demandés si l'ambition de l'Agence n'était pas de mettre en fiche la population mondiale. LEFÉBURE Antoine, *L'affaire Snowden, op. cit.*, p. 152.

Pour mettre en œuvre l'analyse des métadonnées, la NSA fait appel à des sociétés privées qui lui fournissent l'infrastructure et les logiciels. Parmi les sociétés qui bénéficient des projets de surveillance, on trouve notamment *Eagle Alliance*, *Booz Allen Hamilton* ainsi que *Palantir Technologies* et *Science Applications International Corporation* (SAIC[27]). Ces entreprises parviennent d'autant mieux à s'imposer dans le champ du renseignement que les agences étatiques sont critiquées pour n'avoir pas su anticiper les attaques du 11 septembre 2001[28]. À travers leur travail pour le compte de la NSA, ces sociétés participent aussi à la normalisation de l'idée selon laquelle la lutte contre le « *terrorisme* » doit se faire à travers des chasses à l'homme qui reposent sur l'exploitation de grandes quantités d'informations. Comme exposé plus loin, cette conception va beaucoup bénéficier aux start-ups. Pour cette raison, il faut considérer le recours aux contractants par la NSA dans le contexte de la « *guerre contre le terrorisme* » comme l'antichambre du développement de l'IA par les start-ups. Ajoutons que l'analyse des métadonnées ne contribue cependant guère à la compréhension des problèmes de violence politique au Proche et Moyen-Orient, problèmes qui restent essentiellement liés au maintien de régimes politiques autoritaires entre autres soutenus par les États-Unis et leurs alliés.

1.3. L'infrastructure de « l'œil qui ne scille pas »

En 2001, la CIA déploie des paramilitaires en Afghanistan. Ils y opèrent aux côtés de milices locales. Leur présence est à l'origine d'une rivalité bureaucratique entre l'Agence et le département de la Défense. En effet, le secrétaire à la Défense, Donald Rumsfeld, n'apprécie pas la présence des paramilitaires dans une guerre qu'il considère être de la responsabilité du Pentagone[29]. C'est notamment en réaction à cette rivalité que les militaires décident de faire évoluer le Commandement des opérations conjointes (*Joint Special Operation Command* - JSOC) afin de le transformer en une vaste machine à recueillir, analyser, diffuser des renseignements et les exploiter pour éliminer des personnes cataloguées comme « *terroristes*[30] ». L'ambition du commandement des opérations spéciales est de se transformer en un dispositif de surveillance permanente, de devenir un « *œil qui ne scille pas* » (« *unblinking eye*[31] »). Pour ce faire, le général Stanley McChrystal, à la tête du JSOC depuis 2003, coopte dans son équipe des opérateurs issus de la NSA et de la CIA[32]. Il recrute aussi le colonel Michael T. Flynn, qui deviendra ultérieurement directeur de l'Agence de renseignement de la Défense (*Defense Intelligence Agency)*. Dans le cadre

[27] *Ibid.*, p. 133.

[28] PRIEST Dana et ARKIN William M., *Top Secret America. The Rise of the New American Security State*, New York, Back Bay, 2011, p. 176, 189 et 194.

[29] MAZETTI Mark, *The Way of the Knife. The CIA, a Secret Army, and a War at the Ends of the Earth,* New York, 2013, p. 18-19.

[30] URBAN Mark, *Task Force Black. The Explosive True Story of the SAS and the Secret War in Iraq*, Londres, Abacus, 2010, p. 53.

[31] *Ibid.*, p. 85.

[32] MCCHRYSTAL Stanley, *My Share of the Task. A Memoir*, New York, Penguin, 2013, p. 117, p. 137-139, p. 149 et p. 155. Dans un premier temps, Stanley McChrystal s'appuyait sur des agents de liaison. 75 de ces agents travaillaient au sein de diverses bureaucraties à Washington et une centaine d'entre eux étaient déployés sur le terrain. PRIEST Dana et ARKIN William M., *Top Secret America, op. cit.*, p. 242.

de ses nouvelles fonctions au sein du JSOC, il est envoyé en mission à la station de la CIA de Bagdad pendant huit mois afin de se familiariser avec les techniques de l'Agence[33].

La mue du JSOC est rapide et radicale comme le soulignent les journalistes Dana Priest et William Arkin :

> « *Dès l'été 2005, le JSOC a mis en place ce que Michael Flynn a appelé "des opérations de capture, d'interrogation et d'exploitation à l'échelle industrielle". À Balad, en Afghanistan, les cabines d'interrogatoire étaient situées juste à l'angle des grandes salles où se trouvaient les spécialistes chargés d'extraire les clés USB, les ordinateurs, les téléphones portables, les documents et les traductions d'autres interrogatoires. Vingt personnes étaient responsables de recueillir et d'analyser les informations nécessaires pour interroger efficacement un seul détenu. Flynn insistait pour que le chef de l'équipe ayant mené l'assaut rejoigne l'équipe d'interrogation de chaque détenu qu'il capturait, afin que quelqu'un sachant précisément qui avait été trouvé dans quelle pièce de chaque maison et avec quelle preuve – téléphones portables, CD, etc. – puisse déterminer quel élément de preuve incriminant appartenait à qui*[34] ».

Le JSOC est ainsi devenu à la fois un service de renseignement et d'action. Pour le dire autrement, il s'est transformé en une CIA en miniature – dont les opérations secrètes sont cependant moins contrôlées par le Congrès que celles de l'Agence centrale de renseignement.

C'est par ailleurs dans le contexte du renforcement du JSOC qu'est popularisé le concept de « *modèle de vie* » (« *pattern-of-life*[35] »). Le général McChrystal indique qu'il émerge en mai-juin 2004 lors d'opérations de surveillance menées dans la région de Falloujah en Irak. Il écrit à ce propos : « *Nous avons commencé à développer ce que l'on a appelé les analyses du "modèle de vie", qui suivaient les habitudes des cibles dans leur routine quotidienne*[36] ». Ces analyses sont réalisées grâce aux images fournies par les drones *Predator* (« *Predator feeds* »). La connaissance du « *modèle* » (« *pattern* ») est utilisée pour prédire le comportement et choisir un moment pour l'attaque – un moment pendant lequel la cible est peu susceptible d'être physiquement proche de non-combattants. Mais l'analyse du modèle de vie sert aussi à cibler des individus dont le comportement diffère, par rapport à une série d'indicateurs, de celui du reste de la population. Pour le dire autrement, dans ce second cas de figure, l'analyse du modèle de vie est véritablement mise au service de la

[33] BERGEN Peter L., *Man Hunt: The Ten-Year Search for Bin Laden from 9/11 to Abbottabad*, New York, Broadway Paperback, 2012, p. 154.

[34] PRIEST Dana et ARKIN William M., *Top Secret America, op. cit.*, p. 248. Voir aussi : MCCHRYSTAL Stanley, *My Share of the Task, op. cit.*, p. 155 et p. 169.

[35] HARRIS Shane, *@War, op. cit.*, p. 35.

[36] MCCHRYSTAL Stanley, *My Share of the Task, op. cit.*, p. 138.

traque d'individus suspects[37]. Avec la notion de « *pattern-of-life* », les militaires élaborent en fait ce que le philosophe Grégoire Chamayou nomme une « *théorie de la proie*[38] ».

La mise en œuvre de cette théorie de la proie dans les guerres étatsuniennes en Afghanistan et en Irak nécessite une infrastructure. La gestion de celle-ci a notamment été prise en charge par l'entreprise de service spécialisée dans le secteur de la défense, et déjà citée, SAIC. Cette société est assez mal connue[39]. On sait néanmoins que ses employés étaient chargés de l'intégration de systèmes opérés par la NSA avant le début de la « *guerre contre le terrorisme* ». Lors de la guerre de 2003 contre l'Irak, la NSA fait appel à SAIC afin de développer un système qui fusionne « *les signaux numérisés de la NSA avec les images de la National Geospatial-Intelligence Agency (NGA) pour les commandants régionaux américains, qui utilisaient les "yeux et les oreilles" de la NSA et de la NGA afin de trouver des cibles pour les frappes de drones et les bombardements pendant les campagnes militaires*[40] ». SAIC conçoit aussi le prototype de la passerelle régionale en temps réel (*Real Time Regional Gateway* - RT-RG) pour le compte de la NSA[41]. Ce système est utilisé par les forces déployées en Irak au début de l'année 2007[42]. Il fusionne des informations très variées provenant aussi bien de sources ouvertes que d'interceptions de communications[43]. Le système ne repose pas sur une gestion et un stockage informatique centralisé mais sur un « *cloud distribué* ». Ceci permet aux informations d'être mises très rapidement à disposition des unités déployées dans la zone de combat.

Pour des raisons liées à la législation sur les conflits d'intérêt, SAIC ne peut cependant continuer à offrir certains services au gouvernement. La réglementation interdit, en effet, à une société d'engager en tant que contractants ses propres employés pour un programme dont elle assure la gestion[44]. De ce fait, SAIC se scinde en deux entités. La première, la plus réduite, conserve le nom SAIC et se spécialise dans les services techniques notamment à destination des autorités. La seconde prend le nom de *Leidos Holdings* et reprend à son compte 2 500 des 4 000 contrats de SAIC, parmi lesquels ceux qui concernent les activités avec la NSA et la NGA. Pour le dire autrement, *Leidos* développe des technologies pour les forces de sécurité tandis que les employés de SAIC les font fonctionner. En 2016, *Leidos* rejoint *Lockheed Martin*, ce qui montre l'intérêt que le géant de l'armement porte à ces activités. Notons aussi qu'un an auparavant, SAIC avait fait l'acquisition de *Scitor*, une société fondée en 1979 et qui fournissait des services au DS&T et au Bureau du service

---

[37] WOODS Chris, *Sudden Justice. America's Secret Drone Wars*, Londres, Hurst, 2014, p. 78. Au sein de la CIA, les attaques qui résultent d'une analyse du mode de vie sont nommées « *signature strikes* ».

[38] CHAMAYOU Grégoire, *Les chasses à l'homme*, *op. cit*., p. 8.

[39] À notre connaissance, aucun livre n'a jamais été publié sur SAIC.

[40] SHOROCK Tim, « A Major Defense Contractor Buys Its Way Back Into the Spying Business », *The Nation*, 11 mai 2015. Voir également : MCCHRYSTAL Stanley, *My Share of the Task, op. cit.*, p. 117.

[41] HARRIS Shane, *@War, op. cit.*, p. 33-36. La NGA est une agence qui dépend du département de la Défense.

[42] GONZÁLES Roberto J., *War Virtually. op. cit.*, p. 142 ; MOLTKE Henrik, « Mission creep : How the NSA's Targeting System for Iraq and Afghanistan Ended Up on the Mexico Border », *The Intercept*, 29 mai 2019. En 2005, la NSA avait testé un système de ce type, nommé CENTER ICE, en Afghanistan. La version expérimentale du RT-RG était nommée RT10.

[43] PRIEST Dana et ARKIN William M., *Top Secret America, op. cit.*, p. 242-243.

[44] « SAIC board approves services business spin-off », *Reuters*, 9 septembre 2013.

technique (*Office of Technical Services*) de la CIA. *Scitor* opérait pour le compte de l'Agence nationale de renseignements géospatiaux (*National Geospatial-Intelligence Agency* – NGA) des satellites qui collectaient des renseignements électroniques. En achetant *Scitor*, SAIC revient dans le champ du renseignement et s'introduit aussi dans celui des opérations militaires spéciales. Effectivement, depuis 2009, des analystes de *Scitor* travaillaient pour le compte de l'Équipe de conseil et d'assistance en matière de contre-insurrection (*Counterinsurgency Advisory and Assistance Team*) déployée en Afghanistan sous le commandement du général Stanley McChrystal, dans le cadre du renforcement du dispositif étatsuniens décidé par l'administration Obama[45]. Cette société contribuait donc, elle aussi, à faire fonctionner *« l'œil qui ne scille pas »*.

En 2010, une nouvelle étape est franchie au sein du monde militaire lorsque l'Agence pour les projets de recherche avancée de Défense (*Defense Advanced Research Projects Agency* - DARPA) inaugure *Nexus 7*[46]. Il s'agit d'un système d'analyse de grandes quantités de données (« *data mining* ») dont le nom est inspiré par celui d'un robot humanoïde dans le film *Blade Runner*[47]. *Nexus 7* est conçu pour aider les militaires à assurer la surveillance de la zone de combat. Il est aussi doté de la capacité de fusionner des informations provenant de sources diverses. Comme l'écrit un journaliste, il peut « *effectuer une corrélation croisée et une analyse automatisée d'ensembles de données massives et éparses – et recalculer les indicateurs de stabilité dans les minutes qui suivent la mise à jour de nouvelles données*[48] ». L'ambition des concepteurs de *Nexus 7* est de faire de celui-ci un système qui produit du « *renseignement culturel* » (*« cultural intelligence »*) permettant aux militaires de mieux comprendre les populations. La DARPA, qui désire investir plus directement le champ de bataille, déploie le système en Afghanistan. Il trouvera grâce aux yeux de David Kilculen, un lieutenant-colonel australien et docteur en science politique qui conseillera notamment les généraux étatsuniens David Petraeus et Stanley McChrystal en matière de contre-insurrection. David Kilculen s'intéressait alors aux données chiffrées – telles que le coût de certains produits de consommation – en tant qu'indicateurs pour évaluer l'attitude des populations. Il faut noter que David Kilcullen fondera une société de conseil, *Caerus Associates*, qui collaborera avec la DARPA[49]. *Nexus 7* n'a cependant pas fait l'unanimité au sein des forces armées. Les généraux Michael Flynn[50] et David Petraeus, par exemple, se sont montrés sceptiques quant à l'efficacité de ce programme[51].

Bien qu'il ne soit pas certain que *Nexus 7* ait eu un réel impact sur le déroulement des opérations en Afghanistan, son expérimentation prouve malgré tout l'intérêt des forces

---

[45] SHOROCK Tim, « A Major Defense Contractor Buys Its Way Back Into the Spying Business », *loc. cit.*

[46] SHACHTMAN Noah, « Exclusive: Inside Darpa's Secret Afghan Spy Machine », *Wired*, 21 juillet 2011. Voir aussi : GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 139.

[47] WEINBERGER Sharon, *The Imagineers of War. The Untold Story of DARPA, the Pentagon Agency that Changed the World*, New York, Vintage Books, 2017, p. 352-353.

[48] SHACHTMAN Noah, « Exclusive: Inside Darpa's Secret Afghan Spy Machine », *loc. cit.*

[49] Noah Shachtman indique que d'autres sociétés collaboraient avec la DARPA dans ce domaine, comme *Potomac Fusion* et *Data Tactics* Corporation. *Ibid.*

[50] Michael Flynn avait atteint le grade de lieutenant-général lorsqu'il fut déployé avec le général McChrystal en Afghanistan en 2009. Il était responsable du renseignement dans l'état-major de ce dernier.

[51] WEINBERGER Sharon, *The Imagineers of War, op. cit*., p. 354-355.

armées pour ce type de programme. Enfin, et de manière plus générale, l'histoire des systèmes RT-RG et *Nexus 7* atteste du fait que les forces armées étatsuniennes renouent avec de vieilles pratiques coloniales. Au 19e siècle déjà, en Inde, le Britannique William Sleeman avait développé une « *machine à détecter et détruire les bandes de thugs* » basée sur l'indexation d'informations et la constitution d'arbres généalogiques[52]. L'intranet du JSOC, mis en place avec l'assistance de sociétés privées, peut être considéré comme une version modernisée de cette machine. Au surplus, ces éléments montrent que les forces armées étatsuniennes, et plus uniquement les services de renseignement, commencent à jouer un rôle dans la constitution du marché pour les sociétés spécialisées dans le domaine de la collecte et l'analyse automatisée des données. C'est dans ce contexte que *Palantir Technologies* va parvenir à s'imposer.

[52] DASH Mike, *Thug. La confrérie secrète des étrangleurs indiens*, *op. cit.*, p. 241. Des programmes d'élimination, basés sur la collecte de renseignements notamment obtenus par le recours à la torture, furent également mis en œuvre par les forces armées françaises lors de la guerre d'Algérie et par la CIA lors de la guerre du Vietnam.

2. START-UPS ET « BIG TECH » À L'ASSAUT DU PENTAGONE

2.1. *Palantir Technologies* entre en scène

Entre 2005 et 2008, *In-Q-Tel* soutient entre autres une start-up spécialisée dans le développement de logiciels d'analyse de grandes quantités de données : *Palantir Technologies*[53]. Cette société, qui a adopté son nom en référence aux boules de cristal des récits de J.R.R. Tolkien, est basée à Denver dans le Colorado. Elle est dirigée par Alexander Karp, un philosophe qui a suivi les cours du théoricien allemand Jurgen Habermas à l'Université de Frankfort. Après avoir obtenu un doctorat, il utilise l'héritage de son grand-père pour investir dans des start-ups. Peter Thiel investit également dans *Palantir Technologies*. Thiel est un milliardaire qui a fait fortune en créant et revendant *PayPal* à *eBay* pour 1,5 milliard USD en 2002. Il a ensuite travaillé pour *Meta* en tant qu'employé et directeur. Il a notamment investi son argent dans les médias, les biotechnologies, *Spotify*, *Airbnb* ou encore *Postmates* (une filiale d'*Uber*). Alex Karp et Pieter Thiel sont deux hommes d'affaires controversés. Ils se sont notamment fait connaître pour leurs idées politiques libertariennes et nationalistes – les conceptions politiques de Peter Thiel, qui a vécu en Afrique du Sud, pourraient être influencées par celles qui prévalaient dans cet État à l'époque de l'apartheid[54]. Malgré leur réputation sulfureuse, la valeur de leur société ne cesse de croître. En 2013, elle était estimée entre 5 et 8 milliards USD. Au début de l'année 2020, 4 000 personnes travaillaient pour *Palantir Technologies* et sa valeur était estimée à 36 milliards USD[55]. Ceci découlait notamment de la diversification de sa clientèle. *Palantir Technologies* ne s'est, en effet, pas contentée de vendre ses produits aux services de renseignement. Elle a aussi collaboré avec le Service de contrôle de l'immigration et des douanes des États-Unis (*Immigration and Customs Enforcement* - ICE) lorsque l'institution,

[53] GREENBERG Andy, « How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut », *Forbes*, 14 août 2013. Andy Greenberg note que George Tenet, l'ancien directeur de la CIA, a été un des conseillers de *Palantir*. Remarquons aussi que, selon le journaliste Mark Bowden, le programme de surveillance de masse *Total Information Awareness*, développé sous l'égide de la DARPA au début des années 2000, était un précurseur des logiciels de *Palantir*. BOWDEN Mark, *Il faut tuer Ben Laden*, Paris, Grasset, 2014, p. 157-158.

[54] « Palantir: International Tech Despot », *Corporate Watch*, 22 mars 2024 ; MCGREAL Chris, « How the roots of the 'PayPal mafia' extend to apartheid South Africa », *The Guardian*, 27 janvier 2025.

[55] GRANATO Andrew, « How Pieter Thiel and the Stanford Review Built a Silicon Valley Empire », *Stanford Politics*, 27 novembre 2017 ; GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 15.

après l'arrivée de Donald Trump à la Maison-Blanche en 2016, était chargée de séparer les familles des migrants[56].

Au début des années 2010, l'intérêt des militaires pour les logiciels capables de traiter de grandes quantités d'informations se confirme, ce qui va bénéficier à *Palantir Technologies*. Initialement, le Pentagone finance la création d'un « *système de masse commune distribuée* » (« *Distributed Common Ground System – Army »* dit DCGS-A) par *Lockheed Martin*, *Raytheon* et IBM afin de doter ses unités d'un système de visualisation du champ de bataille[57]. Le lieutenant-général Michael Flynn, ainsi que de nombreux soldats, n'était pas satisfait par celui-ci[58]. Il obtient alors qu'en lieu et place, le Pentagone fasse appel à *Palantir Technologies* pour fournir un autre système. Ceci contribue à faire naître une aura d'efficacité autour des programmes de *Palantir.* Comme l'écrivait le journaliste Andy Greenberg : « Palantir *transforme les marécages d'informations en cartes, histogrammes et diagrammes de liens à visualisation intuitive. Donnez à ses "ingénieurs déployés à l'avance" quelques jours pour explorer, étiqueter et intégrer chaque parcelle des données d'un client, et Palantir peut élucider des problèmes aussi disparates que le terrorisme, la réponse aux catastrophes et le trafic d'êtres humains*[59] ». Le logiciel de *Palantir Technologies* ne fait pourtant pas l'unanimité parmi les soldats. En 2016, l'*US Army* décide d'ailleurs de ne pas tenir compte d'une offre de *Palantir Technologies* pour un système de traitement de l'information (*« data-processing »*). L'entreprise décide alors de déposer plainte. La justice donne gain de cause à *Palantir*, ce qui renforcera sa position vis-à-vis du Pentagone[60].

En juin 2021, le magazine *Wired* publie un reportage d'Annie Jacobsen à propos du rôle joué par les produits de la société en Afghanistan[61]. Il expose certains des problèmes relatifs à leur emploi en 2012. Dans son article, la journaliste fait remarquer que les capteurs déployés par les militaires produisaient de grandes quantités d'informations, notamment sous forme de films. La quantité était telle que les militaires n'étaient pas capables de les exploiter. De ce fait, les forces armées ont décidé d'automatiser la tâche d'analyse des images en faisant appel aux produits de *Palantir*. Le logiciel de la société pouvait « *extraire et agréger des données sur des personnes individuelles* » à partir d'une surveillance de masse[62]. Des individus, par exemple suspectés de poser des bombes le long des routes où patrouillaient les soldats étatsuniens, pouvaient donc être surveillés et suivis par des caméras montées sur des plateformes aériennes et les images analysées par le logiciel de *Palantir*. Comme la machine conservait toutes les données, le système pouvait établir des connexions et faire des analyses des « *modèles de vie* ». Sur base de cette analyse, le

[56] HASKINS Caroline, « 'I'm the new Oppenheimer!': my soul-destroying day at Palantir's first-ever AI warfare conference », *The Guardian*, 17 mai 2024.

[57] SHACHTMAN Noah, « Spy Chief Called Silicon Valley Stooge in Army Softwar Civil War », *Wired*, 1er août 2012.

[58] Micheal T. Flynn sera également, pendant 22 jours, le conseiller national à la sécurité de Donald Trump.

[59] GREENBERG Andy, « How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut », *loc. cit.*

[60] KLARE Michael T., « Competition for Defense Contract May Drive Divides Within Trump Circle », *Truthout*, 10 février 2025.

[61] JACOBSEN Annie, « Palantir's God's-Eye View of Afghanistan », *Wired*, 20 juin 2021.

[62] *Ibid*.

système faisait des prédictions concernant les lieux où les personnes surveillées pouvaient potentiellement se rendre. Les militaires pouvaient alors décider d'éliminer une personne, en commanditant une frappe aérienne, sur base des informations rassemblées par les capteurs et triées par le logiciel. L'article d'Annie Jacobsen montre cependant que le système n'était pas infaillible et pouvait recommander de cibler des innocents. Il pointe aussi le fait qu'il n'existait, semble-t-il, aucune procédure pour faire retirer de la banque de données du logiciel les noms de personnes erronément suspectées d'être des « *terroristes* ». Cet article permet de mieux comprendre les réticences des militaires évoquées ci-dessus.

Le 2 mai 2011, Oussama Ben Laden est tué par un commando du JSOC. Dans le livre qu'il a consacré à cette affaire, le célèbre journaliste Mark Bowden aborde notamment la question de l'analyse de grandes quantités de données. Il écrit ainsi :

> « *Commencez par des milliers de données. Des noms, des tas de noms. Des localisations. Des rumeurs. Des comptes rendus d'interrogatoires. Des numéros de téléphone. Des appels enregistrés. Des dates. Des adresses. Des coordonnées géographiques. Des photos aériennes. Des clichés de surveillance au sol. Des vidéos. Des signalements. Des empreintes digitales. De vieux journaux intimes. Des e-mails. Des sites Web. Réseaux sociaux. SMS. Tweets. Missives traditionnelles. Blogs. Bulletins d'informations. Émissions de radio. Factures. Échéanciers. Contredanses. Quittances. Quittances de loyer. Numéros de cartes de crédit. Des comptes en banque. Dépôts. Retraits. Transferts. Numéros de plaques d'immatriculation. Des passeports. Rapports de police. Arrestations. Itinéraires de voyage… Autant d'informations potentiellement exploitables. Lorsqu'on recherche une personne parmi sept milliards d'individus, surtout si cette personne ne souhaite pas qu'on la trouve, il faut ratisser large*[63] ».

Ce type de récit célèbre le rôle de l'analyse de grandes quantités de données dédiée à des chasses à l'homme. Il renforce l'idée selon laquelle la sécurité repose sur la capacité de « *connecter des points* ». Bien que rien ne prouve que les produits de *Palantir* aient réellement joué un rôle dans l'élimination d'Oussama Ben Laden, la société profite de la circulation du fantasme qui veut qu'en « *connectant les points* » on peut assurer la sécurité[64].

Comme on le sait aujourd'hui, l'exécution d'Oussama Ben Laden n'a pas mis un terme à la « *guerre contre le terrorisme* ». Le JSOC a donc continué à traquer et à éliminer des insurgés grâce, notamment, à des moyens électroniques toujours plus sophistiqués, dont ceux de

[63] BOWDEN Mark, *Il faut tuer Ben Laden, op. cit.*, p. 151. Pour rappel, Mark Bowden s'est rendu célèbre en publiant *Black Hawk Down*, ouvrage dont a été tiré le film éponyme. BOWDEN Mark, *Black Hawk Down*, Londres, Corgi, 2000.

[64] COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *Harper's Magazine*, mars 2024. Notons que Mark Bowden évoque une fois la société *Palantir* dans son ouvrage. BOWDEN Mark, *Il faut tuer Ben Laden, op. cit.*, p. 159.

Palantir Technologies[65]. Avec l'utilisation de ces moyens, les militaires sont devenus, pour reprendre l'expression du général Stanley McChrystal, des « *entrepreneurs de la bataille*[66] ». L'efficacité accrue de ces « *entrepreneurs* » s'est cependant accompagnée d'un durcissement du « *terrorisme* », comme l'ont montré les actions de l'État islamique. L'expertise sophistiquée et coûteuse, s'appuyant sur des moyens électroniques, n'a finalement pas tenu ses promesses. La « *chaîne de frappe* » (« *kill chain* ») des forces étatsuniennes est devenue une chaîne sans fin et la traque menée avec ces mêmes moyens technologiques a provoqué, de manière directe ou indirecte la mort de nombreux civils dans cette guerre de plus en plus brutale[67]. Les exécutions résultant de la *« connexion des points* » n'ont, en définitive, pas permis d'assurer la sécurité en Afghanistan et en Irak.

2.2. Le projet *Maven* et l'invention (controversée) du futur

Le 20 mai 2017, une « *équipe interfonctionnelle de la guerre algorithmique* » (« *Algorithmic Warfare Cross-Functional Team »* – AWCFT) est mise sur pied au sein du Pentagone à la demande du sous-secrétaire à la Défense pour le renseignement et la sécurité (*Under Secretary of Defense for Intelligence and Security* – USDI), Robert Work[68]. C'est cette équipe qui sera à l'origine du programme de renseignement et de ciblage *Maven*. Ce système, qui est pensé comme une expérimentation, profitera lui aussi aux industries, notamment à *Palantir Technologies*. Sa conception fera cependant l'objet de contestations par certains employés de l'industrie.

Le développement du système *Maven* procède, une fois encore, de la constatation que les forces armées disposent d'une quantité grandissante d'informations qu'elles sont dans l'impossibilité d'exploiter. En effet, en 2011, les drones déployés génèrent 327 000 heures de films de surveillance, soit l'équivalent de 37 années. En 2017, les engins du seul commandement central (*Central Command*) produisent l'équivalent de 325 000 films commerciaux (à peu près 700 000 heures ou 80 années de vidéo). Les responsables du Pentagone sont convaincus que ces films contiennent des informations utiles pour localiser les combattants de l'État islamique en Irak et en Syrie[69]. C'est pour cette raison qu'est formé un « *groupe de travail sur l'automatisation* » (« *Automation Working Group* ») au sein de l'USDI en 2016. La décision est prise par ce dernier de faire appel aux sociétés de la Silicon Valley pour les aider à solutionner le problème du traitement des données. Des interactions

[65] WARRICK Joby, *Sous le drapeau noir. Enquête sur Daesh*, Paris, Cherche-Midi, 2016, p. 314.

[66] MCCHRYSTAL Stanley, *My Share of the Task, op. cit.*, p. 146 et p. 155.

[67] Sur la notion de « *chaîne sans fin* », voir : PAGÈS Yves, *Les chaînes sans fin. Histoire illustrée du tapis roulant*, Paris, La Découverte, 2023. Au surplus, Edward Snowden, Chelsea Manning et Julian Assange qui ont dénoncé les effets de la *« kill chain »* ont été poursuivis par les autorités étatsuniennes. SNOWDEN Edward, *Mémoires vives, op. cit.* ; MANNING Chelsea, *README.txt*, Paris, Fayard, 2022 ; MELZER Nils, *L'affaire Assange. Histoire d'une persécution politique*, Paris, Editions Critiques, 2022.

[68] SHULTZ Richard H. et CLARKE Richard D., « Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare », *Modern War Institute*, 25 août 2020.

[69] GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 7.

entre les civils et les militaires émergera *Maven*, un système qui fusionne des données et emploie des algorithmes afin de surveiller le champ de bataille et identifier des cibles[70].

Les membres du *Central Command* sont cependant déçus par ce programme. Selon Richard H. Shultz et Richard D. Clarke : « *Bien que l'IA pouvait placer un cadre autour des véhicules, des bâtiments et des personnes et les afficher sur la carte, les algorithmes étaient rudimentaires et comportaient de nombreuses fausses détections*[71] ». Les deux experts indiquent que, dans sa phase initiale, le taux de précision des détections se situait aux alentours des 50 % et que le système ne parvenait pas toujours à distinguer les hommes des femmes et des enfants. Ce système trouve donc aussi son point de départ dans la « *guerre contre le terrorisme* ». Son développement se poursuivra cependant en dehors de ce contexte, de manière à ce qu'il puisse être déployé dans d'autres types de conflits, tels que les conflits classiques[72].

Le projet *Maven* a en fait été conçu comme une « *démonstration de faisabilité* » (« *proof-of-concept* ») en matière d'usage de l''IA dans le domaine militaire aux États-Unis[73]. En novembre 2017, le directeur du Centre conjoint d'intelligence artificielle (*Joint Artificial Intelligence Center* - JAIC), le lieutenant-général John N.T. Shanahan, explicitera cette idée lorsqu'il affirmera que : « *Maven est conçu pour être ce projet pilote, cet éclaireur, cette étincelle qui allume le front de flamme de l'intelligence artificielle dans le reste du département [de la Défense]*[74] ». Il faut donc appréhender *Maven* en tant qu'étape dans la formation d'un horizon d'attente dans le domaine de l'IA à des fins militaires[75]. Il est d'ailleurs question d'augmenter le nombre d'utilisateurs du programme au sein des forces armées[76].

Pour élaborer *Maven*, le Pentagone a fait appel à des grandes et de petites entreprises technologiques (*tech firms*), notamment *Amazon*, *Booz Allen Hamilton*, *Clarifai*, *Cubic Corporation*, *Crowdflower*, *DigitalGlobe, ECS Federal*, *Google, Microsoft* et *Rebellion Defense*[77]. Les employés de *CrowdFlower* – qui se nomme maintenant *Figure Eight* – sont les « *petites mains* » de *Maven*. Ils visualisent des centaines de milliers d'images afin

[70] Déclaration officielle de la *Kentucky National Guard* citée par : HARPER John, « Palantir lands $480M Army contract for Maven artificial intelligence tech », *DefenScoop*, 29 mai 2024.

[71] SHULTZ Richard H. et CLARKE Richard D., « Big Data at War », *loc. cit*.

[72] KAHN Lauren A., « Risky Incrementalism. Defense AI in the United States », *DAIO Study,* 23/07, 2023, p. 23.

[73] MAASE Lucas et VERLAAN Stephanie, « Big Tech Goes to War. Uncovering the Growing Role of US and European Technology Firms in the Military-Industrial Complex », *Rosa Luxemburg Stiftung*, 5/2022, p. 23.

[74] ALLEN Gregory C., « Project Maven brings AI to the fight against ISIS », *Bulletin of the Atomic Scientists*, 21 décembre 2017.

[75] KOSELLECK Reinhart, « Champ d'expériences et horizon d'attente : deux catégories historiques », dans *Le Futur Passé. Contribution à la sémantique des temps historiques*, Paris, Éditions de l'EHESS, 1990, p. 307-329.

[76] FREEDBERG Sydney J., « 'Success begets challenges': NGA struggles to meet rising demand for Maven AI », *Breaking Defense*, 3 septembre 2024.

[77] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 5.

« *d'enseigner* » à la machine comment reconnaitre des objets[78]. La société *Google*, quant à elle, fournit au Pentagone un logiciel d'IA nommé *TensorFlow* dans le cadre du projet *Maven*[79]. Des employés de la société protestent cependant contre l'implication de leur société en soutien à un programme d'armement[80]. D'après des courriels officiels ayant fuité, *Google* avait exigé que sa participation à *Maven* ne soit pas révélée sans son autorisation. La société avait aussi considéré qu'il fallait « *à tout prix* » éviter que son nom ne soit publiquement associé à l'emploi de l'IA à des fins militaires[81]. En 2019, la direction de *Google* décide de ne pas prolonger le contrat qui la lie avec le Pentagone dans le cadre du projet *Maven*. D'autres sociétés – *Amazon Web Services*, *Microsoft* et *Palantir Technologies* – prennent alors le relai de *Google*.

Le coût du développement initial du projet *Maven* aurait été de 70 millions USD[82]. En 2020, on estimait qu'il était financé annuellement à hauteur de 250 millions USD[83]. En 2024, *Palantir* obtient un contrat de 480 millions USD pour travailler sur un prototype nommé *Maven Smart System* (MSS[84]). Remarquons cependant que, pour pouvoir être exploité sur le champ de bataille, *Maven* nécessite que les militaires soient connectés à un « *cloud* ». Dans ce contexte, le Pentagone lance un appel pour développer une infrastructure d'entreprises communes de défense (*Joint Enterprises Defense Infrastructure* – JEDI [85]). Les militaires décident de demander à *Amazon Web Services* d'assurer ce service pendant dix ans à travers un contrat d'une valeur de 10 milliards USD. L'entreprise *Oracle*, considérant qu'*Amazon* a été favorisé, dépose plainte auprès de la justice. Le Pentagone est finalement contraint de mettre un terme à ce programme en juillet 2021. Il le relance ensuite sous le nom de capacité informatique de guerre interarmées (*Joint Warfighting Cloud Capability* - JWCC). *Google*, *Oracle*, *Amazon Web Services* et *Microsoft* sont sélectionnés dans le cadre de ce second appel dont la valeur totale est de 9 milliards USD. Le développement de l'IA est une véritable aubaine pour ces sociétés qui deviennent d'importants clients du Pentagone[86]. Comme on le constate, les protestations de certains employés de *Google* ne sont pas parvenues à faire changer la politique de l'entreprise. En définitive, le projet *Maven* a contribué à donner forme au futur, un futur qui s'avère très profitable pour l'industrie

2.3. Le Pentagone : un relai de l'industrie

À partir de 2014, le Pentagone commence à mettre sur pieds un écosystème bureaucratique pour soutenir le développement de l'IA. Cette mise en place s'est par ailleurs accompagnée

[78] GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 63.

[79] MAASE Lucas et VERLAAN Stephanie, « Big tech goes to war », *loc. cit.,* p. 12-13.

[80] GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 64-65.

[81] COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *loc. cit.*

[82] GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 62.

[83] MAASE Lucas et VERLAAN Stephanie, « Big tech goes to war », *loc. cit.,* p. 12.

[84] « Pentagon awards $480 million deal to Palantir for 'Maven' prototype », *Reuters*, 30 mai 2024.

[85] MAASE Lucas et VERLAAN Stephanie, « Big tech goes to war », *loc. cit.,* p. 5 et p. 14.

[86] COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *loc. cit*

de la formation d'un discours institutionnel sur cette technologie – dont les principaux éléments sont aussi ressassés par des experts issus des think tanks[87]. C'est en effet en 2014 que le secrétaire à la Défense, Chuck Hagel, annonce le lancement de l'Initiative d'innovation de la Défense (*Defense Innovation Initiative*). Il décrit celle-ci comme « *un effort ambitieux à l'échelle du Département pour identifier et investir dans des manières innovantes de pérenniser et faire progresser la suprématie militaire américaine au 21e siècle*[88] ». L'initiative est supervisée par Robert O. Work, un ancien Marine qui avait été nommé sous-secrétaire à la Marine (*US Navy*) par Barack Obama en 2009, avant de devenir secrétaire adjoint à la Défense en 2014. Dans un discours datant de 2016, il relie la nécessité de développer l'IA à la *Third Offset Strategy*, une réflexion débutée en 2014 sur les moyens de faire face à des concurrents internationaux, en particulier la Chine et la Russie[89]. Dans son exposé, il redéfinit la raison d'être de l'IA au service des forces armées ; il conçoit son usage dans le contexte de rivalités entre des puissances, et plus uniquement pour affronter des groupes qualifiés de terroristes. Le successeur de Chuck Hagel, Ashton Carter, poursuit la politique adoptée par son prédécesseur. En 2015, dans le cadre de la *Defense Innovation Iniative*, il inaugure l'Unité d'innovation de défense expérimentale (*Defense Innovation Unit Experimental* - DIUx) – le terme « *experimental* » sera ultérieurement abandonné. Cette unité s'installe à Mount View, en Californie, à proximité de *Googleplex*, le siège de la société *Google* – il est à noter que les géants de l'armement *Lockheed Martin* et *Northrop Grumman* ont également des bureaux à quelques kilomètres de là[90]. La DIUx est en fait un « *accélérateur de start-ups* » (« *startup accelerator* ») qui s'inspire de *In-Q-Tel*[91]. Un autre accélérateur de start-ups, *MD5*, qui sera ensuite renommé le Réseau national d'innovation en matière de sécurité (*National Security Innovation Network*), est également mis sur pied et intégré dans la *Defense Innovation Unit* en 2016[92]. Son objectif est de soutenir l'innovation technologique, notamment en finançant des activités menées dans des universités.

C'est également en 2016 que le Comité d'innovation en matière de défense (*Defense Innovation Board* - DIB) voit le jour. Il s'agit d'un groupe de réflexion composé de civils. Le président du DIB, qui est nommé par Ashton Carter, est Eric Schmidt. Il a été PDG de *Google* entre 2001 et 2011. Parmi les membres du groupe, on trouve aussi des cadres et anciens

---

[87] Sur les discours des think tanks, notamment ceux du *Center for a New American Century* (CNAS) et du *Center for Strategic and International Studies* (CSIS), voir : GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit*., p. 8 et p. 22; MAASE Lucas et VERLAAN Stephanie, « Big tech goes to war », *loc. cit.,* p. 14.

[88] PELLERIN Cheryl, « Hagel Announces New Defense Innovation, Reform Efforts », *DOD News*, 15 novembre 2014.

[89] PELLERIN Cheryl, « Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence », *DOD News*, 31 octobre 2016. Robert Work indiquait dans son discours qu'il avait commencé à penser à la *Third Offset* en 2012 lorsque Ash Carter était secrétaire adjoint à la Défense et qu'il avait créé un *Strategic Capabilities Office*.

[90] GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 54-56.

[91] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 11 et p. 12.

[92] « MD5 Adopts New Name to Reflect Refined Mission », *National Security Innovation Network*, 6 mai 2019.

cadres de *Facebook*, *Google* et *Instagram*[93]. Ils ont pour mission de formuler des recommandations en matière d'innovation, inspirées par les pratiques de la Silicon Valley, à destination des responsables du Pentagone. En 2018, l'administration Trump prend la décision d'augmenter l'enveloppe de la DIU. Son budget passe alors de 30 à 71 millions USD pour l'année 2019. La même année, le Pentagone publie sa première *Stratégie sur l'IA* (*Artificial Intelligence Strategy*[94]). Selon le document, l'IA est essentielle pour garantir aux États-Unis leur prééminence face à des compétiteurs tels que la Chine et la Russie[95]. Le document précise aussi que l'IA est indispensable au bon fonctionnement des systèmes dits « *legacy* », c'est-à-dire des équipements plus anciens[96]. En 2020, le budget de la DIU est à nouveau augmenté ; l'Unité perçoit 164 millions USD[97]. C'est également en 2020 que naît le JAIC. Celui-ci est chargé de centraliser les initiatives liées à l'IA[98].

En matière de soutien au développement de l'IA, le Congrès n'est pas en reste. En 2018, il nomme 15 personnes qui forment la Commission nationale de sécurité sur l'intelligence artificielle (*National Security Commission on Artificial Intelligence* - NSCAI) et qui ont pour mission de réfléchir aux implications de l'IA pour les États-Unis. Eric Schmidt, l'ancien PDG de *Google*, et Robert Work, l'ancien sous-secrétaire à la Défense, sont respectivement nommés président et vice-président de celle-ci. En 2021, la Commission publie un rapport volumineux dans lequel on peut lire que l'IA va bénéficier à l'humanité. Il indique aussi, et surtout, que cette technologie constitue un enjeu de puissance[99]. Pour soutenir cette thèse, le rapport met en avant le fait que la Chine et la Russie cherchent à améliorer leurs potentiels dans ce domaine. Pour cette raison, le document recommande que les États-Unis investissent davantage dans ce secteur. La recherche dans le champ de l'IA est même présentée comme une « *frontière* » (« *Frontier* ») scientifique, ce qui revient à la placer dans le « *roman national*[100] ». Enfin, à travers ce rapport, la Commission fait de l'IA un outil nécessaire à la suprématie militaire des États-Unis et à la défense des valeurs démocratiques[101]. Le rapport préconise aussi que les États-Unis ne signent pas de traité d'interdiction sur les équipements létaux autonomes, c'est-à-dire des systèmes qui font feu sans intervention humaine. De fait, les experts qui ont rédigé ce rapport ont créé ce que Lauren A. Kahn a nommé un « *syndrome de l'inévitabilité* » à propos du développement de

---

[93] GONZÁLES Roberto J., *War Virtually., op. cit.*, p. 57; MARSHALL Shana, « The Military-Industrial Venture Complex », *Security in contex*t, 7 décembre 2023.

[94] Nous n'avons malheureusement trouvé qu'un résumé de ce document disponible en ligne. « Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity », *Department of Defense*, 2018.

[95] La rivalité économique et technologique entre les États-Unis et la Chine est bien analysée par : BÜRBAUMER Benjamin, *Chine/Etats-Unis, le capitalisme contre la mondialisation*, Paris, La Découverte, 2024, p. 147 et suivantes.

[96] « Summary of the 2018 Department of Defense Artificial Intelligence Strategy », *loc. cit.,* p. 5.

[97] GONZÁLES Roberto J., *War Virtually., op. cit.*, p. 58.

[98] KAHN Lauren A., « Risky Incrementalism », *loc. cit.*, p. 23-24.

[99] « Final Report » , *National Security Commission on Artificial Intelligence*, 2021. Le rapport fait 752 pages.

[100] *Ibid.*, p. 173.

[101] Les discours laudatifs à propos de la nature supposément démocratique de certains armements a naguère fait l'objet d'une critique par : MUMFORD Lewis, *Technique autoritaire et technique démocratique*, Saint-Michel-de-Vax, Éditions La Lenteur, 2021.

l'IA et des systèmes autonomes à des fins militaires[102]. À la lumière de ce document, on réalise, en effet, que la question qui se pose, pour le Pentagone, n'est pas celle de savoir si des systèmes autonomes seront développés mais quel sera leur degré d'autonomie[103].

En 2022 est aussi créé le Bureau principal du numérique et de l'intelligence artificielle (*Chief Digital and Artificial Intelligence Office*), qui chapeaute le JAIC et se penche à la fois sur les dimensions « *hardware* » et « *software* » de l'IA[104]. La même année, le Pentagone établit l'*Office of Strategic Capital*, une sorte de fonds d'investissement qui prête de l'argent ou offre des garanties pour des prêts aux sociétés pour les aider à développer des capacités de production dans le domaine des « *technologies critiques* » (« *critical technologies* »), dont l'IA fait partie[105]. La *Stratégie nationale de Défense* (*National Defense Strategy*) de 2022 prend également acte du développement de l'IA et met en exergue le rôle du secteur privé dans ce champ[106]. Enfin, en juin 2022, le département de la Défense publie un document intitulé *Stratégie responsable en matière d'intelligence artificielle et parcours de mise en œuvre* (*Responsible Artificial Intelligence Strategy and Implementation Pathway*[107]). Le document souligne le fait que le Pentagone se doit de développer des capacités recourant à l'IA, comme le font ses « *adversaires et compétiteurs* ». Le document cherche par ailleurs à projeter une image de responsabilité, de légalité et de respect de l'éthique autour des initiatives étatsuniennes en matière d'IA. En janvier 2023, la directive 3000.09 concernant l'autonomie des systèmes d'armes est aussi rendue publique. Ce document du Bureau du sous-secrétaire à la politique de Défense *(Office of the Under Secretary of Defense for Policy*) vise « *à établir la politique et assigner les responsabilités pour le développement et l'usage des fonctions autonomes et semi-autonomes des systèmes d'armes*[108] ». Il participe lui aussi à la construction d'une image « *responsable* » des initiatives étatsuniennes dans le domaine de l'IA. Toujours en 2023, le Pentagone fait paraître une *Stratégie d'adoption des données, de l'analyse et de l'intelligence artificielle* (*Data, Analytics, and Artificial Intelligence Adoption Strategy*[109]). On peut notamment lire dans celle-ci que : « *les États-Unis possèdent des atouts que leurs concurrents ne peuvent égaler, notamment la diversité et l'ouverture de leur société, leur culture de l'ingéniosité, leur base d'innovation et leur réseau mondial d'alliés et de partenaires*[110] ». Le discours sur l'IA s'accompagne donc d'une représentation de la supériorité technologique des États-Unis.

---

[102] KAHN Lauren A., « Risky Incrementalism », *loc. cit.*, p. 32.

[103] GONZÁLES Roberto J., *War Virtually., op. cit.*, p. 31.

[104] *Ibid.*, p. 25.

[105] « Secretary of Defense Establishes Office of Strategic Capital », *DOD News*, 1er décembre 2022 ; MARSHALL Shana, « The Military-Industrial Venture Complex », *loc. cit*.

[106] « National Defense Strategy of the United States of America », *U.S. Department of Defense*, 2022, p. 6, p. 19 et p. 20.

[107] « Responsible Artificial Intelligence Strategy and Implementation Pathway », *Department of Defense*, juin 2022.

[108] « Autonomy in Weapon System », *Departement of Defense*, DoD Directive 3000.09, 25 janvier 2023. Une première version de ce document a été publiée en 2012.

[109] « Data, Analytics, and Artificial Intelligence Adoption Strategy. Accelerating Decision Advantage », *Department of Defense*, 27 juillet 2023.

[110] *Ibid.*, p. 3.

Toujours la même année, le Pentagone met sur pied, avec la *Small Business Administration*, une *Small Business Investment Company Critical Technology* (SBICCT) *Initiative*. L'objectif de celle-ci est d'encourager les investissements privés, à travers des prêts garantis par le Pentagone, dans les « *technologies critiques*[111] ». Dans le budget de l'année fiscale 2023 du Pentagone, 130,1 milliards USD concernaient la recherche et le développement, notamment dans le domaine de l'IA[112]. À la lumière de ce montant, il faut conclure que la modernisation perpétuelle des forces est sans conteste prise au sérieux par l'institution.

En résumé, depuis environ 2014, l'IA est nettement moins connectée à la « *guerre contre le terrorisme* » que dans le passé aux États-Unis. Dans les discours des responsables du département de la Défense, l'IA est désormais perçue comme une technologie vertueuse dont le développement permettra de garantir la suprématie étatsunienne (ou occidentale) sur la Chine et la Russie. Pour le dire autrement, les références à l'IA sont intégrées dans un imaginaire géopolitique[113]. Cet imaginaire est le produit d'un véritable écosystème de l'IA au sein du Pentagone. Celui-ci justifie sa mise en place en arguant notamment qu'il contribue à façonner le marché qui lui fournit des équipements. En réalité, cet écosystème semble tout autant façonné par les intérêts de l'industrie dont le Pentagone se fait finalement le relai.

2.4. Écosystèmes financiers et vision libertarienne

Les 7 et 8 mai 2024 s'est tenue l'*AI Expo for National Competitiveness*. Cet événement était organisé par le *Special Competitive Studies Project*, un think tank fondé en 2021 par Eric Schmidt, l'ancien PDG de Google, pour faire l'apologie du développement de l'IA. La société *Palantir* avait par ailleurs en partie financé l'exposition. Pendant celle-ci eut lieu une conférence lors de laquelle Alex Karp, un des fondateurs de la société, prit la parole. La journaliste Caroline Haskins a rapporté une partie de ses propos :

> « *Il a commencé par déclarer que les États-Unis devaient "effrayer nos adversaires à mort" en temps de guerre. Se référant à l'attaque du 7 octobre du Hamas contre Israël, il a déclaré : "Si ce qui leur est arrivé nous arrivait, il y aurait un trou quelque part dans le sol". Des membres du public ont ri lorsqu'il s'est moqué des nouveaux diplômés de l'université de Columbia, qui ont*

[111] « Department of Defense and Small Business Administration Roll Out the Small Business Investment Company Critical Technologies (SBICCT) Initiative », *DOD News*, 29 septembre 2023; MARSHALL Shana, « The Military-Industrial Venture Complex », *loc. cit*.

[112] KAHN Lauren A., « Risky Incrementalism », *loc. cit.,* p. 11.

[113] Pour une perspective historique sur ces questions, voir aussi : ADAS Michael, *Dominance by Design. Technological Imperatives and America's Civilizing Mission*, Cambridge, Belknap Press, 2006 ; ADAS Michael, *Machine as the Measure of Men. Science, Technologies, and Ideologies*, Ithaca et Londres, Cornell University Press, 1989. Il serait intéressant d'évaluer jusqu'à quel point les membres du Pentagone croient sérieusement en la mythologie que l'institution s'évertue de diffuser depuis des années à propos des mérites de l'intelligence artificielle. KAHN Lauren A., « Risky Incrementalism », *loc. cit.,* p. 18.

> *organisé certains des premiers camps de protestation du pays* [en réaction aux actions des forces israéliennes]. *Il a déclaré qu'ils auraient des difficultés sur le marché du travail et a décrit leurs opinions comme une "religion païenne qui infecte nos universités" et "une infection à l'intérieur de notre société* [114]*"* ».

Alex Karp, se réappropriant un discours progressiste, n'a pas non plus hésité à affirmer lors de cette conférence que : « *Les militants de la paix sont des militants de la guerre* […]. *Nous sommes les militants de la paix*[115] ». On l'aura compris, selon lui, les fabricants d'armes sont plus aptes à assurer la paix dans le monde que les pacifistes. Alex Karp, à travers ces propos cyniques et grotesques, incarne « *l'entrepreneur rebelle*[116] ». En fait, par-delà l'accumulation de « *buzzwords* » – tels que « *innovation* », « *disruption* » ou « *révolution technologique* » – et la projection d'une imagerie du « *cool* », les responsables des start-ups telles que *Palantir* propagent une vision martiale et politiquement conservatrice, finalement peu originale[117]. Plus encore, ils usent de ces « *buzzwords* » pour faire pression sur les décideurs afin qu'ils adoptent une législation aussi libérale que possible pour leurs activités, le profit restant l'objectif principal de ces start-ups[118].

Selon le journaliste d'investigation Andrew Cockburn, expert des questions de défense, ces discours cachent une réalité bien plus prosaïque. En 2016, une « *bulle* » financière s'est formée dans le domaine de l'IA civile. Avec l'explosion de cette bulle en 2021, les investisseurs auraient perdu 7 400 milliards USD. Certains se seraient repliés sur les applications militaires, espérant pouvoir profiter de l'argent public, afin de compenser une partie de leurs pertes[119]. Comme l'écrit aussi très justement Thibault Prévost, en matière d'IA, il est surtout question de la « *captation des richesses par une poignée d'entités privées en situation d'impunité, qui déguisent leur voracité derrière une théologie d'entreprise sur mesure et tentent de nous convaincre qu'elles sont les seules dépositaires du mystère technologique*[120] ».

---

[114] HASKINS Caroline, « 'I'm the new Oppenheimer!' », *loc. cit.*

[115] *Ibid.*. Voir aussi : « Palantir: International Tech Despot », *loc. cit.* Comme l'ont montré Luc Boltanski et Eve Chiapello, l'appropriation de discours progressistes par les tenants du capitalisme le plus dur n'est pas rare. BOLTANSKI Luc et CHIAPELLO Eve, *Le nouvel esprit du capitalisme*, Paris, Gallimard, 2011.

[116] Palmer Luckey, le directeur général de Anduril Industries, adopte également une posture d'« *entrepreneur rebelle* ». MYRE Greg, « He created Oculus headsets as a teenager. Now he makes AO weapons for Ukraine », *NPR*, 9 juillet 2024.

[117] GONZÁLES Roberto J., *War Virtually., op. cit.*, p. 53. À propos de cette vision, voir aussi : GALLUZZO Anthony, *Le mythe de l'entrepreneur. Défaire l'imaginaire de la Silicon Valley*, Paris, Zones, 2023 ; MACGILLIS Alec, *Le Système Amazon. Une histoire de notre futur*, Paris, Seuil, 2021 ; DURAND Cédric, *Techno-féodalisme. Critique de l'économie numérique*, Paris, La Découverte, 2020. Pour une critique de fond de l'idéologie de l'« *innovation* », voir : FRANK Thomas, *The Wrecking Crew. The American Right and the Lust for Power*, Londres, Harvill Secker, 2008, p. 267. Notons au passage que Alex Karp et Peter Thiel, qui joue également un rôle de premier plan au sein de la société *Palantir*, ont financé la campagne de Donald Trump – mais ils ont également fait des donations à des Démocrates. « Palantir: International Tech Despot », *loc. cit.*

[118] MAASE Lucas et VERLAAN Stephanie, « Big Tech Goes to War », *loc. cit.,* p. 9.

[119] COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *loc. cit*.

[120] PRÉVOST Thibault, *Les prophètes de l'IA., op. cit.,* p. 63.

Les responsables de start-ups savent aussi que pour pouvoir capter les ressources du Pentagone, elles ont intérêt à recruter des personnalités issues du monde de la défense. En août 2024, *Palantir* a ainsi annoncé avoir engagé Mike Gallagher, un ancien membre républicain de la Chambre des Représentants qui a présidé le Comité restreint sur la Chine (*Select Committee on China)*, en tant que responsable des affaires liées à la défense[121]. Cet homme politique est un vétéran du Corps des Marines qui a travaillé dans le renseignement. Il est aussi connu pour ses prises de positions belliqueuses vis-à-vis de la Chine[122]. *Palantir* n'est cependant pas la seule start-up à s'offrir les services de personnes en vue de l'appareil de défense américain. La société *Shield AI* a fait appel à Michèle Flournoy, une ancienne sous-secrétaire du département de la Défense et co-fondatrice du think tank *Center for a New American Century*. Flournoy était déjà connue pour avoir fait l'apologie de l'IA[123]. Robert Work, le secrétaire adjoint à la Défense dont le nom a déjà été évoqué, a quant à lui rejoint la société *Hawkeye 360* – il est aussi membre du conseil d'administration du fabricant de missiles *Raytheon*[124]. David Norquist, un autre ancien secrétaire adjoint à la Défense, qui s'était lui-aussi montré favorable à davantage de dépenses dans le champ de l'IA, est devenu le responsable de l'Association nationale des industries de Défense (*National Defense Industrial Association*). Enfin, Patrick Shanahan, un homme d'affaire qui a travaillé pour *Boeing* avant d'assurer la fonction de secrétaire adjoint à la Défense entre 2017 et 2019, est devenu membre du conseil de direction de *Leidos*[125]. Ces exemples constituent des illustrations parmi d'autres du processus dit du « *pantouflage* » (ou « *revolving doors* », en anglais) par lequel des décideurs politiques, des fonctionnaires ou encore des officiers quittent le secteur public pour offrir leurs services à des sociétés privées[126]. Ce processus a été maintes fois décrié car il remet en cause l'intégrité du secteur public, en particulier lorsque les personnes concernées avaient pour mission de réguler les sociétés qui produisent les équipements des forces armées. Comme le souligne William Hartung, ceci pose aussi la question du développement d'une politique étrangère orientée par la vision de l'industrie, et donc notamment des start-ups, qui tente à tout prix de décrocher des contrats auprès du Pentagone[127].

Ces éléments ne doivent pas non plus nous faire perdre de vue un autre point essentiel : le fait que *Palantir Technologies* et les start-ups impliquées dans le développement de l'IA à

---

[121] HARTUNG William, « The Last Thing We Need Is A Palantir Inspired Foreign Policy », *Responsible Statecraft*, 28 août 2024.

[122] GALLAGHER Mike et POTTINGER Matthew, « No Substitute for Victory: America's Competition With Chine Must Be Won, Not Managed », *Foreign Affairs*, mai-juin 2024.

[123] FLOURNOY Michèle, « AI is Already at War. How Artificial Intelligence Will Transform the Military », *Foreign Affairs*, novembre-décembre 2023 ; COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *loc. cit*.

[124] Avant d'intégrer le Pentagone, il avait présidé le *Center for a New American Century*.

[125] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 21.

[126] Manifestement, ce problème concerne également le Royaume-Uni où l'ancien ministre de la Défense Ben Wallace a intégré le *Boka Group*, une société américano-britannique spécialisée dans les investissements dans le domaine des technologies militaires. PFEIFFER Sylvia, DEMPSEY Harry et FISHER Lucy, « Ben Wallace to join defence-focused firm », *Financial Times*, 1er octobre 2024.

[127] HARTUNG William, « The Last Thing We Need Is A Palantir Inspired Foreign Policy », *loc. cit.*

des fins militaires sont aussi le produit d'un écosystème industriel et financier qui dépasse l'écosystème institutionnel du Pentagone. Comme cela a été évoqué plus haut à propos des « *clouds* », pour que les forces armées puissent utiliser de manière optimale les logiciels élaborés par les start-ups, elles ont besoin d'une infrastructure informatique conséquente. Pour acquérir cette infrastructure, le Pentagone doit faire appel à des grandes sociétés privées spécialisées dans le domaine, telles que *Amazon*, *Dell*, *Google*, IBM, *Intel*, *Microsoft*, *Motorola* ou *Oracle*. Les sommes versées par les militaires à ces dernières sont conséquentes. Entre 2019 et 2023, les forces armées et agences de renseignement étatsuniennes ont ainsi signé des contrats avec les « *tech firms* » pour une valeur supérieure à 53 milliards USD. Une fraction de cette somme est allée aux start-ups. Les principaux bénéficiaires ont été les *« big tech »* qui fournissent les infrastructures[128]. Pour cette raison, il convient de considérer les start-ups – comme *Anduril Industries*, *Shield AI, HawkEye 360*, *Palantir Technologies*, *Skydio*, *Rebellion Defense* ou encore *Epirus* – comme des excroissances de fait d'*Amazon*, *Dell*, *Google*, *IBM*, *Intel*, *Microsoft*, *Motorola* ou *Oracle*, c'est-à-dire des entreprises qui gèrent les grandes infrastructures informatiques militaires[129].

Au sein de l'écosystème dans lequel les start-ups évoluent, on trouve aussi des entités spécialisées dans le financement des start-ups, dont des fonds de « *capital-risque* » (« *venture capital* ») tels que *Sequoia Capital* et *Andreessen Horowitz*. Sans ces fonds, les start-ups auraient beaucoup de difficultés à développer leurs activités. Entre 2021 et 2023, ces fonds ont fortement augmenté leurs investissements dans les start-ups qui fournissent des systèmes aux départements de la Défense[130]. Au total, elles auraient injecté plus de 100 milliards USD dans le secteur pendant cette période[131]. Pour la seule année 2023, ce montant s'élèverait à 27 milliards USD. Remarquons enfin que le phénomène du *« pantouflage »* touche également les fonds de capital-risque qui investissent dans l'IA à destination des militaires. Mark T. Esper, qui a été le secrétaire à la Défense lors du premier mandat de Donald Trump, a ainsi intégré un fonds nommé *Red Cell*[132]. Ryan McCarthy, qui a été le secrétaire à l'Armée des États-Unis (*United States Secretary of the Army*) et Raj Shah, qui a été le responsable de la *Defense Innovation Unit*, travaillent aussi pour de tels fonds.

---

[128] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 2.

[129] Amazon, Google, Microsoft et Oracle se sont positionnés sur le créneau des « *clouds* ». KELLEY Alexandra, « Microsoft, Palantir partner to expand AI offerings to defense and intelligence agencies », *Nextgov/FCW*, 8 août 2024 ; HARTUNG Willam, « Getting Past The Hype On Emerging Military Technologies Is A Life And Death Issue », *Forbes*, 19 avril 2024 ; COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *loc. cit.* ; GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 6 et p. 7.

[130] BLUM Sam, « As War Rages in Ukraine and Gaza, Venture Capitalists See a Boon in Defense Startups », *Inc.*, 22 février 2024 ; MARSHALL Shana, « The Military-Industrial Venture Complex », *loc. cit.* Andreessen a notamment investi dans *Anduril* et *Shield AI*.

[131] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 3.

[132] LIPTON Eric, « New Spin on a Revolving Door: Pentagon Officials Turned Venture Capitalist », *The New York Times*, 30 décembre 2023.

Comme on le constate, la captation de l'argent public est un moteur du développement des applications militarisées de l'IA.

3. FAIRE PROLIFÉRER L'INTELLIGENCE ARTIFICIELLE

3.1. Comment l'Ukraine est devenue un laboratoire de l'IA

En juin 2022, le CEO de *Palantir Technologie*, Alex Karp, s'est rendu en Ukraine. Il y a été reçu avec les honneurs par Volodymyr Zelensky, comme les chefs d'État qui défilent à Kiev depuis la reprise de la guerre en février de la même année. Lors de la rencontre, Karp a assuré Zelensky du soutien de son entreprise à l'Ukraine. Karp a aussi comparé l'alliance entre les Ukrainiens et *Palantir Technologies* à David devant lutter contre Goliath. Les produits de *Palantir* seraient employés par une demi-douzaine d'agences civiles et militaires ukrainiennes. Des ingénieurs ukrainiens travailleraient à l'adaptation des logiciels de la société aux besoins de leur pays. Une version du programme *Maven* qui emploie des technologies de la société *Palantir* aurait par ailleurs été mise à disposition des forces ukrainiennes[133]. Ce logiciel génère, grâce à des informations provenant de sources variées, une image aussi détaillée que possible du champ de bataille ukrainien[134]. En 2023, Karp dira même que sa société était « *responsable de l'essentiel du ciblage en Ukraine* », une affirmation cependant difficile à vérifier[135]. Ajoutons que *Palantir Technologies* assure ne pas facturer le gouvernement ukrainien pour ses services. À travers cette aide qu'elle fournit gracieusement à l'Ukraine, *Palantir* tente de se construire une image philanthropique, qui prend cependant des accents martiaux[136].

[133] SANGER David E., « In Ukraine, New American Technology Won the Day. Until It Was Overwhelmed », *New York Times*, 30 avril 2024

[134] RICKLI Jean-Marc et MANTELLASSI Federico, *The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare*, GCSP, 2024, p. 20.

[135] BRAMFORD James, « How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza », *The Nation*, 12 avril 2024.

[136] Sur la philanthropie comme élément de légitimation, voir : GUILHOT Nicolas, *Financiers philanthropes. Sociologie de Wall Street*, Paris, Raison d'Agir, 2006. Notons que les responsables de *Palantir Technologies* ne sont pas les seuls à avoir joué la carte philanthropique. Le milliardaire Elon Musk l'a également fait en mettant à disposition des Ukrainiens son réseau de communication satellitaire *Starlink*. MILLER Christopher, SCOTT Mark et BENDER Bryan, « UkraineX: How Elon Musk's space satellites changed the war on the ground », *Politico*, 8 juin 2022.

Palantir Technologies n'est pas la seule start-up présente en Ukraine. *Clearview AI*, une start-up spécialisée dans la reconnaissance faciale, y opère aussi. Elle aurait « *fourni son outil à plus de 1 500 fonctionnaires ukrainiens, qui l'ont utilisé pour identifier plus de 230 000 Russes sur leur territoire ainsi que des collaborateurs ukrainiens*[137] ». D'autres petites sociétés travaillant entre autres sur des drones autonomes poursuivent aussi des activités en Ukraine – on peut par exemple citer la start-up européenne *Helsing*. En août 2024, Eric Schmidt, l'ancien PDG de *Google* et président de la *National Security Commission on Artificial Intelligence*, a également fait savoir que sa start-up *White Stork*, allait soutenir l'Ukraine en développant des drones capables d'identifier leurs cibles de manière autonome[138]. Eric Schmidt fait partie de ceux qui font l'apologie de l'usage des drones opérant « *en réseau* » ou « *en essaim* » (« *swarm* ») dans le contexte de la guerre en Ukraine[139]. Ces drones légers et bon marché se coordonnent en utilisant l'IA. Ils sont capables de reconfigurer leur dispositif d'attaque lorsque l'un d'eux est abattu.

L'Ukraine est ainsi devenue un vaste laboratoire pour les start-ups qui se spécialisent dans la production d'équipements militaires recourant à l'IA[140]. En 2022, les autorités ukrainiennes ont d'ailleurs mis en place un accélérateur de start-ups nommé D3 (*Dare to Defend Democracy*). L'initiative décrite comme « *visant à soutenir les innovateurs du monde entier qui aident l'Ukraine à protéger et à faire progresser sa démocratie grâce à la technologie*[141] » a été développée avec l'aide d'Eric Schmidt[142]. Au total, les Ukrainiens auraient reçu plus de 1 000 propositions pour tester du matériel militaire recourant à l'IA. Il faut noter que les initiatives dans le domaine ne concernent pas que des sociétés étatsuniennes. L'Union européenne (UE), notamment, a décidé de financer l'installation d'un « *centre d'innovation pour la défense* » (« *defense innovation hub* ») à Kiev[143]. Le projet a pour objectif de connecter les start-ups européennes avec l'industrie ukrainienne. Remarquons par ailleurs que les Ukrainiens emploient les « *cloud services* » d'*Amazon*, *Google* et *Microsoft* dans le conflit.

L'efficacité des nouvelles technologies dans la guerre en Ukraine fait cependant l'objet de questionnements[144]. Selon certains témoignages, ces équipements s'avéreraient coûteux,

---

[137] BRAMFORD James, « How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza », *loc. cit*.

[138] « Ex-Google CEO Eric Schmidt's startup White Stork aims to arm Ukraine with AI-powered attack drones », *Livemint*, 20 août 2024. Eric Schmidt est par ailleurs à la tête d'un fonds, *Innovation Endeavours*, qui a investi dans *Rebellion Defense*. De par sa position dans ce fonds, il siège dans le conseil d'administration de *Rebellion Defense*. MHALLA Asma, *Technopolitique. Comment la technologie fait de nous des soldats*, Paris, Seuil, 2024, p. 184.

[139] SANGER David E., « In Ukraine, New American Technology Won the Day. Until It Was Overwhelmed », *loc. cit.*

[140] BERGENGRUEN Vera, « How Tech Giants Turned Ukraine Into an AI War Lab », *Time*, 8 février 2024.

[141] « About », *Dare to Defend Democracy*, consulté le 17 avril 2025.

[142] MOZUR Paul et SATARIANO Adam, « A.I. Begins Ushering In an Age of Killer Robots », *New York Times*, 2 juillet 2024.

[143] RUITENBERG Rudy, « EU opens defense innovation hub in Kyiv to boost industry outreach », *Defense News*, 30 septembre 2024.

[144] GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 26; BORCHERT Heiko, SCHÜTZ Torben et VERBOVSZKY Joseph, « *Beware the Hype.*

fragiles et vulnérables aux contre-mesures russes[145]. D'après un article publié en avril 2024 dans le *Wall Street Journal* : « *La plupart des petits drones des start-ups américaines n'ont pas réussi à s'illustrer au combat*[146] ». Ces équipements décevraient leurs utilisateurs, qui préféreraient employer des drones chinois[147]. De surcroît, comme le mettent en exergue Jean-Marc Rickli et Federico Mantellassi : « *Les champs de bataille de l'Ukraine montrent que même si la guerre évolue indubitablement, son avenir aura encore beaucoup à voir avec son passé*[148] ». Pour le dire autrement, la guerre reste une affaire de technologies anciennes. Les équipements fournis par les start-ups – au même titre que les équipements plus anciens d'ailleurs – sont loin d'être des armes magiques et de créer les conditions d'une victoire décisive[149]. En dépit de cela, l'intérêt de l'Ukraine pour les appareils autonomes ne cesse de croître. Comme l'écrit un journaliste : « *L'Ukraine dispose d'une ressource précieuse : des millions d'heures d'images filmées par des drones, qui peuvent être utilisées pour former des modèles d'intelligence artificielle capables de prendre des décisions sur le champ de bataille*[150] ». À en juger par cette remarque, la souffrance des combattants filmés est considérée comme une source potentielle de revenus par l'industrie.

L'expérience du conflit en Ukraine est aussi utilisée pour valider des projets datant d'avant 2022, et qui ont été développés dans le contexte de la montée des tensions entre les États-Unis et la Chine. Comme le révélait une étude de la *RAND Corporation* de 2020, ces projets envisagent notamment la possibilité que des centaines de drones bon marché opérant en réseau puissent guider des missiles à longue-portée qui viseraient des navires chinois[151]. Le rapport *Swarm over the Strait*, publié en juin 2024 par le *Center for a New American Century* offre une autre illustration de ce phénomène[152]. Ce rapport s'appuie non seulement sur l'analyse de la guerre en Ukraine mais aussi sur une étude du conflit libyen et de celui qui a opposé l'Azerbaïdjan à l'Arménie. Les autrices adoptent un ton nuancé. Elles ne prétendent pas que les nouvelles technologies et les drones sont des armes décisives. Mais elles

What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War », *DAIO Study*, 21/01, 2021.

[145] SANGER David E., « In Ukraine, New American Technology Won the Day. Until It Was Overwhelmed », *loc. cit*.

[146] SOMERVILLE Heather et FORREST Brett, « How the American Drones Failed to Turn the Tide in Ukraine », *Wall Street Journal*, 10 avril 2024. Voir aussi : HARTUNG Willam, « Getting Past The Hype On Emerging Military Technologies Is A Life And Death Issue », *loc. cit.*

[147] SOMERVILLE Heather et FORREST Brett, « How the American Drones Failed to Turn the Tide in Ukraine », *loc. cit.* ; MYRE Greg, « He created Oculus headsets as a teenager. Now he makes AO weapons for Ukraine », *loc. cit.* ; ROBERSTON Noah, « The Pentagon's 'Replicator' drone bonanza faces an uncertain future », *Defense News*, 14 janvier 2025.

[148] RICKLI Jean-Marc et MANTELLASSI Federico, *The War in Ukraine*, *op. cit*., p. 38.

[149] GADY Franz-Stefan, « Why There Are No Game-Changing Weapons for Ukraine », *Foreign Policy*, 14 septembre 2023.

[150] Citation traduite de l'anglais. HUNDER Max, « Ukraine collect vast war data trove to train AI models », *Reuters*, 20 décembre 2024. L'auteur évoque 2 millions d'heures, soit l'équivalent de 228 années d'enregistrement.

[151] HAMILTON Thomas et OCHMANEK David A., *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments. Preliminary Evaluation of Operational Concepts*, RAND Corporation, 2020.

[152] PETTYJOHN Stacie, DENNIS Hannah et CAMPBELL Molly, « Swarms over the Strait. Drone Warfare in a Future Fight to Defend Taiwan », *CNAS*, 20 juin 2024.

soulignent le fait que ces équipements, aux côtés d'autres matériels, sont nécessaires pour faire face à la Chine. En juin 2024 également, l'amiral Samuel Paparo, qui est à la tête du Commandement indopacifique (*Indo-Pacific Command*), a décrit, lors d'une conférence qui s'est tenue à Singapour, une guerre imaginaire résultant d'une tentative d'invasion de Taïwan par la Chine[153]. Selon lui, dans un tel conflit, les États-Unis lanceraient *« des milliers et des milliers »* de drones aériens, navals et terrestres, opérant en essaim au combat. Ces drones auraient pour mission de créer un « *un paysage infernal* » (« *hellscape* ») pour retarder l'avancée chinoise et permettre aux forces étatsuniennes de mobiliser des moyens plus conséquents pour les repousser.

Ces discours viennent légitimer des décisions en matière d'acquisition d'armements. Cela est attesté par l'annonce faite par le Pentagone, en août 2023, de lancer le projet *Replicator* – un nom tiré de *Star Trek*[154]. L'objectif de ce projet est de développer des drones relativement bon marché, utilisant l'IA et opérant en essaim. Ce projet est présenté comme une réponse à l'amélioration des capacités dites de « *déni d'accès et interdiction de zone* » (« *anti-access/area-denial* » ou AD/A2) chinoises. En mai 2024, la vice-secrétaire à la Défense Kathleen Hicks a aussi annoncé que la première tranche du projet se concentrerait sur les « *All Domain Attritable Autonomous Systems*[155] ». Cette tranche vise à acheter des milliers de drones recourant à l'IA. Actuellement, le projet *Replicator* bénéficie notamment à *AeroVironment* et à la start-up *Anduril*[156].

À la lumière du conflit en Ukraine, les experts les plus critiques doutent cependant de l'efficacité de ce projet pour contrer une éventuelle menace chinoise[157]. Des chercheurs s'inquiètent aussi de ce que ces discours et ces décisions ne soient en fait que la simple traduction des intérêts des fonds de capital-risque. Les chercheuses Shana Marshall et Elke Shwartz se demandent ainsi si ces fonds ne sont pas en train de redéfinir le futur de la guerre à travers la promotion de concepts tels que « *guerre attritive* » (« *attritable warfare* »), « *déploiement rapide autonome* » (« *autonomous rapid deployment* ») ou « *essaim*[158] ». En tous les cas, la panique créée autour du manque de munitions classiques et de drones dans le contexte de la guerre en Ukraine a fait le lit de ce nouvel imaginaire guerrier, reposant sur la conviction qu'il faut user l'adversaire, ce qui nécessiterait d'augmenter les capacités de production d'armes et d'investir massivement dans l'innovation. Pour la chercheuse

[153] KELLER Jared, « The Pentagon Is Planning a Drone 'Hellscape' to Defend Taiwan », *Wired*, 19 août 2024.

[154] BAJAK Frank, « Pentagon's 'Replicator' gambit may speed decisions on lethal autonomy », *C4ISR*, 26 novembre 2023 ; BARROW Michael, « Shield AI sees Dod opening for 'intelligent, affordable mass' of drones », *Breaking Defense*, 13 octobre 2023.

[155] « Deputy Secretary of Defense Hicks Announces First Tranche of Replicator Capabilities Focused on All Domain Attritable Autonomous Systems », *DOD News*, 6 mai 2024.

[156] *AeroVironment* fournira, pour ce projet, des drones Switchblade-600. Les drones *Switchblade* ont été utilisés, dans une version dépourvue d'intelligence artificielle, pour combattre l'État islamique. STONE Mike, « Pentagon's Replicator selects AeroVironment's Switchblade-600 as first buy », *Reuters*, 6 mai 2024 ; ALBON Courtney, « Anduril to open software-based manufacturing hub to scale production », *Defense News*, 8 août 2024 ; VINCENT Brandi, « Army moves to rapidly field Anduril's Ghost-X drones via Replicator », *DefenseScoop*, 7 octobre 2024.

[157] ROBERSTON Noah, « The Pentagon's 'Replicator' drone bonanza faces an uncertain future », *loc. cit.*

[158] MARSHALL Shana, « The Military-Industrial Venture Complex », *loc. cit.* ; SCHWARZ Elke, « Unicorns for Uniforms: On the Problematic Allure of VC Investments in Defense », *Opinio Juris*, 18 septembre 2024.

Shana Marshall, les fonds et start-ups qui se présentent comme des acteurs pouvant apporter des solutions aux problèmes collectifs, devraient plutôt être perçus comme des parasites spécialisés dans l'extraction de ressources publiques[159].

3.2. La machine israélienne à assassiner

Le cas israélien s'avère également important à analyser pour comprendre la normalisation du recours à l'IA par les forces armées. Ce cas est d'autant plus intéressant à étudier que l'industrie israélienne qui élabore des logiciels employés par les forces de sécurité est liée aux entreprises étatsuniennes qui ont été évoquées jusqu'ici. L'importance du recours à l'IA en Israël est révélée en novembre 2023 par un article d'investigation publié dans le média *+972 Magazine*. L'auteur de l'enquête, Yuval Abraham, y annonce que les forces israéliennes déployées à Gaza utilisent un système automatisé de sélection des cibles reposant sur l'emploi de l'IA[160]. Abraham fait remarquer dans son article que ce système, nommé « *Habsora* » (ou « *The Gospel* »), « *produisait* » 100 cibles par jour. Une fois les cibles désignées, les militaires peuvent décider de les éliminer en recourant notamment à des bombardements d'artillerie. On apprend aussi dans cette enquête que *Habsora* a été conçu par la *Targets Administrative Division*, une unité fondée en 2019. Les membres de cette unité avaient pour mission d'élaborer un dispositif permettant d'accélérer le processus de sélection des cibles grâce à l'emploi de l'IA. Les militaires israéliens déployés à Gaza considèrent ce système comme une « *usine* » (« *factory* ») à tuer des combattants ennemis. Dans les faits, cette machine tue aussi énormément de civils.

En avril 2024, Yuval Abraham publie un nouvel article, également dans *+972 Magazine*, sur un autre programme de ciblage recourant à l'IA employé par les forces israéliennes : *Lavender*[161]. Le journaliste explique que *Lavender* attribue un chiffre allant de 1 à 100 à chaque habitant de Gaza afin d'évaluer la probabilité qu'il ou elle appartienne au Hamas. Pour réaliser cette évaluation, la machine utilise de nombreuses sources d'informations (des informations provenant des téléphones portables et des réseaux sociaux, des contacts téléphoniques, des photos, etc.). Elle tient par exemple compte du fait que les habitants de Gaza font partie des groupes *WhatsApp* au sein desquels est enregistré au moins un membre du Hamas. Le fait que la personne change régulièrement de téléphone ou d'adresse est également pris en compte dans l'évaluation automatique. *Lavender* aurait ainsi désigné jusqu'à 37 000 cibles potentielles à Gaza. Le système s'avère cependant peu discriminant[162]. Il lui arrive, en effet, de désigner comme cible un policier ou un membre de la défense civile ou encore des proches des militants. *Lavender* ne prend certes pas lui-même la décision de lancer une attaque, les cibles qu'il désigne sont analysées par des soldats. Mais ceux-ci prennent peu de temps pour effectuer leurs vérifications. Le contrôle

[159] MARSHALL Shana, « The Military-Industrial Venture Complex », *loc. cit.*

[160] ABRAHAM Yuval, « 'A mass assassination factory': Inside Israel's calculated bombing of Gaza », *+972 Magazine*, 30 novembre 2023.

[161] ABRAHAM Yuval, « Lavender': The AI machine directing Israel's bombing spree in Gaza », *+972 Magazine*, 3 avril 2024.

[162] ISMAILOVIC Muzen, « Ciblage algorithmique : le rôle de l'intelligence artificielle dans les frappes israéliennes à Gaza et ses implications éthiques », *Éclairage du GRIP*, 20 février 2025.

humain sur ce système, autrement dit, s'avère faible. Dans son article, Yuval Abaham explique aussi qu'une autre application, nommée *« Where's Daddy »*, est utilisée par les forces israéliennes. Elle permet de suivre des individus à distance afin de les faire éliminer lorsqu'ils entrent dans leur domicile. Une source citée dans l'article de *+972* indique à propos de ce logiciel que : *« Vous introduisez des centaines* [de cibles] *dans le système et vous attendez de voir qui vous pouvez tuer »*. La même source ajoute : *« C'est ce qu'on appelle la chasse large* [*« broad hunting »*]*: vous copiez-collez des listes produites par le système cible*[163] ». Cette citation confirme aussi la tournure « *industrielle* » que prend le massacre réalisé à l'aide de l'IA.

Bien que le conflit qui se déroule actuellement à Gaza illustre de façon saisissante une normalisation de l'emploi militaire de l'IA par les forces israélienne, il faut indiquer que celui-ci n'est pas tout à fait nouveau. Les forces israéliennes ont déjà utilisé un logiciel de « *fusion des données* » *(« data fusion* ») nommé *Crystal Ball* lors de l'opération « *Bordure protectrice* » de 2014, qui se soldera par la mort de plus de 1 500 Palestiniens[164]. Depuis 2017 au moins, des porte-paroles des forces israéliennes affirment qu'ils considèrent l'IA comme essentielle[165]. En 2021, le général Yossi Sariel, qui commande l'unité 8200 en 2024, a aussi publié un livre dans lequel il évoque « *un système d'IA supposé fictif et d'une grande portée* »[166]. La description qu'il en donne n'est pas sans rappeler *Lavender*. Il souligne le fait que : « *Les humains sont le goulot d'étranglement qui empêche la création de dizaines de milliers de cibles en contexte*[167] ». La même année, les forces israéliennes employaient les programmes *Alchemist*, *Gospel* et *Depth of Wisdom* à Gaza pour combattre le Hamas lors de l'opération « *Gardien du mur* », lors de laquelle 256 Palestiniens ont été tués et des dizaines de milliers blessés[168]. En 2023, le général Eyal Zamir, lors d'une conférence organisée à Herzlya, faisait aussi connaître un plan de plusieurs années visant l'amélioration des capacités militaires israéliennes. Le général Zamir mettait en exergue l'apport révolutionnaire de l'IA pour le renseignement et le ciblage pendant cette conférence,

---

[163] Les forces israéliennes utilisent par ailleurs « *AnyVision* », un logiciel de reconnaissance faciale notamment installé aux checkpoints pour contrôler les Palestiniens. Elles emploieraient aussi *« The Alchemist »*, qui permet la détection visuelle de cibles, et « *The Depth of Wisdom* ». DOLINKO Inbar et ANTEBI Liran, « Embracing the Organized Mess: Defense AI in Israel » dans BORCHERT Heiko, SCHÜTZ Torben et VERBOVSZKY Joseph (Ed.) *The Very Long Game. 25 Case Studies on the Global State of Defense AI,* Springer, 2024, p. 397-420.

[164] POULSON Jack, « Microsoft and Google have been working closely with the Israeli military's Computer Services Directorate for years, in shadow of flashier military intelligence unit », *Substack*, 2 mai 2024.

[165] MERCHANT Brian, « Column: We don't know how Israel's military is using AI in Gaza, but we should », *Los Angeles Times*, 2 novembre 2023.

[166] BRAMFORD James, « How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza », *loc. cit.* ; Y.S., *The Human Machine Team. How to Create Synergy Between Human & Artificial Intelligence That Will Revolutionize Our World*, eBookPro Publishing, 2021. L'auteur a rédigé cet ouvrage lorsqu'il était étudiant à la *National Defense University*, aux Etats-Unis.

[167] Y.S., *The Human Machine Team*., *op. cit.*

[168] PG Apoorva, « Seeing The World Like A Palestinian. Intersectional Struggles Against Big Tech and Israeli Apartheid », *Transnational Institute*, 14 février 2023; AHRONHEIM Anna, « Israel's operation against Hamas was the world's first AI war », *The Jerusalem Post*, 27 mai 2021.

attestant lui aussi de l'importance que les forces israéliennes accordent à cette technologie[169].

Derrière ces discours et ces programmes, on décèle également la présence d'un écosystème militaro-industriel en Israël, lequel est par ailleurs lié aux entreprises étatsuniennes. Au sein de celui-ci, on trouve tout d'abord l'unité 8200 (*shmone matayim*). Cette unité est l'équivalent israélien de la NSA aux États-Unis. Ses experts travaillent notamment sur le développement d'outils d'« *exploration des données* » (*« data mining »*), capables de fusionner de grandes quantités de données, ainsi que sur des « *logiciels prédictifs* » (« *predictive software* »), censés pouvoir prédire les comportements des acteurs. Pour concevoir ces programmes, l'unité sélectionne des jeunes considérés prometteurs (mais qui ne peuvent pas être des Arabes) et leur offre un travail alléchant dans le domaine technique[170]. Comme l'écrivait à son propos le journaliste Idan Tener :

> *« La 8200 est une unité spéciale et, à bien des égards, elle est gérée comme une start-up de haute technologie. Cela commence par la recherche des meilleurs talents. Les recruteurs* [des forces israéliennes] *passent en revue les écoles secondaires du pays afin d'identifier les candidats à fort potentiel dès leur plus jeune âge. Ils ciblent les étudiants dotés de capacités analytiques supérieures, capables de prendre des décisions rapides et de travailler en équipe. Seuls les meilleurs et les plus brillants sont orientés vers ce groupe d'élite de la cybersécurité*[171] ». Et le même d'ajouter : *« Il en résulte que les anciens élèves de l'unité 8200 ont acquis des compétences et une expérience essentielles en matière de création d'entreprise avant même de créer leur première société. C'est pourquoi il n'est pas surprenant que des entreprises technologiques telles que* CheckPoint*,* Imperva*,* Nice*,* Gilat*,* Waze*,* Trusteer *et* Wix *aient toutes leurs racines dans cette unité de la* [force israélienne de défense][172] ».

Cette unité est donc un « *incubateur* » de start-ups qui rapproche les services de sécurité des universités et du monde de l'entreprise. Elle n'est par ailleurs pas la seule bureaucratie issue de l'appareil de sécurité israélien à favoriser l'émergence de start-ups spécialisées dans l'IA. On peut ainsi citer l'*Operational Technology Intensification* (LOTEM) et l'unité 81 de la direction du renseignement militaire israélien (« *Aman »* en hébreu[173]). Leur impact est loin d'être nul sur le plan économique si l'on en juge par exemple par le fait que, entre 2003 et 2010, d'anciens membres de l'unité 81 ont créé une cinquantaine de sociétés, parmi

---

[169] BERMAN Lazar, « Defense Ministry to invest heavily in AI in bid to improve intel on Iran », *The Times of Israel*, 22 mai 2023, cité par DOLINKO Inbar et ANTEBI Liran, « Embracing the Organized Mess: Defense AI in Israel », *loc. cit.*, p. 21.

[170] REED John, « Unit 8200: Israel's cyber spy agency », *Financial Times*, 10 juillet 2015. Ajoutons que les membres de l'unité 8200 auraient peut-être créé le *« worm » Stuxnet* qui a été utilisé contre des ordinateurs iraniens employés dans le secteur nucléaire.

[171] TENDLER Idan, « From The Israeli Army Unit 8200 To Silicon Valley », *TechCrunch*, 20 mars 2015.

[172] *Ibid*.

[173] DOLINKO Inbar et ANTEBI Liran, « Embracing the Organized Mess: Defense AI in Israel », *loc. cit.*, p. 17.

lesquelles *Innovi*, *D-Fend* et *Exodigo*[174]. Cette dernière est une start-up qui a développé un appareillage capable de produire, à l'aide de capteurs et de l'IA, une cartographie en trois dimensions de ce qui se passe sous terre[175]. Le service de renseignement intérieur, le *Shin Bet*, a quant à lui été à l'origine de la formation de *SpeechRecognition*[176]. Enfin, le Mossad aurait fondé *Libertad*, un fonds pour encourager l'innovation technologique.

Il faut noter que les produits de ces start-ups ne sont pas uniquement destinés aux forces israéliennes. Ils sont également exportés, notamment vers des pays usant de la répression contre une partie de leur population. Cela est notamment attesté par les ventes de logiciels de surveillance de *Verint* et *Nice Systems* au Kazakhstan et à l'Ouzbékistan, des États répressifs d'Asie centrale[177]. En 2014, les exportations de systèmes « *cyber* » israéliens, à destination des secteurs privés et publics atteignaient 6 milliards USD, soit plus que la valeur des exportations d'armes de cet État. La réputation de ces équipements repose en partie sur la mythologie de la « *start-up nation* », qui s'appuie elle-même sur un discours qui fait du « *génie technique* » israélien, une caractéristique pour ainsi dire ethnique[178]. Dans le champ des armements, cette mythologie a notamment pour effet d'occulter le fait que ces équipements sont utilisés par les forces israéliennes qui répriment les Palestiniens.

Le « *génie national* » ne se traduit cependant pas par une indépendance totale de l'appareil de sécurité israélien. Ce dernier, pour faire fonctionner ses gadgets électroniques, a besoin de l'assistance de grandes entreprises étatsuniennes. Ceci a bien été illustré dans le contexte du projet *Nimbus*. Ce projet, d'un montant de 1,2 milliard USD, avait pour objectif de doter l'État israélien des capacités civiles et militaires de « *cloud computing*[179] ». Pour l'exécution de ce projet, les Israéliens ont dû faire appel à *Amazon* et *Google* – *Microsoft* avait aussi été sollicitée mais, à cette époque, mise sous pression par certains de ses employés, a finalement décidé de ne pas collaborer avec le gouvernement israélien. De manière générale, il existe une relation symbiotique entre le secteur informatique israélien et celui, étatsunien, des « *big tech* ». Ces liens contribuent à faire vivre le secteur en Israël et, dans le même temps, à l'industrie de la surveillance électronique de se développer[180]. Les liens en question n'ont par ailleurs pas été remis en question par les récentes accusations de génocide formulées à l'encontre des forces israéliennes. Au contraire même, ils se sont renforcés ces derniers mois car les forces israéliennes ont eu besoin de davantage de capacités informatiques et de stockage pour mener à bien leurs opérations en Palestine. Pour cette raison, elles ont à nouveau fait appel à *Amazon*, *Google* et *Microsoft*[181]. Cette

[174] *Ibid.*, p. 17.

[175] *Ibid.*, p. 17.

[176] *Ibid.*, p. 27.

[177] REED John, « Unit 8200: Israel's cyber spy agency », *loc. cit.*

[178] SENOR Dan et SINGER Saul, *Start-Up Nation. The Story of Israel's Economic Miracle*, New York, Twelve, 2009.

[179] PG Apoorva, « Seeing The World Like A Palestinian », *loc. cit.* ; GONZÁLES Roberto J., « How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex », *loc. cit.*, p. 9.

[180] PG Apoorva, « Seeing The World Like A Palestinian », *loc. cit.*

[181] DE VYNCK Gerrit, « Google rushed to sell AI tools to Israel's military after Hamas attack », *Washington Post*, 22 février 2025 ; DAVIES Harry et ABRAHAM Yuval, « Revealed: Microsoft deepened ties with Israeli military to provide tech support during Gaza war », *The Guardian*, 23 janvier 2025.

dernière, qui collabore dorénavant avec Tel-Aviv, fournit notamment aux militaires israéliens des accès à *GPT-4* et participe à la maintenance des systèmes *Ofek*, une « *target bank* » des forces aériennes, et *Rolling Stone* qui contrôle les mouvements des populations palestiniennes à Gaza et en Cisjordanie.

Enfin, il convient d'évoquer ici les liens plus spécifiques qui unissent *Palantir Technologies* à l'État israélien[182]. Pour commencer, il faut noter qu'Alex Karp, le PDG de la société, s'est montré publiquement très favorable à la politique israélienne. En 2023, alors qu'il participait au *Reagan National Defense Forum*, il a affirmé qu'il ne connaissait que trois sociétés réellement pro-israéliennes aux États-Unis : *Booz Allen Hamilton*, *Anduril Industries* et *Palantir*[183]. En janvier 2024, alors que Tsahal pilonnait la bande de Gaza sans retenue, Alex Karp s'est rendu en Israël. Avant d'être conduit dans des installations du ministère de la Défense, il a loué le talent de ses hôtes. Il a ensuite signé des accords pour la mise à niveau des produits de *Palantir* pour les forces israéliennes[184]. Peter Thiel, un autre fondateur de *Palantir*, entretient lui aussi des liens étroits avec l'industrie israélienne. Il a par exemple investi dans *Carbyne*, une société qui ressemble à *Palantir* et qui est dirigée par Ehud Barak, l'ancien général et Premier ministre israélien[185].

Les logiciels recourant à l'IA utilisés par les forces israéliennes ont, semble-t-il, été développés localement. Ils sont le produit d'un écosystème qui préexiste aux opérations menées à Gaza depuis le mois d'octobre 2023. Les acteurs de cet écosystème entretiennent aussi des relations avec les grandes sociétés étatsuniennes spécialisées dans les infrastructures informatiques. L'appareillage électronique que les industries issues de cet écosystème ont élaboré contribue à consolider le sentiment national de sécurité, au même titre d'ailleurs que le « *dôme de fer* », un système antiaérien interceptant des roquettes. Cet appareillage n'est cependant pas parvenu à empêcher l'attaque du 7 octobre 2023. Il faut en conclure que les garanties de sécurité offertes par l'IA relèvent, au moins en partie, de l'illusion. En dépit de cela, la confiance accordée à cet appareillage n'a visiblement pas décru, les forces israéliennes n'hésitant pas à employer des programmes tels que *Lavender* et *Habsora* à Gaza. Ces programmes ont cependant la réputation d'être peu discriminants dans la détermination des cibles. Au final, on peut en déduire que le recours à ces systèmes a essentiellement servi à donner aux massacres qui se sont déroulés à Gaza l'apparence de la rationalité stratégique et d'un usage proportionné de la force.

---

[182] L'unité 8200 et le *Shin Bet* auraient décidé de ne pas travailler avec *Palantir Technologies*, ces organisations préférerant faire appel à des sociétés israéliennes. En revanche, *Palantir Technologies* vend ses services aux forces armées israéliennes. GILEAD Assaf, « What is Palantir doing in Israel », *Globes*, 29 janvier 2024 ; POULSON Jack, « Microsoft and Google have been working closely with the Israeli military's Computer Services Directorate for years, in shadow of flashier military intelligence unit », *loc. cit.*

[183] « Palantir: International Tech Despot », *loc. cit.*

[184] BRAMFORD James, « How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza », *loc. cit.*

[185] « Palantir: International Tech Despot », *loc. cit.* Jeffrey Epstein, un « *business partner* » de Ehud Barak, a également investi dans cette société. Notons aussi que *Palantir* a soutenu le développement de *Cellebrite*, une société qui a créé un logiciel de piratage téléphonique (*« phone-hacking »*) utilisé par les autorités du Bahreïn pour appréhender et torturer des activistes. Le logiciel est aussi employé par les autorités britanniques.

Il faut noter que l'expansion de l'écosystème en charge du développement de l'IA se poursuit actuellement. Les forces de sécurité israéliennes sont ainsi en train de développer un système de type *ChatGPT* destiné à assurer la surveillance de l'ensemble de la population palestinienne à partir d'une immense banque de données sur celle-ci. Il est possible que ce système soit entre autres mis au point par des réservistes des forces israéliennes travaillant pour des grandes entreprises étatsuniennes spécialisées dans le domaine informatique, comme *Google*, *Meta* ou *Microsoft*[186]. Le recours à cette technologie est présenté par ses thuriféraires israéliens comme un moyen de réduire les effectifs et les dépenses militaires[187]. Ces arguments, qui contribuent à la normalisation de l'IA dans le champ militaire, passent allègrement sous silence les coûts humains associés au déploiement de l'IA par les forces de sécurité.

3.3. La circulation transnationale de l'« innovation »

Depuis quelques années, les États-Unis font la promotion de l'IA à des fins militaires auprès de leurs alliés. En 2020, le Pentagone met ainsi sur pied un « *Partenariat IA pour la Défense* » (« *AI Partnership for Defense*[188] »). Il s'agit d'un forum au sein duquel des représentants des États alliés des États-Unis échangent à propos de leurs politiques en matière d'IA. Des délégations allemande, australienne, britannique, canadienne, danoise, estonienne, finlandaise, française, israélienne, japonaise, néerlandaise, norvégienne, singapourienne et sud-coréenne participent aux discussions en son sein. Le partenariat promeut un usage « *éthique* » de l'IA et tente de coordonner les efforts des alliés afin de garantir l'interopérabilité de leurs moyens. De fait, il contribue à la normalisation de l'usage de l'IA à des fins de défense parmi les alliés des États-Unis. Le projet AUKUS (pour *Australia, United Kingdom and United States*), qui concerne principalement l'acquisition de sous-marins à propulsion nucléaire par l'Australie, comporte également un volet collaboratif dans le domaine de l'IA. À l'été 2024, les trois États impliqués dans ce projet ont, dans ce cadre, testé des drones autonomes qui scannaient un terrain à la recherche des véhicules ennemis à détruire[189].

La promotion du développement de l'IA au profit des forces armées passe aussi par l'Organisation du traité de l'Atlantique nord (OTAN). En 2021, lors de son sommet de Bruxelles, l'alliance atlantique a annoncé la création d'un « *accélérateur d'innovation* » nommé Accélérateur d'innovation en matière de défense pour l'Atlantique nord (*Defence Innovation Accelerator for the North Atlantic*- DIANA). DIANA est présenté comme un fonds

[186] DAVIES Harry et ABRAHAM Yuval, « *Revealed: Israeli military creating ChatGPT-like tool using vast collection of Palestinian surveillance date* », *The Guardian*, 6 mars 2025.

[187] GREENBERG Tzally, « Israel creates hub to hasten military AI, autonomy research », *Defense News*, 2 janvier 2025.

[188] KAHN Lauren A., « Risky Incrementalism », *loc. cit.,* p. 28.

[189] *Ibid.*, p. 28; BROWN Larissa, « UK and allies use AI drones in battlefield exercise for first time », *The Times*, 9 août 2024. Le projet AUKUS concerne notamment l'acquisition de sous-marins à propulsion nucléaire par l'Australie.

de capital-risque multinational destiné notamment à investir dans le domaine de l'IA, du traitement des données massives (« *big data* ») et des technologies quantiques[190]. Lors de ce sommet, les membres de l'alliance ont aussi convenu de créer un « NATO *Innovation Fund*[191] ». Ce fonds de capital-risque alimenté par 23 États membres est approvisionné à hauteur de, approximativement, 1 milliard EUR. Cet argent est destiné à soutenir des start-ups qui développent des « *solutions technologiques concurrentielles* » (« *cutting-edge technological solutions*[192] »). Ces initiatives, qui s'inspirent directement des développements étatsuniens, font de l'OTAN un acteur contribuant à la normalisation de l'IA à des fins militaires[193].

L'Europe participe aussi à la diffusion de l'IA à des fins de sécurité. Ceci est notamment illustré par la décision du Conseil et de la Commission européenne de financer le développement d'armes autonomes via le Fonds européen de la défense (FED), et ce malgré l'opposition des parlementaires européens[194]. En parallèle, les États européens développent depuis quelques années des politiques nationales dans le domaine de l'IA. Ainsi, en 2017, le Parlement français a confié au mathématicien et député Cédric Villani la mission de rédiger une étude sur l'IA. En 2018, son rapport, intitulé *Donner sens à l'intelligence artificielle*, est rendu public[195]. Dans ce document, la sécurité et la défense sont identifiées comme des secteurs prioritaires du développement de l'IA, aux côtés de la santé, des transports et de l'environnement. Deux ans plus tard, le ministère des Armées publie *L'intelligence artificielle au service de la défense*[196]. Le document indique que : « *Dans cette course* [au développement de l'IA]*, l'enjeu et le rythme sont tels que tout décrochage serait irrémédiable*[197] ». Le vocabulaire utilisé dans le texte fait écho aux discours et initiatives étatsuniens. Dans le sillage de ces prises de position, les autorités françaises soutiennent de nombreux projets recourant à l'IA pour les forces armées. Ces projets font non seulement appel à l'expertise des start-ups mais aussi aux grands fabricants d'armes tels que *Airbus*, *Dassault*, *MBDA*, *Nexter/KNDS* et *Thales*[198].

---

[190] « NATO sharpens technological edge with innovation initiatives », *NATO*, 7 avril 2022 ; « Emerging and Disruptive Technologies », *NATO*, 8 août 2024.

[191] « NATO Innovation Fund closes on EUR 1bn flagship fund », *NATO*, 1er août 2023.

[192] *Ibid*.

[193] LYNCH Lily, « Looking East », *New Left Review*, 9 septembre 2022.

[194] SIMPERE Anne-Sophie, « La prolifération des « robots tueurs » inquiète la communauté internationale », *basta!*, 13 juin 2018.

[195] VILLANI Cédric, « Donner sens à l'intelligence artificielle : pour une stratégie nationale et européenne », *Premier Ministre*, 2018. Ce passage sur la France s'appuie sur : MARTIN Kévin et LIVERSAIN Lucie, « A Winding Road Beforce Scaling-Up? Defense AI in France », *DAIO Study*, 23/17, 2023. Pour une analyse détaillée des conditions sociales d'émergence d'une offre commerciale dans le domaine de l'intelligence artificielle militarisée en France, lire : SURUBARU Alina, « Les données numériques, le nouveau nerf de la guerre ? L'émergence d'un marché militaire de l'Intelligence Artificielle en France », *Réseaux*, n°245, 2024, p. 277-299.

[196] « L'intelligence artificielle au service de la défense : Rapport de la Task Force IA », *Ministère des Armées,* septembre 2019.

[197] *Ibid.*, p. 3.

[198] MARTIN Kévin et LIVERSAIN Lucie, « A Winding Road Beforce Scaling-Up? », *loc. cit.*, p. 6 et 17. Notons au passage que la société aéronautique *Safran* a acquis *Preligens*, un start-up spécialisé dans l'intelligence

Depuis quelques années, l'Allemagne manifeste également un intérêt pour l'usage de l'IA à des fins militaires. En 2020, elle a décidé de consacrer 1,5 milliard EUR à la recherche dans le secteur de la défense. Une partie de l'enveloppe était destinée à l'IA. Elle a aussi soutenu la mise en place d'un écosystème – au cœur duquel on trouve le *Frauhofer Group for Defence and Security*, le *Wehrtechnische Dienstellen*, des sociétés privées ainsi que les universités de la Bundeswehr de Hambourg et Munich – spécialisé dans la recherche sur les applications militaires de l'IA[199]. Il faut ajouter que les conceptions allemandes dans le domaine sont fortement influencées par celles des États-Unis et celles qui circulent au sein de l'OTAN[200]. Cette influence se perçoit, dès 2017, dans des notes conceptuelles, publiées par les forces terrestres, décrivant un champ de bataille futuriste au sein duquel les combattants recourent à l'IA[201]. Le mimétisme s'observe aussi dans les réflexions de l'armée de l'Air allemande (*Luftwaffe*) sur l'IA. On décèle, dans celles-ci, de nombreuses similitudes avec la vision de la Force aérienne des États-Unis (*US Air Force*) sur cette technologie[202].

En 2020, le gouvernement britannique a aussi pris la décision de consacrer une partie du budget dédié à la recherche en matière de défense (1,1 milliard GBP) à des développements dans l'IA[203]. Un an plus tard, il a publié un document intitulé *La Grande-Bretagne mondiale à l'ère de la concurrence* (*Global Britain in a Competitive Age*), qui souligne l'importance de soutenir le développement de l'IA[204]. Il est complété, en 2022, par une *Stratégie de défense sur l'IA* (*Defence Artificial Intelligence Strategy*) du ministère de la Défense[205]. À travers ce document, les forces britanniques s'approprient le discours sur l'« *innovation* » et la « *disruption* » qui s'est imposé aux États-Unis. De la même manière que son homologue étatsunien, le ministère de la Défense œuvre à la mise en place d'un écosystème composé d'institutions qui ont pour mission de soutenir l'innovation – et au sein duquel on trouve le Laboratoire des sciences et technologies de défense (*Defence Science and Technology Laboratory* - DSTL), l'unité *jHub*, la société *QinetiQ*, l'Accélérateur pour la défense et la sécurité (*Defense and Security Accelerator*- DASA) ou encore la *Defense Innovation*

artificielle. BEZAT Jean-Michel et PIQUARD Alexandre, « Preligens-Safran : le mariage d'une start-up d'IA de défense avec un grand groupe industriel », *Le Monde*, 24 juin 2024.

[199] BECKER Sophia, MÖLLING Christian et SCHÜTZ Torben, « Learning together: UK-Germany cooperation on military innovation and the future of warfare », *Hanns Seidel Foundation / The Policy Institute / King's College London*, novembre 2020, p. 4.

[200] *Ibid.*, p. 7. Ce rapport contient un tableau qui liste les principaux acteurs de l'écosystème de l'intelligence artificielle dans le domaine de la défense (*ibid.*, p. 30). Le ministère allemand de la Défense ne cherche pas à développer des systèmes complètement autonomes. *Ibid.*, p. 17.

[201] *Ibid.*, p. 19.

[202] *Ibid.*, p. 20.

[203] Ibid. ; PAYNE Kenneth, « Bright Prospects. Big Challenges. Defence AI in the United Kingdom », *DAIO Study*, 22/04, 2022.

[204] *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, HM Government, CP403, mars 2021, p. 7. Le chancelier de l'Echiquier Jeremy Hunt affirme à cette époque qu'il espère faire du Royaume-Uni la prochaine Silicon Valley. Le développement de l'intelligence artificielle est notamment perçu par lui comme un moyen d'améliorer la productivité britannique. ELLIOTT Larry, « Britain's AI sector expected to get £100 extra funding in budget », *The Guardian*, 4 mars 2024.

[205] « Defence Artificial Intelligence Strategy », *Ministry of Defence,* juin 2022.

Initiative[206]. Comme en France, les projets qui intéressent les forces armées britanniques n'impliquent pas que des start-ups, comme *Ardaga* ou *Rebellion*, mais aussi les grands fabricants d'armes tels que *BAE Systems* et *MBDA*. Les initiatives britanniques dans le secteur de la défense visent aussi à enrôler les chercheurs issus des universités civiles. Notons aussi que *Palantir Technologies* et *Amazon* sont déjà des prestataires de service du ministère de la Défense britannique.

Les initiatives étatsuniennes n'ont cependant pas uniquement eu un impact sur leurs alliés. Depuis 2014, les autorités russes considèrent qu'elles doivent mettre les bouchées doubles dans le domaine de l'IA car leur potentiel dans ce domaine est inférieur à celui des États-Unis et de leurs alliés[207]. L'objectif des Russes est de faire de cette technologie un outil permettant de répondre de manière « *asymétrique* » à la menace que représente l'OTAN. Autrement dit, pour les stratèges russes, l'IA serait utile pour compenser la faiblesse de leurs capacités militaires face à celles des États-Unis et de l'OTAN. C'est dans ce contexte que les Russes se sont servis du conflit syrien comme d'un laboratoire pour leur industrie. En Syrie, les forces russes ont testé 200 équipements incorporant des technologies récentes, dont l'IA[208]. Des systèmes recourant à l'IA – parmi lesquels des robots terrestres – ont aussi été déployés par l'armée russe en Ukraine après le 24 février 2022. Il faut ajouter qu'en août 2024, des officiels russes ont annoncé le lancement d'un nouveau plan de défense dont une partie porte sur le développement d'armes autonomes faisant usage de l'IA[209]. Ne développant pas ces systèmes lui-même, le ministère de la Défense russe encourage les industriels et les universitaires à travailler au développement de ceux-ci.

La Chine n'est pas non plus en reste dans le domaine de l'IA à des fins de défense[210]. Depuis 2014, elle cherche à renforcer son potentiel en la matière en s'appuyant sur des instituts de recherche et des universités civiles. L'intérêt de la Chine est aussi influencé par la politique de défense des États-Unis qu'elle considère comme déstabilisante. Plus précisément, la décision de la Chine est au moins en partie motivée par le lancement de la *Third Offset Strategy* des États-Unis, mentionnée plus haut[211]. Comme dans le cas de la Russie, les développements de la Chine dans le domaine de l'IA militaire doivent surtout être appréhendés comme une réaction aux projets étatsuniens.

En matière de développement de l'IA pour les forces armées, les États-Unis ont donc exercé une influence importante au niveau mondial. Cette influence est notamment la conséquence de l'action délibérée du Pentagone et des alliés étatsuniens, c'est-à-dire les États qui se targuent de représenter l'« *Occident* ». L'OTAN fait aussi pression pour que ses membres développent des moyens dans ce domaine. On a également vu que l'UE cherche à investir dans l'IA à des fins de défense. Enfin, les gouvernements des États alliés et leurs ministères de la Défense tendent à reproduire ce qui se fait aux États-Unis, moyennant

[206] BECKER Sophia, MÖLLING Christian et SCHÜTZ Torben, « Learning together », *loc. cit.,* p. 4.
[207] ZYSK Katarzyna, « High Hopes Amid Hard Realities. Defense AI in Russia », *DAIO Study*, 23/11, 2023.
[208] *Ibid.*, p. 29.
[209] STARCHAK Maxim, « Russian defense plan kicks off separate AI development push », *Defense News*, 16 août 2024.
[210] LEE John, « Overtaking on the Curve », *DAIO Study*, 23/13, 2023.
[211] *Ibid.*, p. 9, 15 et 23.

certaines adaptations censées profiter aux industriels nationaux, dont les grands fabricants de systèmes d'armes[212]. Enfin, la Russie et la Chine ont pris acte des développements aux États-Unis et ont aussi décidé de développer l'IA pour leurs forces armées. Le recours à l'IA à des fins militaires se généralise donc au sein des forces armées à travers le monde, participant ainsi à la pérennisation du sens commun stratégique.

3.4. Une administration sous influence

Les États-Unis, comme berceau de l'IA, continuent d'être le moteur de son expansion. Comme cela a déjà été évoqué, 100 milliards USD ont été investis entre 2021 et 2023 par des fonds de capital-risque dans les sociétés qui proposent du matériel et des programmes de haute technologie au Pentagone[213]. Bien que ce montant soit impressionnant, il ne s'est pas traduit par des contrats qui le sont autant. En effet, lors de l'année fiscale 2023, très peu de start-ups ont signé des contrats de plus de 25 millions USD avec le Pentagone – *Skydio* et *Epirus*, qui ont respectivement signé des contrats de 100 et 66 millions USD pour des drones et un système de défense contre ces mêmes engins avec l'*US Army* font figures d'exceptions. Les résultats des start-ups, par comparaison avec ceux des géants de l'armement, tels que *Lockheed-Martin* ou *Boeing*, qui engrangent des contrats pour des milliards de dollars chaque année, ont donc été relativement modestes. Les start-ups soutenues par les investisseurs en capital-risque ont en fait obtenu moins de 1 % des 411 milliards de contrats conclus par des sociétés privées avec le département de la Défense en 2023[214].

La situation évolue cependant de manière positive pour les entreprises qui développent des applications recourant à l'IA. Le fait que 686 projets en lien avec cette technologie ont été supervisés par le Pentagone en 2024 en atteste[215]. Au total, plus de 1 000 start-ups financées par des fonds de capital-risque sont impliquées dans la production de matériel militaire aux États-Unis[216]. L'engouement pour l'IA a notamment bénéficié à *Palantir*, dont la valeur des actions a cru de 330 % en 2024, faisant passer sa capitalisation boursière à 160 milliards USD[217]. *Anduril Industries* a également connu une importante croissance. La montée en puissance de cette entreprise résulte en partie, comme nous l'avons vu, du soutien apporté par Kathleen Hicks, lorsqu'elle était secrétaire adjointe à la Défense, à

[212] Pour plus d'informations à ce sujet, nous revoyons vers les publications du *Defense AI Observatory*. Ce centre propose des rapports sur les développement de l'intelligence artificielle dans le domaine militaire pour de nombreux États : https://defenseai.eu/english.

[213] SOMERVILLE Heather, « Investors Are Betting on Defense Startups. The Pentagon Isn't », *The Wall Street Journal*, 25 janvier 2024 ; LIPTON Eric, « New Spin on a Revolving Door: Pentagon Officials Turned Venture Capitalist », *loc. cit*.

[214] KAHN Lauren A., « Risky Incrementalism », *loc. cit.,* p. 30. Voir aussi : GONZÁLES Roberto J., *War Virtually*, *op. cit*., p. 68.

[215] COCKBURN Andrew, « The Pentagon's Silicon Valley Problem », *loc. cit*. Frank Bajak évoquait plus de 800 projets pour l'année 2023. BAJAK Frank, « Pentagon's 'Replicator' gambit may speed decisions on lethal autonomy », *loc. cit.*

[216] *Ibid*.

[217] KESTELOO Haye, « Palantir Eyes Major Investment in AI Drone Maker Shield AI at $5 Billion Valuation », *Drone XL.co*, 20 janvier 2025.

l'initiative *Replicator*[218]. Elle découle aussi de l'injection de 200 millions USD dans son capital par le *Founders Fund*, qui appartient à Peter Thiel, et *Andreesen Horowitz*. Du fait de cet apport financier, la valeur en bourse d'*Anduril* a atteint 2 milliards USD en 2020. Une seconde injection de capital de 450 millions USD a ensuite fait grimper cette valeur en bourse à 4,5 milliards USD en 2021. En 2025, la valeur de la société, qui a obtenu de nouveaux financements de fonds de capital-risque, est estimée à 14 milliards USD[219]. Une troisième entreprise, *Shield AI*, a aussi profité de cette conjoncture. La valeur boursière de celle-ci serait passée de 2,8 milliards USD en 2023 à 5 milliards USD en 2025. Notons enfin qu'en février 2025, dans un contexte dans lequel l'entreprise fait des bénéfices moins importants que prévus, *Google* décide de modifier ses règles éthiques et annonce que l'IA doit être utilisée à des fins de sécurité[220].

Les intérêts des entreprises qui opèrent dans le champ de l'IA sont par ailleurs bien représentés au sein de la nouvelle administration Trump. Plusieurs des membres de son équipe sont proches des milliardaires de la Silicon Valley[221]. C'est par exemple le cas d'Elon Musk et du vice-président J.D. Vance. Celui-ci était à la tête du fonds de capital-risque *Narya Capital* – un nom issu du *Seigneur des anneaux*. Lors des élections, J.D. Vance a été soutenu par le milliardaire Peter Thiel, un des fondateurs de *Palantir*. Le nouveau secrétaire adjoint à la Défense nommé par Donald Trump est le milliardaire Stephen A. Feinberg. Il a été membre de *Cerberus Capital* Management, une société qui a acquis la start-up militaire *Stratolaunch*. Dans le contexte de ces nominations, on ne sera guère surpris de la décision, adoptée en janvier 2025, d'augmenter la dotation de la *Defense Innovation Unit* du Pentagone[222]. En mars 2025, Donald Trump a aussi décidé de nommer Michael Obadal sous-secrétaire de l'Armée américaine[223]. Michael Obadal est un ancien officier de forces spéciales qui a ensuite travaillé pour le compte d'*Anduril*. En tant que sous-secrétaire des forces terrestres, il participera à la gestion d'un budget de 185 milliards USD, notamment destiné à l'acquisition de matériel.

Les entrepreneurs de la Silicon Valley sont donc en train de placer leurs pions au sein du département de la Défense. Ils cherchent, au sein de celui-ci, à faire évoluer la politique d'acquisition des armes dans le sens de son assouplissement[224]. La mise en place d'un écosystème destiné à soutenir l'innovation au sein de Pentagone s'est en effet accompagnée de l'adoption de procédures de financement atypiques. Grâce à celles-ci, les forces armées peuvent verser rapidement de l'argent à des sociétés afin d'acquérir des technologies dites « *off-the-shelf* », c'est-à-dire déjà disponibles sur le marché civil. Ces

---

[218] KLARE Michael T., « Competition for Defense Contract May Drive Divides Within Trump Circle », *loc. cit*.

[219] CORBYN Zoë, « Move fast, kill things: the tech startups trying to reinvent defense with Silicon Valley values », *The Guardian*, 29 mars 2025.

[220] KOLLEWE Julia, « Google owner drops promise not to use AI for weapons », *The Guardian*, 5 février 2025.

[221] *Ibid*.

[222] ALBON Courtney, « Trump's Pentagon should expand innovation hub, tech panel says », *Defense News*, 16 janvier 2025.

[223] HARPER Jon, « Trump nominates Anduril executive, former special operations officer to be Army undersecretary », *Defensescoop*, 11 mars 2025.

[224] MARSHALL Shana, « The Military-Industrial Venture Complex », *loc. cit*.

nouvelles procédures, qui font l'objet d'un contrôle limité, sont décrites comme plus économiques par le secteur de la haute technologie. Les grands fabricants d'armes conventionnelles – tels que BAE, *Lockheed Martin* ou RTX (anciennement nommée *Raytheon*) – ne bénéficient pas de ces procédures. Ils demandent en compensation que les autorités acceptent que des clients étrangers puissent participer à la phase de recherche et de développement des nouveaux matériels qui sont notamment destinés aux forces étatsuniennes. Les clients envisagés pour financer le développement des équipements pourraient entre autres être des dictatures du Moyen-Orient. De tels financements étrangers, par des États qui ont la réputation de ne pas respecter les normes internationales en matière d'usage de la force, renforceraient un peu plus encore la dépendance des grands fabricants d'armes à leur égard. Récemment, l'industrie de la haute technologie a aussi préconisé que le Pentagone la soutienne financièrement pour développer des équipements avant même que les militaires n'en aient fait la demande[225].

De fait, les entrepreneurs de la Silicon Valley ont clairement l'intention de s'imposer sur le marché de l'armement. Et ce, à tel point, que l'on peut se demander si cela les mettra en compétition avec les producteurs traditionnels – tels que *Boeing*, *Lockheed Martin* ou encore *Northrop Grumman*. À ce propos, on se souviendra du message d'Elon Musk, affirmant qu'il était « *idiot* » de continuer à fabriquer des appareils comme le *F-35*, piloté par un humain[226]. Pour Musk il serait, en effet, plus avisé d'acquérir des drones opérant, grâce à l'IA, en essaim. Ces prises de parti en faveur de l'intégration des nouvelles technologies dans le domaine de l'armement ne sont pas sans inquiéter les plus gros fabricants. Il est également possible que le budget du département de la Défense soit, une fois encore, augmenté de manière à satisfaire l'ensemble du complexe militaro-industriel. On retrouve en tous les cas ce souhait dans les propos d'un cadre supérieur de *Lockheed Martin*, Jay Malave, lorsqu'il dit espérer que la recherche d'efficacité au Pentagone aille de pair avec une augmentation des budgets[227]. L'annonce de Donald Trump selon laquelle *Boeing* pourrait fabriquer un appareil *F-47* qui puisse opérer aux côtés des drones va d'ailleurs dans ce sens. *Boeing* devrait recevoir 20 milliards USD rien que pour le développement de cette nouvelle machine[228]. Le président Donald Trump a aussi exigé la relance de projets de défense antimissiles en janvier 2025[229]. En référence au « *dôme de fer* » israélien, il évoqua la création d'un « *dôme doré* » (« *Golden Dome* »). Les capacités du système étatsunien seraient bien plus développées que celles du système israélien. Le projet, qui risque d'être dispendieux, pourrait bénéficier à *Anduril*, *Palantir*, *SpaceX* mais aussi à *Lockheed Martin*.

[225] TUCKER Patrick, « Are AI defense firms about to eat the Pentagon? », *Defense One*, 15 décembre 2024.

[226] HAMBLING David, « Elon Musk Calls F-35 Builders 'Idiots', Favors Drone Swarms », *Forbes*, 26 novembre 2024.

[227] HARTUNG William, « Will Trump Actually Rein In War, Inc.? », *Responsible Statecraft*, 6 janvier 2025.

[228] « Trump awards Boeing contract to build next-generation US fighter jet », *The Guardian*, 21 mars 2025.

[229] HOLMES Frank, « SpaceX, Palantir And Anduril Lead The Race To Build Trump's Golden Dome », *Forbes*, 28 avril 2025.

Afin de donner sens à cette situation, il est utile de se référer aux travaux d'Anthony Galluzzo[230]. Selon lui, pour attirer les investissements publics, les start-ups ont développé un argumentaire qui repose sur la dénonciation des grands groupes industriels, qu'elles accusent d'être des bureaucraties incapables d'innover[231]. En réalité, comme l'écrit à ce propos Anthony Galluzzo :

> « *Il existe* […] *une complémentarité des rôles joués par les petites et les grandes entreprises dans le développement d'un marché. Des start-ups se montent rapidement pour occuper ce qui est encore une niche. Elles y expérimentent et font peu à peu émerger des standards. Lorsque la demande atteint un niveau suffisamment élevé, il devient possible, pour l'exploiter, de mettre en place un vaste système de production et de distribution que seules les très grandes entreprises sont capables de déployer*[232] ».

Les déclarations du président étatsunien concernant un budget de la défense qui devrait avoisiner les 1 000 milliards USD, pourraient aussi signaler son désir de contenter l'ensemble du complexe militaro-industriel[233]. Si l'on suit ce raisonnement, l'économie des start-ups ne serait peut-être pas tant « *disruptive* » qu'elles veulent le faire croire. Les start-ups contribueraient plutôt à assurer la continuité d'un secteur industriel en développant des produits pour moderniser des équipements militaires dont les modèles initiaux ont vu le jour il y a des années, voire des dizaines d'années – comme les drones, les véhicules blindés ou les chasseurs-bombardiers qui pourront être dotés de fournitures électroniques employant l'IA. Pour le dire autrement, le succès de l'IA dépendrait, au moins en partie, du maintien de ces mêmes moyens anciens dans les forces armées. Si cela vient à se vérifier sur le long terme, cela signifierait que les start-ups participent tout simplement à la fabrication de ce que la chercheuse Mary Kaldor avait naguère nommé l'« *arsenal baroque*[234] ». Selon elle, par l'ajout ponctuel de composants, notamment électroniques, destinés à l'améliorer marginalement, cet arsenal parvenait à réactiver un imaginaire d'efficacité et à se pérenniser. Bien entendu, en contribuant à perpétuer l'arsenal baroque, les start-ups contribuent automatiquement à perpétuer la possibilité de faire des guerres[235].

Sans aucun doute, les liens entre l'administration Trump et l'industrie contribueront encore à renforcer la position de cette dernière et à normaliser le recours à ses produits. De manière plus générale, il apparaît que pour les entrepreneurs de la Silicon Valley, la guerre est avant tout perçue comme un problème qui leur permet de vendre des solutions techniques. Pour ces acteurs, la guerre est donc un problème rentable, et pas seulement au

---

[230] GALLUZZO Anthony, *Le mythe de l'entrepreneur*., *op. cit.*

[231] *Ibid.*, p. 62.

[232] *Ibid.*, p. 69.

[233] MEHTA Aaron, « A $1 trillion defense budget? Trump, Hegseth say it's happening », *Breaking Defense*, 7 avril 2025.

[234] KALDOR Mary, *The Baroque Arsenal*, Londres, Andre Deutsch, 1982.

[235] Ce que nous avons appelé, le « *sens commun stratégique* ». WASINSKI Christophe, *Rendre la guerre possible. La construction du sens commun stratégique*, Bruxelles, Peter Lang, 2008.

niveau national[236]. L'industrie de l'IA cherche aussi, en effet, à exporter ses produits. Palmer Luckey, le fondateur d'*Anduril*, l'a d'ailleurs exprimé sans ambiguïté en mars 2025 : « *Mon point de vue est que les États-Unis ne devraient pas être la police du monde, nous devrions être le magasin d'armes de nos alliés*[237] ».

[236] PRÉVOST Thibault, *Les prophètes de l'IA., op. cit*., p. 165. Voir aussi : PAJOT Benjamin, *Le solutionnisme technologique : vrais problèmes, fausses solutions ?*, *IFRI*, mars 2025.

[237] MARISSAL Pierric, « Anduril : Qui est Palmer Luckey, ce post-adolescent qui veut faire des États-Unis le magasin d'armes du monde ? », *L'Humanité*, 6 avril 2025.

Conclusion : pérenniser la guerre à travers les nouvelles technologies

Ce rapport a exposé le processus par lequel le développement de l'IA s'est normalisé dans le champ militaire. Il a d'abord souligné le rôle joué par les services de renseignement étatsuniens qui ont fait entrer des start-ups dans le champ de la sécurité. Ensuite, il a mis en exergue le fait qu'avec la « *guerre contre le terrorisme* » les start-ups spécialisées dans le domaine du renseignement sont devenues des clientes du Pentagone. De fil en aiguille, le Pentagone est même devenu un relai des intérêts des start-ups. L'IA a par ailleurs été repensée de manière à devenir un équipement adapté aux conflits interétatiques. Dans sa troisième et dernière partie, ce rapport a abordé la circulation transnationale de l'IA. Dans celle-ci, il a pointé le rôle de laboratoire joué par l'Ukraine et la Palestine et abordé la diffusion de l'IA dans les armées contemporaines.

Ce rapport a aussi démontré que la normalisation du recours à l'IA est un phénomène interpellant. Cette technologie n'est pas parvenue à faire pencher la balance d'une manière décisive dans le conflit russo-ukrainien, un conflit qui s'est transformé en une terrible guerre d'usure. L'usage par les forces israéliennes de l'IA en Palestine pose, quant à elle, de sérieuses questions éthiques et juridiques. Contrairement à ce qu'affirme l'industrie, les systèmes recourant à l'IA ne sont pas des armes magiques – et, n'en déplaise aux responsables des start-ups, la guerre réelle n'a rien à voir avec l'*heroic fantasy*[238]. Au surplus, l'idée que la guerre puisse être menée sans soldats, sans champs de bataille, voire sans morts, grâce à des équipements « *innovants* » relève avant tout du fantasme[239]. Les discours mirifiques sur les capacités de ces équipements – au même titre, il est vrai, que ceux qui font les louanges d'équipements plus anciens – ont donc aussi pour effet d'occulter l'essentiel, à savoir la nécessité de penser des solutions politiques et diplomatiques aux conflits et crises contemporains[240]. Plus grave encore, les discours dithyrambiques sur l'IA risquent de créer une confiance illusoire en la capacité des armes dotées de cette technologie à régler les conflits[241]. En fait, l'expansion du secteur de l'IA semble davantage liée aux financements des fonds de capital-risque qu'aux capacités réelles d'un matériel

[238] À propos des « *armes magiques* », voir : TLUSTY Ann B., « Invincible Blades and Invulnerable Bodies: Weapons Magic in Early-Modern Germany », *European Review of History*, vol. 22, n°4, 2015, p. 658-679.

[239] GONZÁLES Roberto J., *War Virtually, op. cit.*, p. 1.

[240] PRÉVOST Thibault, *Les prophètes de l'IA, op. cit*.

[241] LUSHENKO Paul et CARTER Keith, « A new military-industrial complex: How tech bros are hyping AI's role in war », *The Bulletin of Atomic Scientists*, 7 octobre 2023. L'inexpérience de cette industrie est notamment illustrée par l'histoire de la start-up *Rebellion* : BREWSTER Thomas, EMERSON Sarah et JEANS David, « How Rebellion Defense, The $1 Billion Military AI Startup Hyped By Silicon Valley, Wound Up In A NooseDive », *Forbes*, 22 décembre 2023.

produit dans l'urgence et assez peu testé[242]. Il est impératif de garder à l'esprit que les discours qui font l'apologie de l'IA sont tenus par des individus qui n'ont bien souvent aucune expérience de la guerre, espèrent décrocher de juteux contrats financés par de l'argent public et produisent des représentations inquiétantes du monde – notamment en se focalisant sur le rôle de la Chine – afin de justifier leur activité[243]. En définitive, le risque principal de l'IA dans les arsenaux est qu'elle contribue à pérenniser la capacité des États à faire la guerre.

Le discours de l'industrie a certes fait l'objet de critiques par des acteurs et initiatives issus de la société civile – tels que la *Campaign to Stop Killer Robots*, *Code Pink*, le *Bureau of Investigative Journalism* et l'*International Committee for Robot Arms Control* (ICRAC) – qui mettent en exergue les risques liés à l'usage de l'IA par les forces armées[244]. Le *Future of Life Institute* et Stuart Russel, un expert de l'IA, ont aussi réalisé une vidéo intitulée « *Slaughterbots* » en 2017, qui a popularisé les dangers de la militarisation de l'IA[245]. Jack Poulson un ancien professeur de l'Université de Stanford qui a travaillé pour *Google* jusqu'en 2016, a quant à lui lancé le site « *Tech Inquiry* », dont l'objectif est d'informer le public sur les activités de l'industrie[246]. Par ailleurs, en 2023, un *Airspace Tribunal* s'est réuni à Londres, Sidney, Toronto et Berlin[247]. Lors de celui-ci, l'usage de l'IA fut également critiqué. Enfin, depuis 2014, des négociations ont lieu à Genève à propos des armes autonomes, dans le cadre de la Convention sur certaines armes classiques (CCAC). Même si l'adoption d'un traité d'interdiction des armes autonomes est loin de faire l'unanimité au niveau international, ces négociations ont, *a minima*, le mérite de contribuer à attirer l'attention sur le risque que représente la militarisation de l'IA.

[242] CORBYN Zoë, « Move fast, kill things », *loc. cit.*

[243] MHALLA Asma, *Technopolitique, op. cit.*, p. 201.

[244] WEBER Jutta, « Autonomous drone swarms and the contested imaginaries of artificial intelligence », *Digital War*, vol. 5, 2024, p. 146-149.

[245] « Sci-Fi Short Film "Slaughterbots" | DUST », *YouTube*, 17 octobre 2019.

[246] « Tech Inquiry simplifies public records analysis for the surveillance and weapons industries », *Tech Industry*, consulté le 17 avril 2025.

[247] Pour plus d'informations à propos de ce tribunal, voir : https://airspacetribunal.org/.

LES RAPPORTS DU GRIP

2021/4 **Résumé du SIPRI Yearbook 2021 - Armements, désarmement et sécurité internationale,** Traduction GRIP, 20 p., gratuit

2021/5 **Dépenses militaires, production et transferts d'armes. Compendium 2020**, SIPRI/GRIP, 48 p. , 10 €

2021/6 **Robots tueurs: Le début de la fin?,** Stan Brabant, 28 p., 10 €.

2021/7 **Est de la RDC : le paradoxe d'un état de siège et d'une insécurité grandissante,** Adolphe Agenonga Chober, 28 p. , 10 €

2022/1 **Industries de défense saoudienne et émiratie : défis semblables, évolutions divergentes,** Georges Berghezan, 28 p., 10 €

2022/2 **Résumé du SIPRI Yearbook 2022 – Armements, désarmement et sécurité internationale,** Traduction GRIP, 32 p., 10 €

2022/3 **Dépenses militaires, production et transferts d'armes,** Compendium 2020, GRIP/SIPRI, 52 p. , 10 €

2022/4 **Si importantes qu'elles disparaissent. L'invisibilité des femmes combattantes dans les programmes DDR,** Clémence Buchet-Couzy**,** 28 p., 10 €

2022/5 **Un programme en eaux troubles-Incertitudes autour des sous-marins nucléaires australiens,** Maïté Bol, 40 p., 10 €

2023/1 **La Turquie, nouveau leader de non-alignés?,** Georges Berghezen, 60p., 10 €

2023/2 **Résumé du SIPRI Yearbook 2023 Armements, désarmement et sécurité internationale,** Traduction GRIP, 24p., 10 €

2023/3 **Dépenses militaires, production et transferts d'armes,** Compendium 2023, SIPRI/GRIP, 52 p., 1

2023/4 **Faut-il acheter le F-35 pour participer au partage nucléaire dans l'OTAN,** Samuel Longuet, 50 p., 10 €

2024-1 **Hors OTAN, mais partenaires: Bosnie-Herzégovine, Serbie, Kosovo**, Georges Berghezan, 36 p., 10 €

2024-2 **L'intégration des enjeux climato-environnementaux dans les doctrines et stratégies militaites: état des lieux et pistes de réflexion**, Maïté Bol, 120 p., 10 €

2024-3 **Hausse des achats d'armement au Viêt Nam et en Thaïlande**, Anne Xuan Nguyen, 36 p., 10 €

2024-4 **Puissance aérienne et gouvernement du ciel en Afrique. Vivre dans les fantasmes sécuritaires d'Autrui**, Christophe Wasinski, 28 p., 10 €

2024-5 **Vendre des armes à Taïwan sans régler «la question de Formose». Les ambigüités états-uniennes et européennes**, Samuel Longuet , 62p., 10 €

2024/6 **L'influence de la Chine au Moyen-Orient. Entre avancées notables et limites persistantes,** Thierry Kellner et Nadine Loutfi, 32p., 10 €

2024/7 **Dépenses militaires, production et transferts d'armes** – Compendium 2024, SIPRI, Traduction GRIP, 54 p., 10 €

2025/1 **Est de la RDC: inflation des prix du cacao, émergence des réseaux de contrebande et de criminalité** – Adolphe Agenonga Chober, 34p., 10 €

2025/2 **Trafics d'armes des États-Unis vers le Mexique** – Georges Berghezen, 40p., 10€

Pour commander votre exemplaire de ce Rapport du GRIP, rendez-vous sur www.grip.org / publications / rapports (10 € frais de port inclus)

L'imaginaire« start-up » de la guerre : L'intelligence artificielle et le réenchantement de la défense de l'« Occident »

Le recours à l'intelligence artificielle (IA) par les forces armées fait craindre des dérives, notamment en ce qui concerne les risques découlant de biais algorithmiques et à propos de la dilution de la responsabilité humaine dans les décisions d'emploi de la force. En dépit de cela, la recherche, le développement et l'utilisation de l'IA à des fins militaires se normalise.

Ce rapport analyse le processus par lequel cette normalisation a eu lieu. Dans une première partie, il aborde le rôle joué par les services de renseignement, en particulier dans le cadre de la « guerre contre le terrorisme », dans ce processus. Toujours dans ce contexte, il se penche ensuite sur les rapprochements entre les start-ups et le Pentagone. Il souligne, dans cette partie, à quel point le Pentagone est devenu, de fait, un relais de l'industrie. Au surplus, il montre que l'IA est également conçue comme un moyen adapté aux conflits interétatiques. La troisième et dernière partie aborde la circulation transnationale de l'IA, un phénomène en grande partie influencé par les États-Unis. Sont entre autres évoqués dans celle-ci les usages de l'IA en Ukraine et en Palestine, et sa diffusion dans les armées alliées des États-Unis. Cette partie propose donne aussi un aperçu des évolutions étatsuniennes récentes, où l'on assiste à un resserrement des liens entre les entreprises et le Pentagone depuis l'investiture de Donald Trump en 2025.

De manière générale, ce rapport insiste sur les enjeux économiques qui sont à l'origine du développement de l'IA. Il met aussi en exergue le fait que ces enjeux économiques jouent un rôle déterminant dans la construction d'un imaginaire militariste qui contribue à la re-légitimation de la guerre au nom de la protection de l'« Occident ».

Professeur en sciences politiques (relations internationales) à l'Université libre de Bruxelles. Il est membre du centre Recherche et études en politique internationale (Repi) et chercheur associé au GRIP. Ses recherches portent sur les questions militaires et de sécurité.

GRIP

LES RAPPORTS DU GRIP
2025/3

ISBN : 978-2-87291-251-3