Le sentiment de sécurité par le recours dissuasif des armes dissuasion militaire

Jacques Fontanel

Le sentiment de sécurité par le recours dissuasif des armes

dissuasion militaire

Jacques Fontanel

La sécurité, un bien collectif économique et humain indispensable
Université Grenoble Alpes, CESICE, ILERI
Grenoble, Paris, 2017

Résumé : Les dépenses militaires et la production d'armes répondent à un sentiment de sécurité des Etats, face aux actions supposément agressive des autres Etats. Elles sont, la plupart du temps, jugées dissuasives, mais elles peuvent aussi être augmentées pour faire face à une volonté de domination sur d'autres pays ou alliances. D'un point de vue économique, elles font l'objet de trois questions principales concernant le choix entre le beurre et le canon, à la détermination de la force d'un pays obtenue pour un euro dépensé (bang for a buck) selon les stratégies choisies, notamment nucléaires, et le développement plus sournois des cyber armes et la cyber guerre, souvent instruits hors du camp militaire, mais menaçante aussi pour la défense nationale.

Military expenditure and arms production respond to a sense of security on the part of states in the face of supposedly aggressive actions by other states. They are, in most cases, considered to be a deterrent, but they can also be increased in response to a desire for domination over other countries or alliances. From an economic point of view, they are the subject of three main issues concerning the choice between butter and barrel, the determination of the strength of a country obtained for a euro spent (bang for a buck) according to the strategies chosen, notably nuclear, and the more devious development of cyber weapons and cyber warfare, often educated outside the military camp, but also threatening national defence.

Sécurité nationale, dissuasion militaire, coût d'opportunité des dépenses militaires, coût des stratégies, cyber armes, cyber guerres.

National security, military deterrence, opportunity cost of military spending, cost of strategies, cyber weapons, cyber wars.

La question de l'armement soulève trois interrogations principales :

- Le choix du « beurre ou du canon » est particulièrement important, notamment pour les pays en développement[1]. Il renvoie à la fois à la question du niveau optimal des dépenses de défense et à celle du désarmement.
- La détermination de la force obtenue pour un euro dépensé (« Bang for a buck »[2]) est une question économique impossible à résoudre. L'arme nucléaire est monopolisée par cinq puissances militaires, qui empêchent les autres pays d'en disposer, sans vouloir elles-mêmes y renoncer.
- L'émergence des cyber armes et de la « cyber guerre », souvent hors du champ particulier du secteur militaire, constitue une menace dont l'importance n'est pas encore bien estimée.

Les dépenses militaires, fardeau ou facteur de sécurité et de développement économique ?

Pendant presque toute l'histoire de l'humanité, la question « du beurre ou du canon » n'a pas été posée en termes d'effets d'éviction réciproques, contrairement à cette proposition à laquelle adhèrent de nombreux individus ou groupes organisés. La guerre avait d'ailleurs une fonction sociale, la prédation, celle des butins, celle des hommes réduits à l'esclavage, celle des occupations de sols qui permettaient de disposer de matières premières à bon marché, celle des langues interdites ou celles des citoyennetés disparues ou englouties. Aujourd'hui, l'armée n'appartient plus à un Ministère de la guerre, mais à un Ministère de la Défense nationale. Il s'agit donc de se protéger face à des voisins envieux ou guerriers pour de multiples raisons, lesquelles ne se conjuguent pas toujours directement avec les valeurs économiques. La disponibilité d'une force militaire aux ordres d'une stratégie bien établie a normalement pour objectif de dissuader les autres Etats d'engager des actions violentes à l'encontre du pays qui l'a construite. Les guerres entre Etats ont des effets macroéconomiques considérables, non seulement par les destructions d'hommes et de matériels qu'elles supposent, mais aussi par les coûts d'opportunité qu'elles infligent aux belligérants en termes de ressources humaines, d'investissement ou de « welfare » : si la construction, la permanence et l'utilisation des forces armées engendrent parfois, selon les propos de Schumpeter, des destructions positives, elles représentent toujours un coût, lequel est aussi susceptible de réduire le potentiel de développement d'un pays.

---

[1] Fontanel, J. (1990), The economic effects of military expenditure in Third World Countries, Journal of Peace

[2] Cette expression américaine pourrait être traduite en français comme un « boum » pour un biffeton. Boum, représente l'efficacité explosive de l'arme, le « buck » (daim en anglais) représente, en jargon, un billet de un dollar de couleur daim.

En 2016, les dépenses militaires des Etats-Unis sont plus élevées en dollars constants que les dépenses moyennes annuelles engagées pendant la guerre froide[3]. Elles ont de nouveau baissé depuis le départ des troupes américaines d'Afghanistan et d'Irak de 741 à 585 milliards de dollars de 2010 à 2015. Pourquoi les démocraties s'engagent-elles dans des guerres qu'elles ne gagnent pourtant jamais à long terme, et pourquoi, à chaque période électorale, une demande d'augmentation des dépenses militaires réapparaît-elle ? Les Etats-Unis croient fondamentalement dans la puissance des armes, ce pays veut la primauté dans ce domaine, de façon à renforcer son rôle de leadership économique, technologique et culturel mondial. Dans ce contexte, face aux BRICS en devenir, aux extrémismes, à l'existence de « rogue states » et à l'instabilité de nombreux Etats fragilisés, l'escalade de l'armement reste une constante du système politique et économique américain[4]. Le Pentagone achète des systèmes d'armes de plus en plus coûteux, l'avion de combat F-35 coûtera 400 milliards de dollars en 20 ans, et plus de 1400 milliards de dollars durant toute sa vie pour la maintenance. Les 12 sous-marins lanceurs de missiles balistiques coûteront 60 milliards de dollars. L'armée souhaiterait disposer de 490.000 hommes, mais elle doit travailler avec 420.000 personnes. Les ventes internationales d'armes (70 milliards de dollars en 2014) permettent de rentabiliser une partie de l'armement, mais celles-ci se retournent bien souvent contre ceux qui les ont produites. Si les Etats-Unis sont toujours le plus important exportateur d'armes au monde, la Russie développe ses liens avec plus de 56 pays par le canal des ventes de systèmes d'armement. En 2015, les ventes d'armes en Russie ont explosé, elles représentent 15,5 milliards de dollars d'exportation, ce qui fait de ce pays le deuxième exportateur d'armes au monde derrière les Etats-Unis[5]. L'industrie d'armement dispose d'un portefeuille de commandes de 56 milliards de dollars à destination de l'Inde, la Chine, le Vietnam, l'Irak et l'Algérie. Elles concernent principalement l'évolution de matériels militaires déjà[6] disponibles dans nombre d'armées étrangères, mais aussi des armes bénéficiant de nouvelles technologies adaptées à la lutte antiterroriste. La Russie vend aussi bien à l'Azerbaïdjan qu'à l'Arménie (pourtant en conflit armé dans le Haut Karabagh) qu'à la Chine (notamment pour les appareils disposant de nouvelles technologies), un pays partenaire du groupement BRICS.

En règle générale, l'évolution des dépenses militaires met en évidence l'essor ou la réduction des tensions entre les pays. Cependant, la disponibilité

[3] **Kaufman, R.** (2015), Economists for Peace & Security, Newsletter, Volume 27, Issue 1, March 2015. **Cornetta C.** (2015), Economists for Peace & Security, Newsletter, Volume 27, Issue 1, March 2015.

[4] **Hartung, W.** (2015), Economists for Peace & Security, Newsletter, Volume 27, Issue 1, March 2015.

[5] Le courrier de la Russie (2016), Mistral gagnant : les exportations d'armes russes explosent, 31 mars. http://www.lecourrierderussie.com/economie/2016/03/mistral-perdant-ventes-armes-russes/

[6] Fontanel, J. ? Fontanel, M. (2013), Les BRICS, un concept statistique devenu une force politico-économique mondiale organisée,avec Maxence Fontanel, in « Basculement économique & géopolitique du monde. Poids et diversité des pays émergents » (Mohammed Matmati Ed.). L'Harmattan, Paris.

des armes a un double sens, c'est à la fois un moyen de défense et de dissuasion face à une attaque d'un ou de plusieurs autres pays, mais c'est aussi, entre autres, un facteur de pouvoir destiné à contraindre, par la menace ou la force, un adversaire. Les chiffres fournis par les Etats concernant leurs dépenses relatives à la sécurité internationale ne sont pas toujours homogènes et les comparaisons font l'objet de nombreuses hypothèses restrictives[7]. Il n'existe pas, de manière générale, de relation linéaire entre les dépenses et la capacité. Cette capacité dépendra aussi de la manière dont l'argent est utilisé. Au sein de l'Union européenne, des instruments comme la mise en commun et le partage de matériel militaire, ou le développement et la production en commun sont susceptibles de réduire les coûts, sans diminuer la capacité de d'intervention, sauf si la règle du « juste retour » impose des contraintes économiques spécifiques. Ainsi, plusieurs experts s'interrogent aujourd'hui sur la place stratégique de l'arme nucléaire. Après l'effondrement de l'URSS, le gouvernement des Etats-Unis a considérablement réduit le programme militaire nucléaire (arrêt des essais nucléaires, arrêt de la conception et de la fabrication d'armes nucléaires, réduction de moitié du stock des armes nucléaires, fermeture de sites, action en vue de limiter la prolifération de ces armes, reconnaissance et compensations financières pour les citoyens américains, japonais et des îles Marshall exposés aux radiations nucléaires militaires et aide technologique et financière pour éliminer les armes des pays faisant partie de l'ex URSS). Cependant, en 2010, un nouveau soutien au nucléaire militaire a été acté, en vue à la fois de remplacer les installations trop anciennes et pour maintenir en condition le complexe militaire et scientifique du secteur. Les Etats-Unis financent aujourd'hui le nucléaire militaire à un niveau proche des dépenses militaires totales de la France. De même, la prolifération des armes de destruction massive et de leurs missiles balistiques constitue une menace croissante pour la paix et la sécurité au niveau international. Malgré les traités internationaux et l'existence de mécanismes de contrôle des exportations quelques Etats cherchent toujours à développer ou à acquérir des matériels chimiques, biologiques, radiologiques ou fissiles et leurs vecteurs. Si les pays potentiellement cibles ne trouvent pas les moyens de faire face à la production et à l'utilisation de ces armes par les Etats voyous (rogue states) ou par le terrorisme, l'importance de leurs budgets militaires ne leur permettra pas de faire face à cette menace.

La non-prolifération, le désarmement et la maîtrise des armements peuvent apporter une contribution capitale à la lutte contre le terrorisme à

[7] Cars, H.C., Fontanel, J. (1987), Military Expenditure Comparisons, in "Peace, Defence and Economic Analysis", Editors, C. Schmidt, F. Blackhaby,The International Economic Association, Mac Millan, London, 1987 (12 pages). Fontanel, J. (2015), La base des données des dépenses militaires recueillie par l'Organisation des Nations Unies : origine et évolution. *United Nations Standardized Instrument for Reporting Military Expenditure (*2015) In Paix et sécurité européenne et internationale, http://revel.unice.fr/psei/ , Malizard, J., Guilhaudis, J-F. (2015), Dépenses de défense et de sécurité, PSEI, http://economie-defense.fr/depenses-de-defense-et-de-securite-julien-malizard-j-f-guilhaudis/

l'échelle mondiale en réduisant le risque que des acteurs non gouvernementaux parviennent à se procurer des armes de destruction massive, des matières radioactives et des vecteurs. Cependant, les évolutions majeures du contexte conflictuel mondial conduisent à rendre les stratégies de plus en plus difficiles à organiser, du fait même de l'existence des réseaux sociaux, soucieux de mettre en évidence toutes les situations de conflits militaires avec leurs lots de sauvagerie et de violence, alors même que la non létalité des armes est aujourd'hui recherchée, notamment dans les conflits et émeutes civiles. Aujourd'hui, les combattants et les sont de plus en plus entremêlés, ce qui réduit cette distinction, notamment dans les combats en zone urbanisée.

Cependant, sur le moyen terme, les budgets militaires en baisse réduisent l'efficacité des opérations militaires, comme l'ont démontré les lacunes, en termes de matériels (drones, ravitaillement en vol, bombes de précision...), des moyens disponibles lors de la guerre aérienne contre la Libye**.** En revanche, l'industrie militaire chinoise est montée en puissance, elle a enchaîné les percées technologiques dans les drones de combat, les avions furtifs (J20 et J31), systèmes antimissiles ou les technologies des porte-avions. L'importance de l'effort militaire national dépend de l'importance des dépenses militaires, mais aussi de nombreux autres facteurs, comme l'existence d'un complexe militaro-industriel, le renforcement des forces militaires pour contrôler les forces internes de l'opposition politique, l'essor ou le maintien d'une recherche-développement publique, la mise en place déguisée d'une politique industrielle par le canal du financement d'une recherche-développement à intérêt dual (civil et militaire) ou encore l'existence d'effets d'inertie touchant à l'action territoriale ou sectorielle de l'économie[8]. Selon le patron d'ArianeSpace, le projet spatial SpaceX bénéficie parfaitement de cet engagement (obole ?) militaire. En fait, les contrats militaires obtenus auprès du gouvernement américain sont fixés sur la base de prix 30 % supérieurs à ceux que la même firme offre les marchés internationaux. Grâce à cette forme de subvention implicite qui profite à la recherche fondamentale, à la recherche appliquée et au développement du la firme, elle obtient un avantage économique qui risque de s'avérer mortifère pour tous les autres opérateurs du secteur sans soutien gouvernemental ou européen. « Si aux Etats-Unis, des milliardaires s'intéressent au spatial, c'est qu'ils ont en point de

[8] Fontanel, J., Samson, I. (2008), The economic determinants of military expenditures, in « War, Peace and Security », Contributions to Conflict Management, Peace Economics, and Development, Volume 6, edited by Jacques Fontanel and Manas Chatterji - London, Elsevier/Emerald, London, . Fontanel, J., & Smith, R. (1991). A European defence union?. Economic Policy,13(3), 393-425. Fontanel, J, Hébert, J-P. (1997), The French policy of "Grandeur", Defence and Peace Economics, Vol. 8 (1), pp. 37-55. Coulomb, F., Fontanel, J. (2005), An economic interpretation of French military expenditure, Defence and Peace Economics, 16(4), 297-315. Malizard, J. (2013), Opportunity costs of Defence : an Evaluation in the case of France, Defence and Peace Economics 26(3), pp. 247-259. Fontanel, J., Ward, M. (1993), Military Expenditures, Armaments and Disarmament, Defence Economics, Vol. 4, (16 pages).

mire le marché juteux des contrats militaires et de la NASA pour développer leurs activités »[9].

Les dépenses militaires ont aussi des effets contrastés sur l'économie nationale[10]. Les dépenses militaires d'investissement pour les pays producteurs d'armement ont plutôt des effets positifs à court terme, contrairement aux autres coûts opérationnels des dépenses militaires[11].

La sécurité n'est pas mesurable, elle dépend de la perception nationale des menaces, de l'évolution du processus de globalisation, des négociations et de la nature des alliances internationales, du niveau de solidarité économique et social, mais aussi des tensions politiques, religieuses et idéologiques[12]. Trop de recherche de sécurité par les dépenses adaptées peut conduire à une crise économique interne. La coopération est nécessaire pour les groupes humains et les modèles de théorie des jeux prouvent que les systèmes coopératifs sont généralement plus efficaces que ceux qui valorisent la seule compétition, notamment parce que les accords internationaux réduisent l'autonomie des Etats.

L'URSS a considérablement fragilisé son économie nationale en considérant que la protection de son territoire et de son système d'économie planifiée impliquait une priorité indiscutable, quel qu'en soit le coût. Le système socialiste a sans doute au moins autant souffert de cette militarisation excessive que du fonctionnement normal de son économie. Cette course aux armements s'est apparentée, dès le début des années 1980, à une guerre économique d'épuisement de l'adversaire[13]. L'excès de dépenses peut réduire à terme le potentiel économique attendu du développement de la richesse nationale. Jusqu'au milieu des années 1970, les experts américains estimaient les dépenses militaires de l'URSS à 7 ou 8 % de son PIB. Lorsqu'ils ont revu leurs calculs et ont affirmé que cette somme était largement sous-évaluée, en les estimant à 14 ou 15 % du PIB, l'ensemble des pays non affiliés à l'OTAN ont considéré qu'il s'agissait d'une manœuvre politique. Lorsque l'URSS a connu sa crise mortelle, il a pu être démontré qu'en prenant des mesures de prix comparables à celles des pays occidentaux, l'URSS dépensait plus de 25 % de son PIB à des fins militaires, en accordant toutes les priorités à son complexe militaro-industriel, lequel disposait notamment de près de 90 % du financement de la recherche-développement du pays pour satisfaire ses objectifs.

---

[9] Israël, S. (2016), cité dans « Face à SpaceX, le PDG d'Arianespace se fait lanceur d'alerte », Dominique Gallois, Le Monde, 6 Mai, Economie & entreprise, p.3.

[10] Smith, R., Martin, Fontanel, J.(1987), Time-Series estimates of the macroeconomic impact of Defence spending in France and Britain, in "Peace, Defence and Economic Analysis". Editors, C. Schmidt, F. Blackhaby, The International Economic Association, Mac Millan, London, 1987 (20 pages). Fontanel, J., & Smith, R. (1985). Analyse économique des dépenses militaires. Stratégique, Fondation, Paris

[11] Fontanel, J. (1982). Military Expenditure and Economic Growth: France, Morocco. report written for the United Nations, New York.

[12] Guilhaudis, J-F. (2015) , « Les Alliances collectives(Inf.2/1-11). », PSEI, Numéro 1, 17 août 2015, URL : http://revel.unice.fr/psei/index.html?id=351.

[13] Coulomb, F., Bensahel, L., Fontanel, J. (2007), The concepts of economic war and economic conflicts in a global market economy, in « Arms, War, and Terrorism in the global economy today, Ed. Wolfram Elsner, Ed. LIT Verlag, Bremen Schriften zur Konverzion, Band 13, Hamburg. 2007.

Dans ces conditions, le choix entre le « beurre et le canon » au profit des armes a été un élément essentiel de l'effondrement de l'URSS. Les coûts d'opportunité se sont alors avérés très élevés par rapport à ceux des Etats-Unis, pays qui disposait alors d'un système économique bien plus efficace et développé. En 1983, le Président Reagan, a lancé l'opération SDI (Strategic Defence Initiative), appelée communément la « guerre des étoiles », l'effort en matière de recherche-développement était si élevé que de nombreux instituts de recherche universitaires ont participé à cet élan, attirés par l'importance de cette manne financière. Il remettait ainsi en cause le contenu du Traité antibalistique signé par les deux grandes puissances. L'URSS ne pouvait alors plus suivre ni économiquement, ni en termes de chercheurs disponibles. Soit l'URSS engageait un conflit immédiatement, soit elle devait abandonner le leadership militaire, son dernier atout dans les rapports de puissance entre les deux Grands. L'effondrement de son image auprès des Etats et auprès des populations a dès lors été vite consommé.

Dans les années 1990, avec les réductions de dépenses militaires, le concept de « dividendes de la paix » a de nouveau été avancé, pour considérer que l'économie de tous les pays allait en bénéficier. En réalité, tous les pays producteurs d'armes qui s'engagent dans un désarmement souffrent d'abord de crises économiques régionales et sectorielles liées à l'arrêt de certaines productions militaires. Une réduction des dépenses militaires non compensée peut avoir des effets négatifs sur l'emploi et la demande globale. Certaines installations industrielles deviennent obsolètes et leur transformation pour la production civile s'avère coûteuse, ce qui rend les produits civils reconvertis peu concurrentiels. C'est pourquoi, il est plutôt fait état aujourd'hui « d'investissements de la paix », plutôt que de dividendes, car l'arrêt des chaînes de production n'engendre directement aucun profit, mais plutôt des pertes. Dans ce contexte, il faut investir dans d'autres productions pour retrouver un niveau satisfaisant de reconversion des personnes et des capitaux[14].

Il existe un paradoxe qui n'est pas toujours évoqué dans la littérature économique, plutôt séduite par le dilemme du « beurre ou du canon ». Certaines économies nationales ont de fortes dépenses militaires et un taux de croissance satisfaisant. Inversement, d'autres pays ont peu de dépenses militaires et n'ont pas suffisamment de croissance (Afrique subsaharienne). Par contre le Japon et l'Allemagne d'après Deuxième guerre mondiale ont réussi un développement économique spectaculaire, sans se préoccuper de leurs dépenses de défense. Dominés militairement, ils n'en ont pas moins profité indirectement de leur situation de « passager clandestin » des sommes affectées à leur défense. Sous

[14]UNIDIR (1992), Aspects économiques du désarmement, le désarmement en tant qu'investissement, UNIDIR, A/47/346, 27 Août, Genève. Fontanel, J., Smith, R. (1993), Le couple désarmement-développement dans la pensée économique, in "Economistes de la Paix"(Fontanel J., Ed.) L'Economie en Plus, PUG, 1993, (30 pages). Fontanel, J. (1993), La gestion économique du désarmement. Dix principes positifs. in "Economistes de la Paix" (Fontanel J., Ed.), L'Economie en Plus, PUG, 1993, (21 pages). Shkaratan, O., & Fontanel, J. (1998). Conversion and personnel in the Russian military‐industrial complex. Defence and peace economics, 9(4), 367-379.

certaines conditions, les dépenses militaires exercent parfois des effets positifs. Au niveau macroéconomique, une augmentation de l'effort de défense peut conduire au « militarisme keynésien », par une relance de l'activité économique nationale. Cette politique n'a pas été soutenue par Keynes qui pensait que d'autres dépenses publiques seraient bien plus intéressantes pour soutenir la croissance et le développement économique. Par ailleurs, les investissements des produits militaires ont des retombées parfois positives (en termes de recherche-développement ou de structure industrielle, notamment), ou négatives (notamment parce que l'augmentation des dépenses publiques en situation d'endettement produit une augmentation des taux d'intérêt, lesquels réduisent ainsi la rentabilité et le niveau d'engagement des investissements civils). L'analyse des effets des dépenses militaires sur les économies développées souligne le caractère neutre, mais parfois positif aussi, de leur impact sur l'économie, au contraire de leurs effets négatifs sur les pays en développement[15].

L'importance des dépenses militaires aux Etats-Unis est parfois perçue comme la volonté du gouvernement de mener une politique industrielle, interdite dans le domaine civil par l'Organisation Mondiale du Commerce. Cependant, les produits militaires échappent au système de concurrence internationale appliquée aux produits civils, sous couvert du rôle intangible de chaque Etat à assurer sa propre défense nationale. La recherche-développement du secteur militaire a souvent inspiré les entreprises qui produisaient aussi des biens duaux, à la fois publics et privés. Le complexe militaro-industriel n'en reste pas moins très intéressant dans les économies nationales des grandes puissances. Plusieurs grandes firmes sont confortées dans leur développement par les commandes militaires, notamment lorsqu'elles disposent aussi d'activités civiles subissant des cycles de précarisation récurrents. Boeing ou Airbus ont besoin des commandes d'armement de leurs gouvernements lorsque le marché civil est, temporairement, en récession. En outre, plusieurs secteurs économiques sont dépendants, à des degrés divers, des achats du secteur militaire, comme l'électronique, l'aéronautique, le spatial, etc. Mais surtout, la recherche-développement militaire bénéficie de financements considérables de l'Etat, lesquels peuvent ensuite profiter, si le secret technologique n'est pas revendiqué, au secteur civil. Le secret industriel, commercial et militaire est

[15] Hartley, K., Sandler, T. (1994), Handbook of Defence Economics, Vol.1. Elsevier, North Hollland. Coulomb (2004), Economic theories of Peace and War, Routledge, London and New York. Leontiev, W., Duchin, F. (1983), Military spendings. Facts and figures. Worlwide implications and Future Outlook, Oxford University Press, Oxford. Schmidt, C. (1987), The Economics of Military Expenditures, Mac Millan Press, London. Seiglie, C., Yi-Chun Lin, S., Kohli, T. (2014), Defence expenditures ; Theory and Empirics, in « The Evolving Boundaries of Defence : an assessment of récent shifts in Defence activities, (Renaud bellais, Ed.), Emerald, London. Fontanel, J. (1982). Military Expenditure and Economic Growth: France, Morocco. report written for the United Nations., ONU, New York. Deger, S., Smith, R. (1983), Military expenditure and growth in less developed countries ; Journal of Conflict Resolution, Vol.27, n°2. Dunne, P., Smith, R. (1990), Military expenditure and unemployment in the OECD, Defence Economics, Vol.1, n°1. Fontanel, J, Smith, R. (1990), The impact of strategy and measurement on models of French military expenditures, Defence Economics, Vol.1, n°4.

alors protégé avec l'aide des pouvoirs publics. Parfois, les Etats et les firmes sous-estiment volontairement les montants de la part militaire de la R&D, afin de ne pas prêter trop de critiques lors des discussions parlementaires. Aujourd'hui, face aux nouvelles menaces, les retombées des dépenses de recherche-développement civiles semblent supérieures à celles, de plus long terme il est vrai, de la recherche-développement militaire[16]. L'ouverture des frontières est alors importante pour de nombreux pays, car elle fournit aussi l'acquisition des techniques de sécurité modernes, celles qui échappent partiellement au secret revendiqué par le secteur militaire. Le développement de « l'intelligence service », la restriction de diffusion des informations sensibles et le contrôle de l'exercice de la manipulation sont aujourd'hui des armes dont l'efficacité, à fort potentiel, est sans doute élevée, mais encore mal estimée.

Les procédures de désarmement sont intéressantes lorsqu'elles conduisent les grandes puissances à réduire leurs dépenses militaires[17], leurs stocks d'armes et la méfiance qu'elles s'accordent mutuellement. Dans ce contexte, une guerre mondiale devient moins improbable. Le processus négocié de désarmement a souvent été évoqué et analysé[18], mais il n'a pas été pour autant été engagé, sauf dans le cadre des armes nucléaires et de l'interdiction des armes chimiques et bactériologiques. Dans les années 1980, il a été proposé des procédures de désarmement pour le développement, et même la création d'un Fonds international de Désarmement pour le développement[19]. Il a aussi été possible dans certains cas de développer des forces internationales de maintien de la paix, avec des succès et des échecs très relatifs[20]. Un désarmement pour un pays producteur d'armement constitue d'abord une perte de capital, puis une crise régionale et de l'emploi[21]. Dans ces conditions, les grandes puissances ont

[16] SIPRI Yearbook (2009), Armaments, disarmament, and internatinal security, Oxford, Stockholm, Oxford University Press.

[17] Fontanel, J. (1980). Le concept de dépenses militaires. Défense Nationale.

[18] Coulomb, F., Fontanel, J. (2000), Disarmament in the Next Millenium, Defence and Peace Economics, Volume 11, number 1, 2000. Fontanel, J. (2002), Disarmament : A century of economic thought, Defence and Peace Economics,Tome 28, 2002. Fontanel, J. (1994), The Economics of Disarmament. A Survey, Defence and Peace Economics, Vol. 5, n° 2, (34 pages). Fontanel, J. (1995), The economics of disarmament, in Handbook of Defense Economics, Vol.1. (Hartley and Sandler eds), North Holland, Elsevier Sciences, Amsterdam, 1995.

[19] Fontanel, J. (1985), L'intérêt d'un Fonds International de Désarmement pour le Développement, Etudes Internationales. Québec, Canada, Septembre 1985.(15 pages). Fontanel, J. (1986), The International Disarmament Fund for Development Disarmament, a periodic review by the United Nations, United Nations, New York, 1986. Fontanel, J. Smith, R.P. (1987), The creation of an International Disarmament Fund for Development, in "Defence, Security and Development" (Deger, S. et West R., Ed.), Francis Pinter, London, June 1987, 10 pages.

[20] Sheehan, N. (2003). Le maintien de la paix pour le développement. In J. Fontanel (Ed.), Civilisations, globalisation, guerre. Discours d'économistes. Collection Débats, Presses Universitaires de Grenoble. Sheehan, N. (2013) La réforme ou « reconstruction » du secteur de la sécurité : outil fondamental pour la consolidation de la paix dans les pays post-conflits, in Liber Amicorum, hommage en l'honneur du Professeur Jacques Fontanel, L'Harmattan, Paris

[21] Coulomb, F., Fontanel, J. (2000), Disarmament in the Next Millenium, Defence and Peace Economics, Volume 11, number 1, 2000. Fontanel, J. (1993), Disarmament for development in favour of developing countries, Chatterji & Rima Ed., Mac Millan (30 pages). Fontanel, J. (1993), Investing in peace, The UNESCO Courier, October 1993 (5 pages). Fontanel, J., Fontanel, J., Matelly, S. (2000), Le coût des dividendes de la paix, Mondes en développement, Tome 28, année 2000, n° 112, pp. 59-73. Fontanel, J. (1982). Military Expenditure and Economic Growth (France, Morocco). report written for the United Nations, UNO, New York.

toujours hésité à s'engager dans une voie pacifique sans précautions extrêmes (sauf à la fin des guerres), car la conversion des industries d'armement est périlleuse dans un système de concurrence internationale[22].

Si l'idée d'un désarmement pour le développement peut être mise en place, il est nécessaire de respecter certaines règles qui rendent la procédure complexe[23]. Le désarmement a cependant connu un début d'intérêt de la part des grandes puissances au début des années 1990, après la guerre froide. Cependant, la course aux armements a repris assez rapidement, les progrès dans la conclusion d'accords nouveaux n'ont porté que sur des points mineurs et les négociations sur la convention d'interdiction des armes biologiques, les matières fissiles ou l'espace ont été interrompues. Le traité ABM (Anti Ballistic Missiles) est menacé par les nouvelles recherches engagées par le gouvernement américain concernant sa capacité à réduire les fenêtres de vulnérabilité par la mise en place de missiles capables de détruire les armes offensives de l'ennemi. En outre, l'érosion continuelle du respect du Traité de Non-Prolifération des armes nucléaires (TNP) ne manque pas d'inquiéter la communauté internationale La guerre en Irak a marqué un temps d'arrêt brutal au processus de réduction des armements et a favorisé des conflits ouverts qui concernent aujourd'hui le monde entier[24].

Quelles armes, l'importance d'un « bang for a buck » ?

Quelle est l'importance des armes choisies dans le rapport complexe et souvent contradictoire entre l'efficacité économique et les exigences d'une sécurité nationale ?

a) L'intérêt stratégique d'un bang for a buck

L'expression elle-même, « bang for a buck », met en évidence la capacité destructrice d'une arme compte tenu de son coût. Si une arme est la plus destructrice, mais qu'elle est onéreuse, il peut alors être préférable de choisir d'autres armes dont la complémentarité permettra une destruction plus importante, avec la même enveloppe de dépense globale. Autrement dit, étant

[22] Fontanel, J. (1995), La conversion économique du secteur militaire, Economie Poche, Economica n° 12, Paris, 1995. Borissova, I, Ward, M. (1995), The principles of arms conversion in the case of Russia, Defence and Peace Economics, 1995, 6.3. Shkaratan, O., & Fontanel, J. (1998). Conversion and personnel in the Russian military industrial complex. Defence and peace economics, 9(4), 367-379.

[23] Fontanel, J., Smith, R. (1993), Le couple désarmement-développement dans la pensée économique, in "Economistes de la Paix"(Fontanel J., Ed.) L'Economie en Plus, PUG, 1993, (30 pages) ; Fontanel, J. (1993), La gestion économique du désarmement. Dix principes positifs. in "Economistes de la Paix" (Fontanel J., Ed.), L'Economie en Plus, PUG, 1993. Fontanel, J., Ward, M. (2002), A hard look at the costs of peace, World Economics, Vol.3, n.2, April-June 2002. Coulomb, F. et Fontanel, J. (2003), Disarmament: A century of economic thought. Defence and peace economics, vol. 14, no 3, p. 193-208.

[24] Guilhaudis, J-F. (2015), Désarmement, PSEI, Numéro 1, 17 août 2015, URL : http://revel.unice.fr/psei/index.html?id=357.

entendu que trop de dépenses en matière de défense peuvent fragiliser l'économie d'un pays, et donc, à plus ou moins long terme, sa propre sécurité, il s'agit d'optimiser économiquement la stratégie militaire. Cette présentation s'avère plutôt en faveur de la projection des forces vers l'extérieur. Cependant, même si la défense est plus onéreuse que l'attaque, certaines armes de dissuasion sont suffisamment dissuasives pour réduire les menaces venant de pays ennemis. Ainsi en est-il de l'arme nucléaire, dont le « bang for a buck » est puissant[25], mais dont l'utilisation pose des problèmes moraux de survie de l'ensemble de l'humanité. Dans ce cas, le « bang » est trop fort pour être utilisé dans des conditions qui ne sont pas « extrêmes », et il ne peut l'être que par les pays qui disposent déjà de l'arme nucléaire, le Traité de non prolifération interdisant de nouvelles productions par de nouveaux pays. De tout temps, le choix des armes dépend des circonstances. Les conflits prennent parfois des chemins qui n'étaient pas prévus et des moyens qui ne leur étaient pas destinés. D'autre part, la disponibilité d'une arme peut être contrôlée et réservée à quelques grandes puissances. Enfin, la guerre de l'information se développe et change le périmètre des contenus sécuritaires et militaires des dépenses publiques et privées.

D'abord, le choix des armes dépend de la nature du conflit et des moyens disponibles pour les belligérants. Il existe des objets « à utilisation civile » qui peuvent aussi bien détruire que les armes sophistiquées. Les bâtons de dynamite, l'usage du pétrole ou les fertilisants peuvent devenir des armes capables de détruire les personnes, mais aussi les réseaux d'information. Dans leurs effets destructeurs, ces armes sont susceptibles de provoquer une crise financière. Or, ces actions, facilement accessibles à un groupe de terroristes, sont difficiles à détecter. Au Rwanda, des outils comme les marteaux ou les machettes ont tué un million de personnes en trois mois.

La puissance de feu et de rétorsion est une expression plus juste à retenir concernant les dépenses engagées pour la sécurité d'un pays, au regard des engagements financiers qu'elle suppose. Plusieurs composantes de la défense d'un pays sont concernées, comme la base industrielle de production des armes, les coûts des consommations intermédiaires et leur disponibilité, les salaires nationaux des forces militaires ou de défense, la capacité de stockage d'armes efficaces ou l'achat d'armes à l'étranger à fort ratio force/prix. Se posent alors trois questions principales, d'abord la capacité à produire ses armes, notamment avec des alliés, ensuite, la détermination des processus d'achat et enfin le choix entre des équipements de qualité (souvent très performants, mais sophistiqués) ou en quantité (robustes, et simples d'utilisation). Les chars soviétiques étaient

[25] Coulomb, F., Fontanel, J. (2006), Le coût du nucléaire en France et son avantage comparatif, in Pascallon (Ed.), La sécurité de la France, Economica, Paris, 2006. Fontanel, J. (2006), Le coût des forces nucléaires, in "Désarmement pour le Développement" (Fontanel, J, Guilhaudis, J-F), Ed.), Ares, Défense et Sécurité, Lyon, Grenoble, 1986.

qualitativement inférieurs militairement aux tanks américains, mais plus nombreux et plus rustiques, ils n'étaient pas pour autant en situation d'infériorité.

La supériorité technologique n'est pas toujours une garantie de sécurité, ni de victoire en situation de guerre. La question de la configuration des diverses capacités militaires pour travailler ensemble en toute complémentarité au regard des objectifs définis fait référence aux stratégies mises en place. Lorsque la France s'engage dans la construction onéreuse de la Ligne Maginot pour se protéger de l'envahisseur allemand, elle commet une erreur stratégique qui rend les dépenses engagées inutiles, car elle n'empêche pas l'envahissement du territoire national. Les « jeux » stratégiques ne sont pas si faciles à déchiffrer. Quelle est la juste balance entre les armes (plus d'avions ou de sous-marins nucléaires) et les forces humaines engagées (plus de soldats ou plus d'ingénieurs ?). Un Ministère de la défense nationale doit faire des choix qui engagent le pays sur plusieurs décennies, parfois un demi-siècle. En outre, la transformation des forces militaires en moyens efficaces de défense du pays dépend des tactiques militaires, des vertus et des motivations des combattants, de l'adaptabilité des armes aux réponses de l'ennemi, de la volonté d'une armée centrée sur la défense ou sur l'attaque. S'il est toujours possible d'intégrer de nouvelles armes dans le dispositif, les stocks existants restent dominants dans la stratégie d'aujourd'hui, avec de trop lentes inflexions au regard de la rapidité des destructions.

La sécurité d'un pays ne dépend évidemment pas que de ses efforts militaires, lesquels dépendent normalement de la menace perçue. Les modèles de course aux armements ont mis en évidence les processus d'interaction dans les choix des armes et les dépenses engagées entre deux ou plusieurs pays en opposition. Dans le fameux modèle de Richardson[26], les dépenses militaires des ennemis, le fardeau économique de la défense nationale (effet de fatigabilité) et les griefs entre les Etats sont les trois facteurs fondamentaux présentés comme les déterminants principaux des dépenses militaires nationales, en lien d'ailleurs avec les efforts des pays alliés. Il faut ajouter aussi la puissance économique du pays pour assurer les dépenses nécessaires, sans remettre en cause le potentiel économique des pays.

Cette analyse évidente n'a pourtant pas été en mesure de représenter les situations concrètes d'un demi-siècle de course aux armements entre l'URSS et les Etats-Unis. D'abord, le processus d'action-réaction n'a pas été confirmé, sauf en situation de tension extrême. Les Etats-Unis et l'URSS n'ont pas souvent fait correspondre instantanément leurs efforts de dépenses militaires. Ensuite, les dépenses militaires des ennemis ne sont pas toujours bien connues, surtout quand les systèmes économiques ne sont pas similaires. Enfin, le modèle

[26] Richardson a été le premier à présenter un modèle de course aux armements. Les grandes puissances déterminent leurs dépenses militaires sur la base de leurs PIB, de leurs dépenses militaires passées (effet d'inertie et d'équipements développés sur plusieurs années) et les griefs des pays ennemis ou adversaires.

n'a pas prévu l'effondrement de l'Union soviétique. De manière claire, les forces politiques et militaires nationales sont plus influentes pour déterminer l'effort de défense d'un pays, car les intérêts industriels et politiques, les rivalités à l'intérieur même des forces armées et les influences de la bureaucratie d'Etat sont souvent les considérations les plus décisives dans les choix quantitatifs et qualitatifs des dépenses militaires. L'URSS en est l'exemple même, mais les choix américains ont aussi été dictés par des intérêts qui n'étaient pas en phase avec les nécessités militaires du moment.

Les choix stratégiques impliquent aussi des collaborations ou des ventes d'armes à l'étranger. Il existe des restrictions aux transferts[27], des accords internationaux qui se proposent de respecter la souveraineté des Etats et leur droit inaliénable à la sécurité, tout en stipulant un contrôle dans le cadre du droit international qui s'impose à toutes les Parties. Quel type d'industrie de la défense doit être mis en place, pour quelles retombées sur l'économie civile ? Ces questions ont été posées, mais les réponses n'ont pas toujours été au rendez-vous. En 1990, un amendement auprès du Congrès américain proposait de rendre obligatoire la prise en compte par le Congrès de la dualité (militaire – civile) du développement de nouvelles armes (proposition qui a été, sans surprise, refusée). Il est vrai que le secteur militaire, longtemps impacté par des armes trop sophistiquées (« industries baroques ») pour être utiles à court terme à d'éventuelles productions civiles, exerce une influence à très long terme sur les technologies de demain, bien qu'elles s'avèrent trop onéreuses pour les applications d'aujourd'hui.

b) Le cas spécifique de l'arme nucléaire

L'arme nucléaire n'est pas désarmée. Elle est toujours présente et même son efficacité destructive a été constamment améliorée. Comme l'indique Jean-François Guilhaudis, « les principales puissances nucléaires ont fait le choix de le rester et sont en cours de modernisation de leur dispositif. Le club nucléaire devrait donc, pour l'essentiel, subsister, de même que la tentation nucléaire… Un Etat, les Etats-Unis, est toujours seul de son espèce, la seule vraie superpuissance… Les Etats-Unis sont premiers dans tous les classements et bien décidés à garder cette place. La Russie n'est plus ni une puissance mondiale, ni une puissance globale et le niveau de ses moyens fait qu'il lui sera difficile de le redevenir. La puissance chinoise, quoique clairement montante, reste encore nettement en retrait sur le plan stratégique comme conventionnel. Pour le moment, la Chine n'est ni une puissance globale ni une puissance complète »[28].

[27] Biad, A. (2015), Traité sur le commerce des armes, PSEI, Numéro 2, , mis en ligne le 21 novembre 2015, URL : http://revel.unice.fr/psei/index.html?id=671.

[28] Guilhaudis, J-F. (2015), « Puissances et impuissances, acteurs de la sécurité et de l'insécurité internationale.(A1-A83) », PSEI, Numéro 1, 17 août 2015, http://revel.unice.fr/psei/index.html?id=333.

Tableau 3 : Nombre, type, capacité des armes nucléaires selon les pays[29] en 2014.

Pays (année de disponibilité, nombre d'essais nucléaires)	Capacité fin 2014	Nombre d'armes nucléaires en 2014 (maximum atteint dans le passé) et prévisions.
Etats-Unis : 1945 (1054 essais nucléaires)	Mer-sol : 1152 Sol-Sol : 470 Air-Sol : 300 ANT (tactique) : 200 Armes non déployées : 2530 Démantèlement prévu : 2700	7352 (31255 en 1967) Réduction des ANT Objectif « New START » : 1550 têtes déployées
Russie : 1949 (715 essais nucléaires)	Mer-sol : 480 Sol-sol : 1220 Air-Sol : 810 ANT (oui) Armes non déployées : oui (nombre non connu) Démantèlement prévu : oui	8043 (45000 en 1986) Réduction des ANT Objectif « New START » : 1550 têtes déployées
France : 1960 (210 essais nucléaires)	Mer-sol : 48 Air-Sol : 54 Armes tactiques : ASMPA : 54	300 (540 en 1992), Suppression forces sol-sol Réduction des forces air-sol Et mer-sol.
Royaume-Uni : 1952	Mer-sol	Moins de 225 (> 400 1979, dont air-sol) Objectif : 180 ogives en 2025, dont 120 opérationnelles.
Chine : 1964 (45 essais nucléaires)	Triade (Mer-Sol, Sol-Sol ; Air-Sol), possession ANT incertaine) Armes non déployées	250 (maximum inconnu)
Israël (date inconnue)	Triade (chiffre inconnu)	80 (maximum inconnu)
Inde : 1974 (6 essais nucléaires)	Dyade (air-sol et sol-sol)	90/110 (max inconnu)
Pakistan : 1998 (6 essais nucléaires)	Dyade (air-sol ; sol-sol), Armes non déployées	100/120 (max inconnu)
Corée du Nord : 2006	En cours	6 à 8

On distingue les puissances nucléaires « de jure » ou officielles (Etats-Unis, Russie, Royaume-Uni, Chine et France) qui ne peuvent les utiliser qu'en cas extrême de légitime défense, les Etats disposant d'armes nucléaires « de facto » (Israël, Inde, Pakistan), et ceux auxquels elles sont refusées (Iran et Corée du Nord). Il convient de signaler que les deux grandes puissances nucléaires maintiennent ce type de forces en mode opérationnel et qu'elles les modernisent, tout en améliorant encore les technologies avec l'avancée de la

[29] Sur la base des informations données par : Chabbi, M. (2015), Le Club Nucléaire : des capacités très inégales. PSEI, Numéro 1, 17 août 2015, URL : http://revel.unice.fr/psei/index.html?id=349.

recherche scientifique. C'est aussi le cas de la Chine, de l'Inde, du Pakistan et de la Corée du Nord. En revanche, la France et le Royaume-Uni proposent aujourd'hui la simple modernisation de leurs forces, voire parfois de maintenir leurs conditions opérationnelles de fonctionnement. Cependant, si la France continue à la détenir en revendiquant la stratégie du « faible au fort », la plupart des autres pays n'ont jamais revendiqué la théorie du « no first use ».

Dans un contexte de plus en plus violent, il est légitime de s'interroger sur le maintien de telles forces, dont l'utilisation pourrait encore être rendue possible en cas de conflits frontaux dans les années à venir. L'insécurité, qui provient principalement des conditions économiques précaires, de la pauvreté, mais aussi des rapports de force, peut aussi naître de l'existence d'armes d'une capacité de destruction massive disponible terrifiante. Les Etats-Unis disposent d'un pouvoir nucléaire explosif de 2.400 mégatonnes, soit plus de 100.000 fois la puissance de la bombe d'Hiroshima, pour un coût relativement faible au regard des avantages stratégiques et politiques que le gouvernement en retire. La question de la prolifération de cette arme est toujours aussi pertinente. La réduction partielle du nombre d'ogives nucléaire est plutôt un événement intéressant, mais les dangers de la prolifération, les avancées technologiques et le rôle réduit de la Conférence sur le désarmement laissent planer des doutes sur le non usage potentiel de cette arme.

Au départ, le nouveau Président Barrack Obama s'est présenté comme le chantre de la dénucléarisation militaire du monde. C'est même à ce titre qu'il a obtenu le Prix Nobel de la paix, dès la première année de son mandat. Après huit années de Présidence, même si ses projets ont été le plus souvent contrecarrés par une Russie méfiante, une Chine engagée dans de forts programmes nucléaires et par l'hostilité des Républicains au Congrès, les résultats de son action sont particulièrement modestes, à un moment de l'histoire où l'utilisation de cette arme de destruction massive n'a jamais été évoquée sur les théâtres d'opération. Au terme de son mandat, il n'aura réussi qu'à obtenir un accord de non prolifération des armes atomiques imposé à l'Iran. En 2010, le traité New Start a conduit à une nouvelle réduction des arsenaux nucléaires (1550 ogives nucléaires pour les deux parties, Etats-Unis et Russie), mais cette initiative n'a pas ensuite été poursuivie[30]. La même année, les Etats-Unis vont augmenter les fonds consacrés aux armes nucléaires, en vue de moderniser les installations et matériels vieillissants, mais aussi pour maintenir en condition le complexe militaro-industriel et scientifique. Le Pentagone dépense annuellement plus de 70 milliards de dollars pour son arsenal nucléaire (soit plus que l'ensemble des dépenses militaires russes, pourtant engagées dans de nombreux théâtres d'opération coûteux). En revanche, les Etats-Unis n'ont toujours pas ratifié le Traité pour l'interdiction complète des essais nucléaires, signé sous la

[30] Il faut noter que les armes nucléaires peuvent être désarmées, mais que le coût de l'opération est relativement élevé, de l'ordre du million de dollars d'unité. En revanche, plus de 4000 ogives non déployées font partie de l'arsenal comme force de réserve.

Présidence Clinton, mais jamais ratifié par le Sénat. Enfin, Obama a engagé un programme de plus de 700 milliards de dollars sur les dix prochaines années (1000 milliards de dollars sur les 30 prochaines années sont déjà engagés) pour renouveler et moderniser les forces nucléaires américaines (notamment les armes nucléaires européennes), avec la construction de nouveaux missiles intercontinentaux, de sous-marins nucléaires et de bombardiers. A partir du moment où l'arme nucléaire reste un instrument de défense d'un pays face aux Etats qui eux-mêmes disposent de ces armements, cet effort peut sembler nécessaire. En revanche, la décision de développer de nouvelles armes nucléaires tactiques et d'un nouveau missile de croisière furtif (30 milliards de dollars pour l'opération) ne manque pas d'inquiéter. Les missiles de croisière sont destinés aux frappes préventives et les armes nucléaires tactiques peuvent être utilisées sur des objectifs précis, sans effet de destruction massive. La combinaison de ces deux armes laisse ouverte la mise en place d'une stratégie de guerre nucléaire rapide, laquelle peut être l'occasion d'une escalade entre les belligérants conduisant à une guerre impliquant des armes de destruction massive. La force du Pentagone, soutenue par le complexe militaro-industriel qui vit de la course aux armements et de la production de nouvelles armes, aura été plus forte que les objectifs pacifiques du Président des Etats-Unis.

Les investissements engagés dans le domaine nucléaire ne semblent pas devoir diminuer. L'idée d'une dénucléarisation a été repoussée aux calendes grecques. Pourtant, lors de sa visite à Hiroshima en mai 2016, Barrack Obama a cependant souhaité la reconstruction d'un monde sans armes nucléaires. Bis repetita. Les gouvernants des pays qui disposent de cette arme ne veulent pas s'en séparer, à la fois car elle leur donne un sentiment de puissance, mais aussi pour justifier, face à leurs citoyens, l'utilité des dépenses engagées depuis des décennies.

La recherche-développement militaire

L'avantage technologique militaire américain est incontestable. Les Etats-Unis exercent un leadership incontesté en matière de Recherche-développement dans le monde, mais son avance semble progressivement être grignotée par les pays asiatiques (Tableau 4). Les entreprises restent la source la plus importante de financement de la R&D américaine, notamment dans la recherche appliquée et le développement. La recherche fondamentale est assurée par le milieu universitaire et les agences fédérales, lesquelles possèdent leurs propres laboratoires[31]. Les institutions d'enseignement supérieur et de recherche assurent près de 60 % de la recherche fondamentale et un tiers de la recherche fondamentale et appliquée.

[31] Les recherches engagées par le NIST ((National Institute of Standards and Technology) sont réalisées en interne, notamment pour le Department of Defence et la NASA).

Tableau 4 - Dépenses de R&D en millions de dollars PPA courants[32]

Pays	1992	2006	2013	Coefficient décroissance 2013/1992
Allemagne	39.106	70.229	100.001	2,56
Canada	9.226	24.092	24.565	2,66
Corée du Sud	8.124	35.413	68.937	8,49
Espagne	4.833	16.070	19.133	3,96
USA	165.835	353.326	456.977	2,76
France	25.270	42.013	55.218	2,19
Italie	12.434	20.207	26.520	2,13
Japon	69.682	138.465	160.267	2,30
Royaume-Uni	19.747	37.046	39.859	2,02
OCDE	391.486	850.036	1.126.468	2,88

Depuis la deuxième guerre mondiale, en conflit avec le développement du secteur de la défense de l'Union soviétique, l'État américain a considérablement investi dans le secteur militaire aussi bien dans l'outil de production que dans le domaine de la recherche scientifique. Avec l'effondrement de l'URSS, Washington a souhaité développer son leadership mondial. Le budget fédéral de R&D vise clairement à :

- maintenir le leadership mondial américain en science et technologies,
- stimuler l'innovation,
- attirer les industries de pointe et développer les investissements lucratifs du secteur privé,
- maintenir et développer l'efficacité du système de transfert de technologie entre les secteurs publics et privés,
- soutenir la recherche médicale,
- former les jeunes en science, technologies, ingénierie et mathématiques,
- promouvoir les énergies propres et la lutte contre la menace du changement climatique, dans le cadre des engagements internationaux des Etats-Unis.

La R&D se décompose en trois étapes bien distinctes, la recherche fondamentale (3 % des coûts), la recherche appliquée (17 % des dépenses) et le développement expérimental (80 % des engagements financiers). Elle dépend des financements publics (en incitation, en complément, en soutien), surtout pour la recherche fondamentale. Elle est de nature hétérogène la nature des secteurs économiques considérés. L'Etat américain dépense chaque année près de 4 % de ses dépenses à cette fin (dont 60 % à des fins militaires), plus que tous

[32] Eurostat (2015), Dépenses de R&D, http://ec.europa.eu/eurostat/statistics explained/index.php/R_%26_D_expenditure/fr

les autres pays au monde réunis. Le budget de la R&D du DoD (Department of Defense) est surtout concerné par le développement, le test et l'évaluation des systèmes d'armes avec près de 80 % des dépenses (Tableau 5).

Tableau 5 - Types de dépenses fédérales de R&D de défense[33]

Types	2009	2010	2011	2012	2013	2014	2015	2016**	2017**
Développement des armes	75,3	75,4	72,0	65,1	56,1	54,6	53,2	56,30	58,84
Sciences et technologie	15,6	16,3	13,8	14,2	12,6	13,8	13,9	15,16	13,09
Activités relatives à la défense	4,3	4,3	4,4	4,5	4,4	5,1	6,3	5,73	6,96
Total	**95,2**	**96,0**	**90,2**	**83,9**	**73,1**	**73,6**	**73,5**	**77,18**	**78,88**

Depuis 2009, les sommes allouées à la R&D militaire ont subi une perte de plus de 20 %. La baisse de la recherche développement aux Etats-Unis, dans le domaine militaire, n'est pas sans danger. Les USA pourraient perdre leur première place dans un secteur hautement technologique. Le Tableau 3 met cependant en avant l'importance des dépenses de R&D des Etats-Unis. Leurs forces armées sont toujours les plus sophistiquées de la planète, mais la concurrence chinoise devient inquiétante. Aujourd'hui plus qu'hier, de nombreux financements de R&D militaires ont des répercussions sur la R&D civiles, car il est rare que les industries de haute technologies ne travaillent pas simultanément dans les deux secteurs, civil et militaire. Les financements de la R&D militaire ont été soutenus, ils représentent encore aujourd'hui 17 à 18 % de la R&D totale des Etats-Unis. En l'absence de guerre déclarée, l'effort de défense est en récession, et le secteur militaire de la R&D est directement concerné (Tableau 6 et Tableau 7).

L'endettement de l'Etat fédéral pèse fortement aujourd'hui sur les choix de l'Etat. A priori, cette option paraît légitime et relativement peu contraignante à court terme. L'effort de R&D militaire génère des coûts d'opportunité importants (drainage sectoriel des moyens humains, intellectuels et industriels, réduction effective du potentiel scientifique dévolu au secteur civil), mais il concerne souvent des secteurs technologiques nouveaux que l'économie marchande ne peut immédiatement financer, au regard des coûts relatifs considérables à engager à court terme.

[33] AAAS (2016), Historical Trends R&D Budget and Policy Program, http://www.aaas.org/page/historical-trends-federal-rd

Tableau 6 - Principaux postes de dépense concernant la R&D du budget fédéral américain en 2012[34], puis 2014, 2015 et 2016[35] (en milliards de dollars).

Agences	2012	2014	2015	2016[36]
Défense	72,92	66,02	67,45	72,12
NASA	11,31	11,91	12,15	12,24
Energie	10,61	12,00	11,74	12,60
- dont énergie atomique de la défense	4,25	4,89		
Veterans Affairs	1,16	1,10	1,09	1,15
Homeland Security	0,46	1,32	1,32	0,57
Santé et sciences humaines	31,38	30,69	30,47	31,04
National Science Foundation	5,64	5,83	6,00	6,31
Agriculture	2,33	2,38	2,45	2,88
Environnement	0,57	0,54	0,52	0,56

Tableau 7 - Evolution des dépenses de R&D du gouvernement fédéral (2006-2017), avec imputation sectorielle des dépenses effectives[37]

Dépenses fédérale de R&D	2009	2010	2011	2012	2013	2014	2015	2016**	2017**
Défense	95,2	96,0	90,2	83,8	73,1	73,6	73,5	77,2	78,9
Civile	67,3	69,5	66,4	68,0	64,6	67,0	66,6	70,3	68,1
Total	**162,6**	**165,6**	**156,6**	**151,8**	**137,7**	**140,6**	**140,1**	**147,5**	**147,0**

Les investissements massifs en R&D militaire des USA sont un atout de poids pour l'économie nationale et un vecteur de domination mondiale. En

[34] IHEST (2014) La recherche aux Etats-Unis, http://www.ihest.fr/la-mediatheque/international/etats-unis-science-innovation/la-recherche-aux-etats-unis

[35] Sargent, J.F. (2015), Federal Research and Development, FY2016, Congress Research Service, November 10, 7-5700, www.crs.gov, p.10.

[36] Propositions du Président.

[37] AAAS (2016), Historical Trends R&D Budget and Policy Program, http://www.aaas.org/page/historical-trends-federal-rd

termes d'innovation, la R&D militaire est souvent plus créatrice à long terme que celle qui porte sur des biens de consommation, au regard des exigences technologiques ultimes et du secours systématique des fruits récents du secteur scientifique. En outre, elle accompagne parfois de manière très efficace des financements privés dans des domaines porteurs de la technologie moderne. On dénonce souvent le rôle important, voire excessif, des considérations commerciales dans les dépenses de R&D, mais les financements de l'Etat pour orienter la recherche scientifique exercent aussi un rôle essentiel dans le financement des sciences. On constate que les financements publics de la recherche fondamentale concernent surtout le domaine de la santé et que le secteur militaire est le principal bénéficiaire des développements, sans interférer outre mesure sur la recherche de base[38] (Tableau 8).

Tableau 8 – Les dépenses de R&D par catégorie et principales agences bénéficiaires[39]

Types de R&D	FY 2014 actuel	FY 2015 Engagé	FY 2016, Requis
Recherche de base, dont	32,19	31,90	32,73
- Services de santé et humains	15,86	15,58	16,00
- NSF	4,75	4,83	5,06
- Département Energie	4,10	4,12	4,25
Recherche appliquée, dont	32,55	32,91	32,73
- Services de santé et humains	14,62	14,79	14,86
- Défense	4,66	4,78	4,82
- Energie	4,55	4,36	4,68
Développement, dont	68,99	70,69	75,98
- Défense	58,99	60,37	65,04
- NASA	6,00	6,48	6,42
- Energie	2,56	2,32	2,62
Installations et équipements	2,62	2,58	2,84

Il faut enfin noter que les dépenses fédérales de R&D civiles ont eu aussi tendance à stagner, sauf dans le secteur de la santé. C'est pourquoi cette situation a inquiété le monde scientifique américain. En 2013, dans le cadre d'un accord destiné à éviter un blocage du fonctionnement de l'Etat fédéral lié à un dépassement du plafond de la dette, le Congrès a décidé d'une coupe

[38] Wojcik, D.E., Michaels, P.J. (2015), Is the Government Buying Science or Support ? A Framework Analysis of Federal Funding- Induced Biases, Cato Working Paper, n°29. April 30. http://www.cato.org/publications/working-paper/government-buying-science-or-support-framework-analysis-federal-funding

[39] Recomposition de deux tableaux issus de Sargent, J.F. (2015), Federal Research and Development, FY2016, Congress Research Service, November 10, 7-5700, www.crs.gov, pp. 6 et 7.

budgétaire automatique de 1200 milliards de dollars, ce qui a entrainé la réduction de nombreux programmes, dont plusieurs dans le secteur de la recherche militaire, ce qui n'est pas sans conséquence sur les capacités militaire futures des USA[40], mais aussi sur l'innovation et la compétitivité commerciale dans bien d'autres secteurs. La pression des coûts à la baisse pousse à investir dans des projets à court terme, plutôt que dans l'innovation à long terme, celle qui est susceptible de donner un avantage stratégique à l'économie nationale. Les propositions du Président américain sont une réponses apportées à l'appel des scientifiques pour le maintien du leadership national sur la recherche-développement et les progrès scientifiques, par le canal du financement de la R&D dans le secteur militaire, notamment dans les domaines qui concernant à la fois les secteurs d'applications duales.

C'est l'industrie civile qui réalise la plus grande partie des efforts de R&D et de production liés aux systèmes militaires, mais ce sont les militaires qui prennent les décisions, lesquelles conduisent souvent à un armement « baroque », sophistiqué, trop coûteux au regard de ses capacités tactiques et stratégiques sur les théâtres d'opération. A l'exportation, les industries d'armement sont de plus en plus vulnérables à la concurrence, car leurs produits sont trop chers et leurs avancées technologiques pas suffisantes dans plusieurs domaines importants des armes modernes, comme les drones, la surveillance, les missiles ou les satellites. Avec la fin de la Guerre froide, l'incitation à conserver une avance technologique décisive s'est faite moins pressante, ce qui prive le secteur de la défense de son principal moteur de progrès. En proportion de leurs ventes, les dépenses en R&D des grandes entreprises civiles travaillant pour le secteur militaire ont nettement diminué depuis 2000. Il en résulte un certain affaiblissement de la base industrielle militaire, qui est aussi tributaire de la concurrence industrielle des pays émergents, notamment de la Chine. Il y a encore deux ou trois décennies, l'industrie militaire était souvent pionnière dans les nouvelles technologies, elle est aujourd'hui dépassée par le secteur civil, lequel ne boude pas, cependant, les crédits militaires pour financer les innovations duales. Les recherches dans les secteurs de la santé, des télécommunications, de la biologie, de l'énergie ont été financées majoritairement par les entreprises privées, mais la R&D militaire a été mise à contribution pour faire avancer les recherches. De ce fait, la R&D à fin duale (à des fins civiles et militaires) permet d'élargir le domaine de rentabilité d'opérations de long terme.

Les effets positifs de la préférence donnée à la R&D militaire sur la compétitivité industrielle ont été aux Etats-Unis ont été très contestés pendant la guerre froide et lors l'Initiative de Défense Stratégique proposée par Ronald Reagan. Les grands groupes d'armement américains en ont profité en étant de

[40] La R&D de l'armée de terre, de l'agence des missiles de la défense ou du DARPA (Defense Advanced Research Projects Agency) ont vu leurs crédits diminuer de près de 20 %. Même l'armée de l'air jugée prioritaire a connu une baisse de financement dans ce domaine.

68 à 82 % plus rentables que ceux des autres secteurs de l'économie. L'explication à cet écart portait sir les importants transferts de certains coûts de R&D commerciale vers des programmes militaires[41]. Mampaey et Serfati[42] ont également démontré la valorisation boursière exceptionnelle des groupes de l'armement aux États-Unis. Ces analyses ne sont plus reprises aujourd'hui, sans doute parce que le contexte est différent, qu'il n'y a plus de recherche d'armement « baroque » et que la compétition pour les contrats auprès du Ministère de la défense est plus affirmée, car elle porte sur des produits et des technologies différentes et évolutives. Les analyses de l'impact de la R&D militaire restent confidentielles.

Pour les responsables de la défense américaine, si la pression budgétaire s'oppose aux défis militaires à long terme, il est cependant nécessaire de disposer d'un budget de R&D militaire plus important que celui des adversaires potentiels en vue de conserver l'avance technologique et commerciale des Etats-Unis. Le Department of Defense doit donner des orientations à la recherche, par ses financements qui apparaissent comme autant d'occasions de bénéficier d'effets d'innovation applicables dans de nombreuses activités civiles. Le DoD finance des programmes et projets d'armement mais ce sont les firmes privées qui emploient les trois quarts des chercheurs (70 % des chercheurs contre 17 % dans les Universités), ce qui leur permet de bénéficier des effets d'aubaine, de récurrence, d'opportunité et des économies d'échelle et de fonctionnement. Cela montre la forte compétitivité des entreprises américaines par rapport aux entreprises d'autres pays. L'importance de la R&D militaire permet aux entreprises d'investir dans le domaine de la recherche. En outre, l'IR&D (dite indépendante) est conduite à l'initiative des firmes d'armement, en dehors de leurs contrats courants, sans contrôle et sans financement direct du DoD. Le contractant finance au départ lui-même l'entièreté des dépenses, mais il sait qu'une partie de celles-ci pourront ultérieurement être imputées comme coûts indirects dans les contrats conclus avec l'Etat. L'importance des firmes et leur concurrence sur les mêmes projets expliquent la concentration et la force de la R&D civile et militaire. Les retombées de la R&D militaire américaine, notamment dans le domaine spatial ou du numérique, s'appliquent au domaine civil (satellites, GPS, cybersécurité). Les investissements sont essentiellement concentrés dans les STIC (Sciences et Technologies de l'Information et de la Communication) afin que les USA puissent garder l'avance qu'ils ont dans la maîtrise de l'information, laquelle fournit aux acteurs économiques américains un instrument essentiel quant à la qualité de leur prise de décision.

---

[41] Melman, S. (1970), Pentagon Capitalism : The Political Economy of War, New York, McGraw-Hill. Lichtenberg, F. (1988), Governmeng subsidies to Private Military R&D Investment : DOD's IR&D Policy, NBER Working Papers 2745, National Bureau of Economic Research, Inc.

[42] Mampaey L., Serfati, C. (2004), « Les groupes de l'armement et les marchés financiers : vers une convention 'guerre sans limites' ? », in Chesnais F. (ed.), La finance mondialisée. Racines sociales, et politiques, configuration, conséquences, Paris, La Découverte, p. 223-251.

Cependant, la Chine et l'Inde rattrapent à grande vitesse leur retard, ils essaient de devenir les maîtres de l'information, l'arme efficace du début de ce XXIème siècle. Selon une étude de PWC (2015)[43], l'Asie devient la première région du monde pour les dépenses R&D, tandis que l'Europe prend du retard et que l'Amérique du Nord reste stable. Elle fait état de plusieurs observations intéressantes :

- La mondialisation de l'activité R&D devient la norme (94 % des entreprises ont une activité R&D en dehors de leur pays d'origine), au bénéfice des entreprises.
- En 2007, les dépenses R&D de la Chine ne comptaient que pour 23 % du total américain alors qu'en 2015, elles en représentent 38 %[44]. 80 % des investissements dans l'innovation dans ce pays proviennent d'entreprises étrangères.
- l'Asie est devenue la première destination des dépenses R&D des entreprises, représentant 35 % des investissements R&D, devant l'Amérique du Nord et l'Europe, notamment grâce à une augmentation importante, entre 2007 et 2015, des dépenses de R&D importées en Chine (79 %) et en Inde (116%), en provenance principale des Etats-Unis[45] ;
- L'Europe est passée du statut de première destination mondiale pour les investissement R&D des entreprises à la troisième place du fait de la faible croissance des investissements R&D domestiques et importés, couplée à une augmentation substantielle des exportations R&D vers des pays à coûts élevés comme l'Amérique du Nord ou l'Asie. L'UE se donne pour objectif à la fois d'obtenir des dépenses de R&D de l'ordre de 3% du PIB d'ici à 2020 et d'inciter leurs entreprises à s'aligner sur les contributions relatives observées au Japon et aux Etats-Unis. Depuis 8 années, en France, les 44 groupes français figurant dans l'étude de PwC (PriceWaterhouseCooper), ont réduit leurs investissements en recherche et innovation dans l'Hexagone de 20 % (de 20 à 16 milliards de dollars), malgré l'existence du Crédit Impôt Recherche. Cette évolution se retrouve aussi au Royaume-Uni.
- L'informatique/électronique (Samsung, Intel, Cisco ou Apple), la santé, l'automobile et les logiciels Internet (Microsoft, Google et Amazon) sont les quatre secteurs phare en termes de part du total des dépenses R&D en 2015. La part de la recherche sur les logiciels et Internet augmente de façon très importante toutes les années, notamment avec.
- Des dépenses élevées en R&D n'améliorent pas nécessairement les performances[46], mais les entreprises savent tirer parti d'une présence mondiale

---

[43] PWC (2015), 2015, global innovation 1000. Innovation's New World Order, Strategy&, 15 October. http://www.strategyand.pwc.com/media/file/2015-Global-Innovation-1000-Fact-Pack.pdf

[44] Soit une somme estimée par nos soins de 180.000 milliards de dollars (PPA), soit 3 fois plus que la France.

[45] La proximité des marchés à forte croissance et celle des grands sites industriels constituent les principales raisons avancées pour expliquer cette évolution.

[46] Le Général de Gaulle souhaitait à son époque non pas des recherches qui cherchent, mais des recherches qui trouvent.

diversifiée. On peut voir dans ces résultats les capacités de transfert de la valeur ajoutée de filiales à filiales pour optimiser l'impôt des sociétés. Volkswagen est l'entreprise qui engage le plus de financements dans la R&D au monde (15,3 milliards de dollars en 2015) pour un résultat qui n'est pas à la hauteur de l'investissement. Suivent Samsung, Intel, Microsoft, Roche, Google, Amazon et Toyota).

Aucun pays n'est cependant à l'abri d'une mise en place de technologies militaires sophistiquées capables de modifier les stratégies des Etats adverses. Un Comité du MIT, critiquant les coupes budgétaires de l'Etat touchant à la recherche fondamentale, considère que les Etats-Unis risquent de passer au-delà d'un point critique en termes de capacités stratégiques, notamment dans les domaines des superordinateurs, des systèmes sécurisés d'information et de technologies de la défense[47]. Le leadership chinois sur les super ordinateurs depuis 3 ans lui semble inquiétant (quadrillions de calculs par seconde). Si les USA sont encore en avance concernant les applications commerciales des circuits intégrés, les mécanismes électroniques avancés et internet, ils n'ont plus beaucoup de marge concernant le domaine des circuits optiques intégrés (l'Europe et le Japon ont investi fortement dans ces technologies, mettant en situation de compétition l'industrie des semi-conducteurs américains de 300 milliards d'euros). Les Etats-Unis sont alors très vulnérables à une « cyber attaque », du type de celles qui ont touché Sony, des banques, des distributeurs et des grandes sociétés. Il en va de même dans les domaines de la photonique, de la « cyber sécurité » et du calcul quantique (dominé par les Chinois), un domaine qui assure le leadership en systèmes d'information sécurisés, pour la sécurité des communications à longue distance et l'usage du « super calcul » dans un monde où l'économie numérique tend à s'implanter.

La cyberguerre, ou la nouvelle menace

Le monde immatériel offre de nouvelles opportunités dans l'économie de la connaissance et de l'information, comme l'économie numérique, le marché du stockage des informations, les logiciels, l'essor des réseaux ou le commerce électronique. Il en résulte un potentiel de développement important dans les échanges politiques, sociologiques ou commerciaux propices à une amélioration sensible des conditions de vie des hommes. Cependant, au regard du pouvoir qui naît de chaque source d'information, les conflits d'intérêts commerciaux, politiques ou doctrinaux vont aussi s'exacerber dans les luttes humaines récurrentes. Dans ces conditions, si ce monde immatériel peut provoquer de nouveaux flux de croissance et de bien-être, il peut tout aussi bien déstabiliser les gouvernances des Etats ou des entreprises et porter atteinte aux droits des citoyens. La médiatisation extrême de chaque événement ou pensée en temps

[47] MIT (2015), The future postponed. Why declining Investment in Basic Resaerch Threatens a U.S. Innovation Deficit. A Report by the MIT Committee to Evaluate tyhe Innovation Deficit, April 2015.

utile ou immédiat implique son interprétation ou sa justification au regard des responsabilités individuelles ou collectives.

Le secteur quaternaire est caractérisé par la gestion économique des flux de données produit le secteur quaternaire. Son essor est incontestable, il est puissant, mais on n'en mesure pas encore tous les contours et la profondeur. Compte tenu du caractère virtuel des informations fournies, il se prête particulièrement bien à l'essor de la cybercriminalité. L'espace numérique offre de multiple possibilités de gains, pour des risques pénaux relativement réduits au regard des enjeux financiers et de structures juridiques en retard par rapport aux avancées des techniques de pillage, de contrôle ou d'intention de nuire qui sont aujourd'hui disponibles. Il s'agit d'une délinquance feutrée, fondée sur la valeur des données qu'elles soient globales, structurées ou personnelles. Elle s'appuie sur l'expérience des mécanismes complexes mis en place dans le secteur des banques, des assurances ou plus généralement des services, pour obtenir des avantages économiques jugés illégaux par la loi. Elle traque les renseignements concernant le potentiel concurrentiel des entreprises, la préparation des décisions des Etats surveillés ou l'identité des personnes. Les « data centers » vendent des informations confidentielles ainsi dérobées, permettant à son détenteur de recevoir directement des revenus ou de disposer d'un temps d'avance sur son concurrent pour améliorer ses parts de marché. Les « cyber délinquants » (hackers, « rogue states », ou entreprises de renseignements sur l'étal) visent les personnes, les biens et les services en vue d'en tirer des profits économiques, des rapports de puissance (par le chantage, par exemple) ou des informations sensibles utiles pour conduire leur propre stratégie. L'anonymat et la furtivité du réseau caractérisent l'action inamicale. Aujourd'hui, le fléau est important, mais mal connu. Or, les réseaux vont être de plus en plus attaqués par les « cyber pirates », dont l'action produira des effets négatifs sur l'ensemble des populations concernées. Des partenariats publics et privés devront être mis en place pour développer une assistance mutuelle, car les organismes publics ne sont pas en mesure de contrôler les actions ennemies ou illégales.

Chaque pays doit justifier ses actions sur la base de principes de bonne gestion, mais aussi de choix politiques, moraux ou religieux, notamment. Tout changement de cap est alors disséqué et l'importance des arguments qui justifient cette évolution fait l'objet d'interprétations différentes qui sont autant d'occasions de conflits. Ainsi, toute guerre est justifiée par la libération des peuples, en évitant d'invoquer les richesses naturelles des pays concernés. « La manipulation sur l'Ukraine réalisée dans l'intérêt stratégique d'un de nos alliés ou sur la Syrie pour les intérêts économiques régionaux d'un autre, montre que nos citoyens sensibles au droit des peuples à disposer d'eux-mêmes, continuent à être facilement abusés par des professionnels ayant compris leur mécanisme de

pensée »[48]. L'extrême cruauté d'une décapitation en direct sur les réseaux sociaux manifeste à la fois l'urgence du combat, l'insoutenable pureté de l'action et l'implacable volonté d'aller jusqu'au bout de la lutte, le mécréant n'étant qu'un obstacle infect à l'édification d'un califat rêvé. La guerre de l'information s'exprime aussi dans la philosophie ou la morale serinée chaque jour dans les journaux ou les médias souvent inspirés par des propriétaires fortunés qui défendent ainsi, directement ou indirectement, leurs privilèges ou leurs propres conceptions sociétales. Plusieurs analyses et questions fournissent des réponse quant à l'émergence des cyber armes et à la capacité des pays « attaqués » d'y faire face.

- L'information est une base essentielle du pouvoir.
- La question est de savoir quels sont les bases et les moyens de la guerre de l'information.
- C'est une guerre « tous azimuts.
- L'Etat « attaquant » s'abrite souvent derrière le statut des ONG.
- Quels sont les instruments de protection contre les cyber armes ?

a) « Knowledge is power » (Hobbes)

La « guerre de l'information » s'invite dans les choix stratégiques des Etats. Elle définit l'importance de cette matière première que sont la connaissance et le renseignement dans les stratégies des acteurs internationaux ou nationaux. La maîtrise de l'information permet de vendre à l'étranger ses propres technologies, ses standards, sa culture. La stratégie nationale d'information est une condition de la puissance, au même titre que l'industrie ou l'armée.

Pour le gouvernement américain, le système international a besoin d'un leadership fort. D'abord, les forces du marché ne garantissent pas la prospérité (les économies en transition en portent témoignage). Ensuite, la richesse sans intégration internationale ne produit pas une stabilité garantie, car les conflits peuvent être latents. Enfin, le processus d'intégration des économies nationales par la globalisation rend les conflits si onéreux au regard de l'importance des interdépendances sociales qu'ils apparaissent impossibles ; cependant, il doit lui-même être renforcé par un leadership politique puissant. Il s'agit alors pour les autorités publiques américaines de disposer d'un pouvoir de leader (ou de domination) sur l'information et les systèmes d'information et de contrôler instantanément les sources électroniques et humaines sous-jacentes qui nourrissent les systèmes de décision (économiques, politiques ou militaires). Cette connaissance implique aussi l'interprétation des signes donnés par les informations. Cependant les nations à forte intensité technologiques de

[48] Juillet, P. (2016), Préface, in Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015.

l'information restent vulnérables, car les transactions d'un certain nombre de secteurs (santé, paie, commerce électronique) sont réalisées par le canal d'une architecture ouverte, largement distribuée et disponible[49]. Dans ce contexte, le renseignement est l'ami indispensable de l'intelligence économique et militaire.

Les Etats, les organisations internationales, les entreprises ou même les individus commencent à prendre conscience de l'ampleur et de la gravité des « cyber attaques ». Pour l'ONU, elles menacent la paix et la sécurité internationale, car elles préfigurent les guerres du futur. Aujourd'hui, des accords ont été signés entre la Chine et des Etats-Unis sur la question du cyberspace[50].

La « cyber guerre » définit l'usage des systèmes et réseaux informatiques pour nuire à un pays. Elle est le fait d'acteurs publics dont les relations sont régies par le droit international. Le « cyber terrorisme » et le « cyber espionnage » ont des activités duales, mi militaires, mi civiles, alors que la cybercriminalité dépend plutôt d'acteurs privés. La « cyber guerre » se définit comme une stratégie qui utilise un ensemble d'instruments virtuels sophistiqués du « soft power » en vue de réduire l'efficacité des réseaux de communication de son ennemi potentiel, en vue d'affaiblir la fluidité de ses systèmes de décision centralisées et décentralisées, de créer des difficultés inattendues dans le système de direction de l'Etat ou des entreprises et de réduire, voire supprimer, sa capacité à se réorganiser sans les moyens informatiques nécessaires. Elle intervient aussi bien dans la sphère militaire que dans la sphère civile, dans le secteur public et le domaine privé, en toute légalité ou illégalité. Le gouvernement cherche à contrôler l'information et internet, en vue de dominer le cyberespace, pour disposer d'un instrument nouveau de puissance.
Puissante institution américaine, la NSA (National Security Agency) a aidé le gouvernement des Etats-Unis à comprendre et à traverser de nombreux conflits et crises, mais la médiatisation récente de ses secrets a rendu sa tâche plus difficile. En 2012, Edward Snowden a « cassé » le secret que Churchill et Roosevelt avaient réussi à imposer pour protéger ses activités au début de la guerre froide. Il ne faut pas que les ennemis des Etats-Unis et du Royaume-Uni (Allemands, Soviétiques, Russes ou Chinois) se doutent de leur propre capacité à percer le contenu des messages cryptés concernant la préparation ou les opérations militaires engagées à leur encontre. Les Européens avaient pourtant appris vingt années plus tôt l'existence du système d'espionnage mondial Echelon, engagé par les Five Eyes (USA, Royaume-Uni, Canada, Australie,

[49] Bensahel-Perrin, L., Fontanel, J. (2010), L'intelligence économique, un facteur de sécurité internationale, Economie politique de la Sécurité Internationale (Ed. Jacques Fontanel), L'Harmattan, Paris, 2010. Fontanel, M, Fontanel, J. (2013), L'intelligence économique, une activité d'intérêt public et privé, in Entrepreneuriat, PME durables et réseaux sociaux (Thierry Levy-Tadjine et Zhan Su), en l'honneur du Professeur Robert Paturel, CEDIMES, L'Harmattan Paris, 2013

[50] Gewin, V. (2016), Climate Change Adds Urgency To Push to Save World's Seeds, Yale – Environment 360 – Report – April 21, http://e360.yale.edu/feature/climate_change_adds_urgency_push_save_worlds_seeds/2985/

Nouvelle-Zélande) qui a défrayé la chronique, mais les attentats terroristes du 11 novembre 2001 avaient semblé a posteriori justifier ce programme, malgré l'échec de son action[51]. La militarisation d'Internet permet de comprendre les modalités d'action et les stratégies des ennemis et amis potentiels en vue d'améliorer sans cesse la capacité et la liberté d'action technologique des Etats-Unis.

Depuis 1990, la NSA siphonne toutes les informations communiquées électroniquement, les métadonnées et le contenu des messages. Une gigantesque toile d'araignée de capture d'informations est mise en œuvre et l'organisation est protégée par le plus grand secret, avec des budgets croissants et colossaux (classifiés pour la NSA, de l'ordre de dix à onze milliards de dollars). La collecte (phisting expedition) est massive, avec des infrastructures sur écoute (Upstream System) et la collecte des données sur les serveurs des opérateurs (PRISM system). Le captage peut être ciblé grâce à des filtres ou des sélecteurs. Certains programmes (Stormbrew) sont menés en association avec le FBI. Microsoft, Yahoo, Google, Facebook, YouTube, Apple ou Skype sont devenus partenaires de PRISM., même si seules les personnes vivant en dehors des Etats-Unis sont normalement ciblées. « Le programme Muscular fonctionne clandestinement et illégalement en complément de PRISM. Il permet de surveiller, avec la complicité du GCHQ britannique, les serveurs de Google et de Yahoo [52] en infiltrant des parties de l'infrastructure interne des deux entreprises »[53]. L'exploitation des données est faite par des algorithmes qui détectent les modes opératoires et les anomalies. Seul le contenu intéressant est mémorisé dans des bases spécifiques

La quête de l'hégémonie dans les réseaux d'information est à la fois une ambition secrète et prioritaire. Encore aujourd'hui, les « lanceurs d'alerte » connus sont particulièrement peu protégés, ils sont accusés d'espionnage, d'atteinte à la sécurité du territoire pour tout ce qui concerne les informations stratégiques, ils sont obligés de vivre en exil (Assange ou Snowden) ou alors ils sont exclus des entreprises qui les emploient, poursuivis par la justice, avec bien peu de facilité de retrouver un travail équivalent à celui qu'ils avaient préalablement exercé[54]. Sur ce plan, les forces militaires s'avèrent inadaptées pour contrôler l'information, les outils et les réseaux de communication. L'interconnexion des ordinateurs réduit le potentiel de sécurité et d'invulnérabilité d'un pays et de ses habitants. Les Etats-Unis imposent les standards et les lois internationales du fait de sa puissance technologique, ce qui

---

51 Carter Clarke ancien Directeur Signal Intelligence Service « Ce sont nos amis aujourd'hui et ils seront nos ennemis demain, renseignez vous sur eux autant que vous pouvez tant qu'ils sont à vos côtés, car vous ne pourrez pas le faire quand ils deviendront vos ennemis ». in Delesse, C. (2016), NSA. National Security Agency. Tailladier, Paris. P. 21.

52 Google et Yahoo ! affirment ne pas avoir été au courant de ces pratiques.

53 Delesse, C. (2016), NSA. National Security Agency. Tailladier, Paris., p.191.

54 Vasseur, Q. (2016), Edward Snowden, Stéphanie Gibaud, Hervé Falciani… Que deviennent les lanceurs d'alerte ? Le Monde, 12 Avril.

lui permet de gérer des données importantes susceptibles de favoriser sa défense, ses entreprises, ses objectifs. Le Pentagone dispose d'une Commande cybernétique (Command Cyber), en vue de répondre aux attaques ou de mener une action offensive dans le « cyberspace ».

Les autres pays développés sont les plus menacés par ce risque de guerre, car ils sont tributaires, pour la plupart de leurs décisions, de l'aide des réseaux informatiques et des systèmes de communication. La complexité de la gestion des infrastructures civiles et militaires des Etats suppose un équipement d'ordinateurs sophistiqués, sans lesquels le stockage d'information et l'aide à la décision deviennent obsolètes. De même, les informations confidentielles des Etats n'échappent pas au risque de fuite, même si le réseau de ceux qui peuvent les connaître est particulièrement sécurisé. L'arme cybernétique a été utilisée par Moscou contre l'Estonie, puis la Géorgie, et les virus foisonnent avec des effets indéterminés au regard du silence qui entoure leurs réussites ou leurs échecs[55]. Les révélations d'Edward Snowden[56] ont mis en évidence l'ampleur de la surveillance dans les démocraties concernant les données personnelles des responsables politiques et industriels.

La quête de l'information, ressource stratégique à voler ou à détruire, peut conduire à un conflit électronique. Les virus et infections créées sciemment pour contraindre un ennemi ou le rendre plus vulnérable sont des attaques sournoises qui bloquent les systèmes de commande et la transmission d'informations. Plusieurs méthode d'attaque coexistent, de la propagande, à la désinformation, des données erronées au sabotage des infrastructures, de la panne programmée des ordinateurs au contrôle des références financières et bancaires, en passant par l'interception des commandes ou la neutralisation des infrastructures. Les maladies de l'intelligence économique sont l'espionnage industriel (illégalité dans la recherche de l'information, atteinte à la vie privée), les virus, le piratage informatique ou les écoutes téléphoniques. Les ordinateurs et autres systèmes d'information et de communication forment alors les premières cibles. « L'info guerre » met en évidence la lutte pour le contrôle de l'information, élément clé de pouvoir et de richesse dans le monde contemporain.

b) Les fondements et les moyens de la guerre de l'information

La cyberguerre est un concept flou, qui n'est pas compris à la mesure de sa menace par les principaux intéressés (armée, services de sécurité, entreprises, société civile, notamment). Il s'agit d'une guerre dont les règles dérogent avec

[55] Entre 2009 et 2010, l'Iran a découvert être la cible de la cyber-attaque de Stuxnet. Il s'agit, en fait, d'un ver informatique conçu par la NSA pour s'attaquer aux centrifugeuses iraniennes d'uranium. L'Iran a subi des pertes réelles sur plus d'un millier de centrifugeuses et son processus d'enrichissement d'uranium a été ralenti. Il s'agissait d'un acte de sabotage plus que d'un acte de guerre.

[56] Snowden Edward est un informaticien américain, ancien employé de la CIA et de la NSA (National Security Agency) qui a révélé, dès juin 2013, au monde plusieurs programmes se surveillance de masse opérés par les Etats-Unis et le Royaume-Uni.

celles qui prévalent lors des conflits entre les entités politiques, commerciales ou philosophiques. Elle ne suppose aucune déclaration de guerre[57]. Elle offre un avantage immédiat important, voire parfois décisif, à l'attaquant. L'agresseur n'étant pas toujours clairement identifiable, il n'y a évidemment ni traité de paix, ni arrêt marqué des hostilités. Tout ce qui concerne les actions de renseignements sont secrètes et leur divulgation prohibée. Il est clair que certains pays (Etats-Unis, Russie, Israël) ou groupes organisés (Daech ou Al-Qaeda) sont passés maîtres dans les stratégies d'influence de l'opinion publique mondiale, notamment lorsque leurs intérêts impliquent à terme des actions diplomatiques et militaires.

Lors de la seconde guerre mondiale, la Grande-Bretagne de Churchill a mené une guerre de l'information efficace, grâce notamment à sa capacité à décrypter les messages de l'Allemagne nazi et aux opérations d'intoxication et de désinformation. Elle a pu ainsi empêcher les Allemands de déterminer les lieux et les dates du débarquement en Normandie. L'URSS a aussi été un Etat pionnier en la matière, en fournissant des informations erronées concernant la nature exacte du système socialiste, ce qui a conduit une partie importante de l'intelligentsia occidentale à partager ses combats, en lui offrant une plus grande légitimité. Dans ce cadre bien construit par les « soldats de l'information », l'URSS s'est présentée comme le défenseur des pays dominés par l'impérialisme inhérent au capitalisme. Dans ce contexte, les organisations internationales ont été le lieu de nombreux conflits d'idées, avec un soutien indiscuté de l'URSS en faveur des pays « exploités » et des mouvements de libération nationale. Par cette position renforcée par la propagande, l'URSS détenait une arme puissante, efficace, celle d'un pays faible économiquement face aux pays capitalistes dominants. Il a fallu les actions de répression de l'Etat soviétique à l'égard des pays amis en révolte et l'émergence des dissidences pour que le soutien actif des intellectuels s'érode face à la cruauté des faits et le cynisme des politiques militaires engagées.

Dès 1947, une nouvelle forme de guerre de l'information a été engagée en vue de lutter contre l'influence soviétique dans les milieux politiques, intellectuels et culturels du monde occidental, avec le lancement du « Congress for Cultural Freedom ». La guerre psychologique, les combats idéologiques, le renseignement et la manipulation des connaissances ont été expérimentés, mais la « stratégie du faible au fort » semble toujours l'avoir emporté pendant la Guerre froide. Les Etats-Unis ont eu à souffrir de l'expérience vietnamienne pour se rendre compte de l'écart entre les résultats militaires et le regard porté par l'opinion publique mondiale. Ho Chi Min a su instrumentaliser les journalistes américains pour renvoyer sur tous les médias une image honteuse des exactions de l'armée des Etats-Unis. En revanche, les violences des Vietcongs n'étaient pas retransmises, ni même parfois connues. De même, pour

[57] Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015

les responsables d'une stratégie du « faible au fort », il ne s'agit pas de gagner la guerre militaire, mais de remporter l'onde de choc « médiatique ». Ainsi, le Hezbollah ou le Hamas ont souvent provoqué sciemment les frappes aériennes israéliennes, en installant leurs propres armes au milieu de la population civile, ce qui leur permettait ensuite de dénoncer des actes de guerre contre des innocents, grâce à une couverture télévisée (notamment d'Al Jazeera) particulièrement démonstratrice du sang libanais ou palestinien versé[58].

L'information est contrôlée, volée, pillée et travestie, elle s'inscrit parfois dans les schémas de propagande ou de contre propagande en vue de magnifier certaines actions ou pensées et d'en dénigrer d'autres, d'exercer des pressions politiques, psychologiques ou économiques en vue d'accroître l'essor d'intérêts collectifs ou particuliers au détriment d'entités ciblées et, sur la base d'informations triées ou produites volontairement sans souci de vérité, de manipuler la production des connaissances politiques, scientifiques, médiatiques ou factuelles[59]. Aujourd'hui, ces actions ont une efficacité redoutable, car les systèmes intégrés d'information font l'objet d'actes de malveillance comme les virus, le piratage, l'élimination des informations compromettantes ou même la paralysie des communications sensibles.

En 2011, Barack Obama a souhaité contrôler ces pratiques, mais celles-ci non seulement continuent à s'appliquer mais elles progressent encore. La NSA dispose d'une unité spéciale de hackers, Taylored Access Operations (TAO), qui a pour fonction de siphonner les données des ordinateurs, d'internet, de la téléphonie, et de déployer des moyens efficaces d'utilisation. Il s'agit de s'infiltrer dans les réseaux militaires russes et chinois, de rentrer dans les institutions commerciales européennes ou de lutter contre le terrorisme ou les cartels de la drogue. Le programme Quantum se propose de lutter contre les moyens similaires utilisés par l'armée chinoise, en vue de dérober les secrets militaires, technologiques et commerciaux. C'est un programme qui oriente les personnes physiques ou morales vers de faux sites, afin de pénétrer ainsi dans leurs ordinateurs pour y installer des chevaux de Troie. Ils espionnent aussi les espions et tous les pays sont des cibles potentielles. D'autres systèmes s'engagent dans les opérations clandestines (Remote Operations Center) et obtenir les informations sans laisser de trace en piratant par exemple des téléphones portables de personnes susceptibles d'apporter les informations nécessaires recherchées. Pour justifier ces actions, les Etats-Unis rappellent qu'il y a eu plus de 30.000 tentatives de craquage du système de défense du Pentagone.

La guerre totale contre le terrorisme exigée par le Président des Etats-Unis a permis à la NSA de disposer de plus de moyens, de bénéficier d'un niveau de

[58] Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015

[59] Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015

secret suffisant et d'élargir ses fonctions réglementaires. Elle a déclaré avoir déjoué une cinquantaine d'attentats, ce qui n'est pas prouvé et peut n'être qu'une manipulation pour justifier les entorses faites aux libertés civiles et aux règles fixées par la Constitution. Elle a pu disposer de nouveaux instruments, de nouveaux personnels (informaticiens, mathématiciens, et linguistes, notamment), elle na plus limité son action à la seule fourniture de en offrant des services analytiques aux pouvoirs publics. Soutenue par le complexe militaro-industriel, elle a engagé un programme ambitieux, Traiblazer, bien plus coûteux que nécessaire qui finalement ne sera pas engagé du fait d'employés désireux de protéger les termes de la constitution américaine sur le respect de la vie privée. Elle investit aussi dans la recherche sur l'intelligence artificielle, notamment sur la mise en production de drones militaires efficaces, mais aussi sur le projet Aquaint (Advanced QUestion Answering for Intelligence) qui propose de répondre à la question « Que pense X de Y ? ». Elle dispose enfin de partenaires efficaces du secteur privé, car la sous-traitance est recommandée par le Congrès concernant Internet et la fibre optique. La NSA noue des alliances stratégiques avec les firmes spécialisées, notamment IBM, General Dynamics, Verizon ou AT&T.

Cependant, la « guerre de l'information » ne produit que rarement des vainqueurs à long terme, elle affaiblit. Les services de renseignement ont limité leur recours aux techniques de désinformation et d'intoxication après la chute du Mur de Berlin, en laissant Bush s'engouffrer dans la brèche avec la présence, pourtant très improbable, d'Armes de Destruction massive dans l'arsenal militaire irakien. Le « leardership » américain sur les autoroutes de l'information n'a pas permis à Washington d'exporter pour autant son modèle dans les pays où il a souhaité intervenir. Ses échecs concernant notamment les révolutions de « couleur » de Serbie (2000), Géorgie (2003), d'Ukraine (2004) ou du Kirghizstan (2005) ou son départ d'Irak et d'Afghanistan sans avoir résolu les problèmes politiques, économiques et militaires de ces pays, mettent en évidence la difficulté des stratégies à mettre en œuvre et d'une efficacité partielle et temporaire des armes de l'information « partiale monopolisée ». Les Etats-Unis ont cherché à déstabiliser les pouvoirs en place en soutenant les ONG (souvent financées directement ou directement par des subventions publiques), des fondations privées ou publiques, les réseaux sociaux ou les mouvements d'étudiants opposés aux gouvernements en place sur la base d'informations spécifiques utilisées à bon escient en vue d'un soulèvement. Ainsi, L'« Alliance of Youth Movements » (AYM), organisation à but non lucratif, a développé des liens avec les cyber dissidents et a soutenu leur action d'internautes, en vue de combattre les pouvoirs en place. Dans ce contexte, il s'agit de créer une union des mécontentements et d'organiser l'orientation et la cible de l'action commune entreprise. Dans ce contexte, des gouvernements se protègent contre cette volonté de « leadership » par la censure d'Internet et des médias, ainsi qu'un contrôle policier renforcé.

c) Une guerre tous azimuts

Le combat pour l'information n'a pas de fin. Il favorise souvent l'attaquant, car la défense n'est pas toujours prête à répondre aux multiples actions nouvelles qui s'offrent aux assaillants. Les Etats-Unis et les terroristes de Daech et Al-Qaeda ont bien compris l'asymétrie dans l'interprétation des actions entreprises, soit pour maintenir un leadership, soit pour combattre un système philosophique et religieux honni. L'information vraie ou fausse constitue une arme d'appui aux stratégies politiques et géoéconomiques[60]. Les services de renseignement fournissent des systèmes d'information et de désinformation qui fragilisent, à faibles coûts, le pays ou l'entreprise cible. Les moyens techniques mis en œuvre sont parfois sophistiqués, mais dans d'autres situations ils peuvent être à la disposition d'un simple citoyen, avec des effets médiatiques considérables. Les groupes terroristes ont été en mesure de pirater des média (TV5 par exemple), avec des instruments qui n'impliquent pas d'importants investissements financiers et technologiques

Avant la fin de son dernier mandat, le Président Bill Clinton avait clairement exprimé l'ambition des Etats-Unis de détenir le leadership mondial sur le marché privé de l'information, au détriment de la règle de la concurrence toujours revendiquée par l'Etat américain sur l'ensemble des marchés. Aujourd'hui, les agences du gouvernement des Etats-Unis travaillent avec les sociétés numériques installées sur son territoire. Amazon accompagne ainsi la CIA à construire un espace de stockage de connaissances privées. Les Etats-Unis contrôlent l'infrastructure du web et une grande partie de son contenu avec l'essor des réseaux sociaux. Ce pays dispose d'un avantage très conséquent qu'il cherche systématiquement à fructifier à son avantage.

« L'Agence veut faciliter son accès aux informations les plus sécurisées et consacrerait annuellement 240 millions de dollars pour introduire des failles dans les systèmes de cryptages commerciaux, dans les réseaux informatiques ou les terminaux de communication commercialisés par Microsoft, RSA, Cisco et autres sociétés informatiques »[61]. Il existe une grande porosité entre les secteurs publics et privés aux Etats-Unis, et de fortes relations de connivence. Les opérateurs télécoms ont souvent accepté de fonctionner conformément aux demandes de la NSA, même si aujourd'hui ils sont un peu plus réticents et même inquiets du fait de la médiatisation de cette information. L'allégeance à la

[60] Daech souffre, mais son marketing lui permet de devenir, de facto, « une franchise de la terreur ». Plus le califat perd du terrain en Syrie et plus il devient un « cyber califat », qui devient le symbole des opprimés et des victimes de l'action impérialiste de l'Occident. Il dispose d'un pouvoir d'aimantation important pour polariser les énergies pour accomplir son propre dessein. Il justifie ainsi le « désir de crimes terroristes » pour donner un sens à une mort que la vie avant l'acte n'avait pas été valorisée socialement ni en termes de réussite, ni en termes de courage et d'exploits de guerre. Lioger, R. (2016), La guerre des civilisations n'aura pas lieu. Coexistence et violence au XXIe siècle,CNRS Editions. Paris.

[61] Delesse, C. (2016), NSA. National Security Agency. Tailladier, Paris., p.233.

NSA est moins évidente aujourd'hui, notamment la création de « backdoors ». En outre, la surveillance des personnels des entreprises impliquées (exemple de Gemalto) pose problème. Les opérateurs étrangers obtiennent ainsi des arguments supplémentaires pour s'implanter dans leurs pays, en soulignant le leadership, le monopole et la coopération des opérateurs américains avec leur gouvernement.

Depuis le scandale Edward Snowden, un contrôle plus étroit est opéré. Apple et Google sont concernés et renforcent leur système de cryptologie, au grand dam des autorités américaines. La question est cependant de savoir s'il s'agit d'une vraie méfiance mutuelle ou si cette opération de communication n'est qu'un leurre, pour ne pas fermer les marchés internationaux aux partenaires du gouvernement américain. Le Sénat a adopté le Freedom Act (juin 2015) limitant le pouvoir de surveillance de la NSA en contrepartie d'une prolongation de certaines règles définies dans le Patriot Act. La NSA rappelle pourtant que son activité est banale et légale, alors même que son action lui permet de s'affranchir de nombreuses règles, notamment en menaçant la vie privée ou les droits d'accès à l'information. Elle est souvent aux prises avec les enquêtes d'investigation des médias. Un document publié par le Washington Post met en évidence les budgets consommés, les cibles présentes et futures, les besoins en capacité, les sources et les méthodes utilisées. Aujourd'hui, le budget du programme de renseignement national (NIP) est de l'ordre de 50 milliards de dollars, dont 18 à des buts militaires (dont 30 % pour la cyber guerre), 15 pour la CIA et 11 pour NSA. Il est difficile de connaître le nombre de personnes affecté aux programmes de la NSA estimé cependant à 30 % des 107.000 employés à la communauté du renseignement américain, selon le Congrès américain. La cryptologie constitue une arme déterminante, mais les adversaires sont aussi de taille, notamment les opérateurs russes et chinois. On a même pu parler de guerre cryptologique, ce qui explique l'obsession du secret de la NSA, renforcé par plusieurs trahisons qui ont trouvé un écho auprès des médias, concernant notamment la surveillance des citoyens américains ou les enregistrements des transactions électroniques financières de la base internationale SWIFT.

La NSA est une source importante d'information pour les acteurs politiques, diplomatiques et économiques américains. Elle engage des collaborations importantes avec plusieurs pays, surtout d'ailleurs anglo-saxons. Elle a une relation de type « je t'aime, moi non plus » avec Israël et la France. Cela ne l'empêche pas de collecter toutes les informations sur l'Europe et les pays européens, comme l'ont révélé plusieurs scandales récents. De ce fait, les négociations transatlantiques ne bénéficient plus d'une ambiance confiante, notamment parce que l'espionnage économique s'est généralisé. Elle participe à la « compétition économique » entre les grands blocs de pays, à l'image des politiques d'imitation engagées dans les années 1980 par le Japon. Elle fournit des informations secrètes sur les licences d'exploration, sur les réserves

pétrolières, sur les grands contrats commerciaux impliquant l'intervention des gouvernements, sur les offres des concurrents des entreprises américaines (notamment celles qui appartiennent au complexe militaro-industriel), sur le développement des technologies nouvelles ou sur la gouvernance mondiale d'internet (notamment dans les pays comme la Chine, la Russie, mais aussi l'Europe). La NSA cherche à développer la souveraineté numérique aux Etats-Unis.

Les révélations Wikileaks et PRISM ont mis en évidence l'étendue de l'utilisation des armes de l'information et du sentiment d'insécurité qu'elles procurent[62]. En juin 2013, Edward Snowden, sur la base de près de deux millions de documents, révèle l'ampleur de la surveillance de masse mondiale opérée sur Internet, les téléphones portables et de tous les autres moyens de communication (rassemblement, analyses et stockage) effectuées par l'Agence Nationale de Sécurité (NSA) des Etats-Unis et les services secrets britanniques, au profit de son gouvernement, mais aussi de l'Australie, du Canada, de la Nouvelle-Zélande et du Royaume-Uni. Il s'agit d'un système d'espionnage sophistiqué des équipements informatiques à l'étranger, des institutions internationales et des câbles sous-marins de télécommunications intercontinentales. L'affaire PRISM pose la question de la souveraineté informationnelle des États. Appelé US-984XN, le programme de surveillance créé en 2007, avec la collaboration de Facebook, Apple, Google ou Microsoft, collecte les données personnelles (emails, fichiers, conversations, etc.) des personnes jugées suspectes par les services de renseignement américains. Cependant, ce type d'information supposée que le gouvernement américain a justifié en assurant qu'il avait pour objet la lutte antiterroriste a plutôt dévié vers une surveillance plus étroite et ciblée des hommes politiques, des managers ou des institutions dont on souhaite suivre ou connaître les comportements ou les valeurs. Ces informations n'ont pas permis de déjouer les attentats terroristes, car il est plus difficile de déterminer qui est potentiellement un terroriste actif. Avec cette « surveillance » de masse, chaque citoyen est soupçonné d'être potentiellement un malfaiteur.

En juillet 2013, le programme XKeystore de la NSA a permis de constater que les renseignements américains scannaient 150 sites Web, afin d'intercepter de nombreuses données en vue d'une analyse spécifique, avec un spectre de surveillance plus large et moins précis que PRISM, en vue de repérer les mouvements ou textes suspects. Les métadonnées (définies comme des

[62] WikiLeaks est une ONG fondée par Julian Assange en 2006. Elle a pour but de publier des documents et des analyses sociales, politiques et économiques souvent secrètes. Elle se propose de donner une audience aux lanceurs d'alertes et elle favorise les fuites d'information sécurisées. D'importants documents concernant la corruption, l'évasion fiscale, l'espionnage et les violations de droits de l'homme ont ainsi été diffusés. La sécurité du site est renforcée par l'emploi de technologies cryptographiques de pointe. Julian Assange est poursuivi par la plupart des pays pour violation d'informations secrètes, mais aussi pour viols en Suède. Mediapart et le Monde sont deux principaux organes de presse francophones qui publient ces informations lorsqu'elles ont été vérifiées. Cf Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015

informations qui peuvent être comprises par le Web) servent à étiqueter les ressources numériques (textes ou images), afin de faciliter leur classement et donc leur utilisation présente ou future. Ainsi, une photo peut fournir immédiatement des informations sur son auteur, comme la date de la prise de vue, son titre, les mots-clés associés ou le modèle d'appareil photo utilisé. Le Foreign Intelligence Surveillance Act (Fisa) justifie légalement des programmes de surveillance. Les services de renseignement de quelques autres pays, comme le Royaume-Uni ou l'Allemagne, ont pu aussi l'utiliser. En outre, le TAO (Tailored Access Operations) est une unité spéciale de la NSA dédiée au cyber-espionnage. Elle a piraté le réseau informatique du câble sous-marin de télécommunications SEA-ME-WE 4, auquel appartient Orange. Elle a récupéré des documents concernant la distribution des flux de données entre les différents nœuds du réseau. Elle aurait aussi procédé de même sur le câble SEA-ME-WE 4 qui relie Marseille, l'Afrique du Nord et l'Asie. Elle serait, de plus, capable de gagner un «accès passif» dans un ordinateur donné, en y installant un programme espion - une «porte dérobée», un accès à un logiciel ou à un matériel informatique, non connu de son utilisateur. Apple a toujours nié avoir participé à cette procédure. Enfin, utilisé notamment par Gmail ou Yahoo ! le protocole TLS (Transport Layer Security) est supposé sécuriser les échanges sur Internet, en rendant les données de leurs utilisateurs illisibles durant leur transit. Or, une faille importante a été découverte depuis peu, faille depuis longtemps connue secrètement par la NSA[63].

Les grandes firmes comme Apple, Google ou Yahoo ont été conduites à collaborer lorsque des demandes de données sont faites par la justice américaine, et sans doute par le gouvernement, même si elles s'en défendent. Elles sont sous pression après les révélations du programme américain de surveillance (PRISM). Il a fait l'objet de nombreux amendements, à la suite du 11 Septembre. Il autorise les autorités américaines à mener sous contrôle judiciaire des collectes de données à grande échelle, à condition de ne pas viser intentionnellement des citoyens américains ou vivant aux États-Unis. La résistance d'Apple en 2016 en vue de fournir les codes d'accès d'un téléphone ayant appartenu à un « terroriste » témoigne plus d'une volonté de « réparation » des informations fournies préalablement, aujourd'hui connues, sans référence aux exigences de la loi antiterroriste du « Patriot Act ». Il s'agit de se faire un peu de publicité à bon compte, tout en sachant que le secret des codes sera, peu ou prou, rapidement levé. Le refus d'obtempérer pourrait conduire le gouvernement des Etats-Unis de les accuser de haute trahison dans les cas les plus graves. En outre, lorsque la demande du gouvernement est autorisée par la justice, l'entreprise doit accepter, sans être autorisée à en révéler l'existence.

[63] Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015.

Pour Edward Snowden, la NSA[64] connait déjà les clefs de tous les systèmes de cryptage qui garantit le confidentialité des données sur Internet, grâce au système Bullrun. Il existe des collaborations secrètes entre la NSA (qui dispose d'un budget de 250 millions de dollars) et des sociétés éditant des services Internet, et des actions pour pénétrer dans les services les plus performants comme Google, Yahoo, Facebook ou Microsoft.

La problématique de la sécurité ne se limite donc pas à une approche technique des systèmes d'informations. Le facteur humain joue toujours un rôle essentiel. Au début des années 1990, le Secrétariat Général de la Défense Nationale voulait refuser l'utilisation d'internet dans le cadre administratif, ce qui a été rapidement rendu impossible. Il est devenu quasiment impossible de sécuriser le système Internet. Les entreprises comme les individus doivent en prendre conscience et insister auprès des autorités publiques pour définir des critères de protection applicables, au moins dans l'espace européen. L'essor de l'Open Data, souvent revendiqué par le GAFA, est parfois dangereux, s'il s'agit de limiter les contraintes techniques, financières ou juridiques destinées à protéger la diffusion des données. Un fort lobbying des autorités américaines dans les couloirs de Bruxelles est disponible pour en obtenir la mise en place et son développement.

Dans le monde des affaires, il est toujours nécessaire de distinguer les atteintes à la propriété intellectuelle (appropriation d'un savoir) et la violation du secret des affaires (recueil illégal d'informations stratégiques). Cette culture du danger n'est pas suffisante en France, ce qui conduit souvent à des procès mal engagés du fait des difficultés à faire valoir des droits insuffisamment protégés par la victime et des difficultés des magistrats à rendre justice dans le domaine de l'information immatérielle circulant via Internet. Il est nécessaire à la fois de travailler en réseaux mais aussi de se protéger des dérives légales ou illégales de ceux-ci. L'Etat doit construire des protections pour les entreprises de son territoire, afin de conserver les informations économiques, politiques ou militaires stratégiques hors de portée des entités publiques ou privées prédatrices ou malveillantes.

Les mesures préventives et défensives visent à protéger les firmes contre le pillage de leurs données ou le parasitage de leurs systèmes d'information. Aujourd'hui, nombre d'affaires touchant à l'honnêteté des firmes et de leurs dirigeants commencent à produire des vagues inquiétantes sur le chiffre d'affaires des cibles et sur leur réputation, grâce à des manœuvres de désinformation difficiles à contrecarrer à court terme.

d) Les ONG de type GONGO[65]

[64] Le Government Communications Headquarters (GCHQ) du Royaume-Uni a sans doute le même type de connaissance. Elle a peut-être découvert les portes d'entrée de Google.

[65] Parmi les organisations non gouvernementales, il faut distinguer les PINGO (Public Interest NGO) qui accomplissent des actions d'intérêt général financées par des organismes publics, les BINGO (Business and Industry NGO) qui défendent des intérêts particuliers, parfois même indirectement lucratifs, les GONGO

Le « National Endowment for Democracy » (NED) est une fondation privée à but non lucratif, à financement public, instituée par le Congrès américain le 22 novembre 1983 et confiée à un groupe de travail siégeant au sein du Conseil de sécurité nationale. Il se propose d'encourager et de renforcer les institutions démocratiques dans le monde entier, au bénéfice à la fois des forces démocratiques et des valeurs américaines. Il offre plus de 1000 financements dans près de 100 pays pour soutenir d'autres ONG qui travaillent en ce sens dans leurs pays. C'est une ONG est financé par des fonds publics votés par le Congrès, par le truchement de financements dédiés dans plusieurs agences gouvernementales. Cette quête d'une aide financière et idéologique des Etats-Unis n'est pas nouvelle. De nombreux mouvements de libération ont cherché depuis près de deux siècles à se nourrir de l'expérience et des aides matérielles des Etats-Unis. Chaque année, le NED offre des subventions directes, pour un budget croissant qui est passé de 15 à 20 millions de dollars avant la fin de la guerre froide à plus de 135 millions de dollars en 2010 (avec le soutien de trois associations, Smith Richardson Foundation, John M. Olin Foundation et Bradley Foundation). Les buts sont ainsi énoncés :

- Développement et respect de l'état de droit et des processus et institutions politiques démocratiques ;
- Renforcement et élargissement de l'économie de marché ;
- Respect des droits de l'homme et des idées et valeurs démocratiques ;
- Promotion de la liberté d'information, de l'éducation civile, de la transparence et de la responsabilité individuelle et collective ;
- Soutien accordé aux médias non gouvernementaux, aux organisations de la société civile et à la liberté d'association ;
- Assistance à la résolution démocratique des conflits

Il s'agit principalement de renforcer, par une action non violente, les efforts diplomatiques des Etats-Unis dans le monde, sans référence excessive pour le principe de souveraineté des États. Les Américains dans leur ensemble considèrent que leur démocratie est exemplaire et qu'elle doit être étendue au reste du monde. NED est directement impliquée dans le processus de promotion américaine de la démocratie. Des liens étroits et assumés existent entre la NED et la CIA. En outre, NED est soutenu par des associations gérées par quatre forces politiques des Etats-Unis, le syndicat AFL-CIO (ACILS, American Center for International Labor Solidarity), la Chambre de commerce des Etats-Unis (CIPE, Center for International Private Entreprise), le Parti Républicain (IRI, International Republican Institute) et le Parti Démocrate (NDIIA, National

---

(Governmental Oriented NGO) qui ont pour objectif de servir les intérêts de leurs gouvernements, les IINGO (Indépendant International ONG) qui disposent de filiales dans le monde entier, mais refusent les financements publics et les MONGO (my Own NGO) qui défendent des intérêts collectifs sans contrôle démocratique. Cf. Fontanel, J., Bensahel, L., Corvaisier-Drouart, B. (2009), Les organisations non gouvernementales Collection Librairie des Humanités, L'Harmattan, Paris. 2009.

Democratic Institute for International Affairs). Cela lui confère une légitimité dans la représentation et une certaine transparence[66].

Sur la base de ses principes, la NED encourage les mouvements de protestation, la désobéissance civile, le refus de coopération avec le gouvernement aussi bien dans les sphères politiques qu'économiques. C'est ainsi que Gene Sharp[67] a développé un programme de formation concernant les actions non violentes au Centre des affaires internationales de l'université d'Harvard et une Association (Albert Einstein Institution) dédiée à l'étude et à l'utilisation de l'action non violente stratégique dans les conflits à travers le monde en vue de soutenir les valeurs démocratiques. Son influence dans les milieux estudiantins a été importante dans les pays d'économie en transition. Une formation est organisée aux Etats-Unis (notamment par des accords interuniversitaires internationaux) pour les jeunes leaders des pays en ébullition politique. Il s'agit principalement de former des personnes acquises à l'idéologie libérale et démocratique aux techniques et méthodes de la résistance non violente à l'encontre des dictatures ou des régimes autoritaires.

Les résultats de son action ne sont pas négligeables. NED a soutenu Solidarnosc ou a favorisé le renversement de Milosevic en Serbie, mais il a aussi échoué dans le renversement violent de Chavez au Venezuela. Gene Sharp énumère les actions non violentes pour combattre les dictatures. Elles procèdent notamment par le dénigrement, la moquerie, l'information et la désinformation, les slogans, l'affichage, les T-shirts, les rassemblements populaires, Internet, les téléphones cellulaires, et des médias alternatifs, le renforcement des réseaux contestataires, le soutien des forces vives de la Nation (église, médias, syndicats, associations, régionalistes, etc..), des pétitions, des grèves, la défection individuelle ou collective des forces de sécurité (militaires, police, milices), le blocage des routes et des chemins de fer, l'occupation physique des bâtiments publics clés ou la lutte face aux barricades policières (terreau de la révolution). La violence officielle qui naît de ces actions conduit à une répression qui est rapidement discréditée par les médias internationaux. Il faut alors se rendre sympathique et crédible auprès des fournisseurs d'information, chercher à développer des rapports empathiques avec la police et l'armée, montrer les scènes de violence perpétrées par le pouvoir en place, médiatiser tous les morts, utiliser massivement les messages électroniques, montrer l'incapacité du pouvoir en place de régler le chaos existant. Ainsi, le « soft power » américain ne met en place en vue d'améliorer les rapports de force des Etats-Unis dans les Etats concernés par cette lutte[68]. Les questions propres à la liberté ou à la

---

[66] Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015

[67] Sharp, G. (1994) " La défense par actions civiles. Une proposition pour la défense nationale". Préface Jacques Fontanel, PUG, Grenoble, 1994. Sharp, G. (2009), De la dictature à la démocratie : Un cadre conceptuel pour la libération, Collection « La Librairie des Humanités, L'Harmattan, Paris.

[68] Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris, Mai 2015

démocratie sont, au moins à court terme, secondaires par rapport à l'exercice du « soft power » reçu par le système politique américain.

Fin avril 2016, la Chine vient de restreindre l'action des ONG étrangères travaillant en Chine, notamment celles qui travaillent dans l'humanitaire, l'environnement, la recherche académique ou les chambres de commerce[69]. Elles seront placées sous le contrôle de la police, après un agrément des services de sécurité. Elles pourront être expulsées, si elles portent atteintes aux intérêts nationaux, selon des critères qui ne sont pas clairement définis. Malgré les réactions des ambassades occidentales (et notamment américaines et européennes), les ONG étrangères devront communiquer leurs programmes de travail et leurs informations financières, elles ne pourront pas recruter de Chinois, ni faire appel à des fonds nationaux. Elle peut éventuellement autoriser des ONG à travailler temporairement avec des organisations nationales, mais celles-ci sont aussi contraintes à un contrôle « musclé ». Les ONG sont accusées globalement de comploter contre le Parti Communiste et son rôle déterminant dans le fonctionnement de la société chinoise. Les termes de « société civile », « démocratie » ou « liberté de la presse sont proscrits, afin de protéger la sécurité nationale. L'Etat de droit défini par le Président ne peut pas être contesté.

Les révolutions « vertes » du monde arabe, en quête de liberté, de démocratie, de paix, et donc à la recherche d'un essor significatif es indicateurs du développement humain national ont fait l'objet de cyber armes. Avec le nouvel ordre économique et politique mondial, les événements ne sont pas complètement maîtrisables. Le mouvement contestataire s'est rapidement développé, mais en même temps il a provoqué des effets contraires, entre la libéralisation et la recherche effrénée d'une société islamisée sous l'obéissance aux lois d'Allah et de la Charria. Les pays arabes avaient échoué dans la construction d'Etats modernes, en supportant des régimes autoritaires, corrompus et répressifs, sans oppositions politiques significatives. Or, les inégalités sociales, l'appauvrissement des classes moyennes et le faible avenir promis aux plus jeunes ne pouvaient que conduire progressivement aux contestations d'un peuple de plus en plus informé par les réseaux sociaux internationaux. Dans ce contexte, la désobéissance sociale a été respectée par de nombreux groupes et individus, en vue de faire céder les pouvoirs en place pour un respect des libertés et le refus des inégalités aussi croissantes qu'injustes. Le gouvernement américain a cherché à améliorer son image par le canal des médias sociaux et des technologies de l'information. En Egypte et en Tunisie, les internautes représentent une population nombreuse, respectivement 19 % et 33 % de leur population, sans doute recensées parmi les couches sociales les plus éclairées. L'action des Etats-Unis a été efficace, en fournissant des

[69] Pedroletti, B. (2015), La Chine prépare une loi pour museler les ONG, Le Monde, 4 Avril. AFP (2016), La Chine adopte une loi très restrictive pour les ONG étrangères. 28 Avril

messages vérifiables, mais aussi des campagnes de désinformation efficaces en direction des cuber activistes. Elle a proposé une aide en relation avec les experts des nouvelles technologies, en vue d'exporter la démocratie « à l'américaine ». En revanche, les services de téléphonie et d'Internet ont été interrompus sur ordre des autorités égyptiennes aux quatre fournisseurs d'accès des routes BGP (Border Gateway Protocol), isolant la quasi-totalité des groupes d'adresses pendant 5 jours. Les Etats-Unis ont soutenu financièrement les entreprises et les ONG fabriquant des logiciels anti censure (fournis gratuitement, ainsi qu'une formation d'emploi) pour contourner les ordres des régimes autoritaires.

Les terroristes sont devenus d'excellents internautes. Ils se servent des médias pour structurer leurs modes d'action. Ils utilisent la violence insupportable, la manipulation des médias, l'excès dans les demandes politiques et le chantage émotionnel. Il faut d'abord faire parler de soi et justifier la légitimité des actions entreprises. Ils donnent une grande publicité à leurs actions, en justifiant la « pureté » de leurs motivations, mais ils succombent aussi à la surenchère. Lorsque Daech annonce en 2014 la création du Califat, il donne un sens à la guerre qu'il entreprend sur les territoires conquis de la Syrie et de l'Irak. Il s'agit alors d'imposer la loi islamique, de détruire les frontières territoriales des Etats et de créer un Emirat islamique qui attirerait à termes les musulmans du monde entier. Pour satisfaire cet objectif, la gouvernance sans exclusive ni opposition des territoires occupés est alors possible dans le respect des règles d'Allah. Daech dispose de nombreux soutiens de cybernautes compétents, en, vue de manipuler les réseaux sociaux. Son organisation possède les capacités de commande et de contrôle, qui lui permet de recruter ses partisans et d'expliquer son message sur les autoroutes de l'information. La provocation par la terreur permet de rejeter encore plus violemment les valeurs humanistes qui sont promues dans les sociétés occidentales. En mesure de rétorsion, les ennemis de Daech se doivent de mettre en évidence les contradictions internes par une relecture du Coran, de limiter le potentiel des recrutements nouveaux en contrôlant les sources de propagande et de souligner l'illégitimité des actions entreprises par le terrorisme.

Le rôle de Wikileaks a été considérable. Il a mis en évidence l'importance de l'action des Etats-Unis en faveur des organisations non gouvernementales pour soutenir la démocratie, le respect des droits de l'homme (notamment le refus de la torture), la transparence du système politique, la lutte contre la corruption, l'influence économique excessive de l'armée, l'emploi des jeunes (notamment diplômés). Dans ce contexte, la chaîne Al Jazeera va monnayer son soutien aux Etats-Unis en acceptant de ne pas continuer à critiquer la politique du gouvernement américain.

e) La lutte contre les instruments de la cyber guerre

Pour échapper à ce type de conflit que l'on pressent très violent, les Etats commencent à réfléchir à l'élaboration d'un droit international, mais aujourd'hui le consensus est difficile à obtenir. La militarisation du cyberespace est susceptible d'être qualifiée d'agression selon son niveau d'intensité et ses effets sur les personnes et les biens, mais il n'y a pas de traité international sur la définition d'un acte de cyber agression. Néanmoins, plusieurs initiatives ont été mises en œuvre au niveau national et régional, mais également au niveau international au sein des Nations Unies, dans le domaine du cyber.

La pensée militaire privilégie la stratégie dite du « zéro mort », ce qui donne plus de poids à la NSA. L'espionnage économique et technologique est lui-même encouragé. Il devient même une priorité nationale, officiellement pour faire la chasse à la corruption. Avec la création du National Economic Council en 1993, Bill Clinton accepté l'idée de l'espionnage des communications commerciales. Globalisation, déréglementation, dérégulation, compétition deviennent les « maîtres mots » du maître de Washington, malgré la percée des menaces terroristes. La NSA perd un peu de son importance auprès du Chef d'Etat, ses crédits sont réduits, elle a mauvaise presse, elle échoue dans sa lutte antiterroriste, elle en profite pour s'abriter derrière un plus grand secret dans son antre de SigInt, entre Washington et Baltimore. En 2000, à la suite d'un crash informatique de la NSA, une opération de modernisation informatique et téléphonique de 5 milliards de dollars est décidée sous le contrôle de Lockheed Martin. La NSA s'engage alors fermement dans la R&D. Le passage des technologies analogiques à celles du numérique ou l'utilisation de la fibre optique complique les missions de la NSA. Dans ce contexte, il s'agit de piéger les machines pour accéder aux systèmes et aux données, avec des logiciels espions au cœur même des disques durs fabriqués par les sociétés comme Toshiba ou Micron. NSA travaille en coopération avec d'autres organismes publics et privés sur les nouvelles générations de superordinateur, notamment avec des laboratoires universitaires. Il s'agit à la fois d'attirer les meilleurs experts en informatique, mathématiques, physique, chimie, sciences cognitives, etc.

En 2013, l'Union européenne a mis en place le Centre européen de lutte contre la cybercriminalité. Le Manuel de Tallinn (2013) sur le droit international applicable à la « cyber guerre » a été rédigé par un groupe d'experts du Centre d'excellence pour la « cyber défense » de l'OTAN, en vue de montrer comment les normes juridiques internationales existantes sont également applicables au cyberespace. Les experts internationaux mettent en avant les principes d'humanité, de nécessité, de proportionnalité et de discrimination [entre les combattants et les non-combattants), ainsi que des «normes de comportements» comme l'absence d'attaque contre les infrastructures critiques, la coopération entre les Etats pour renforcer la sécurité des systèmes essentiels ou la prévention de l'utilisation de fonctionnalités cachées malveillantes, notamment les « backdoors » chers aux produits américains. Le Manuel de

Tallinn, qui devrait connaître un prolongement en 2016, n'est pas contraignant, et aucun Etat accusé ne peut faire l'objet de sanctions sur cette base. Les Etats ne sont donc pas obligés d'appliquer ou de respecter les mesures définies dans le Manuel, par ailleurs contesté par l'Europe ou la Russie par son interprétation reflétant la vision américaine du droit international. Le problème c'est qu'il n'y a aucun consensus sur la notion de « cyber guerre. En France, le Directoire Central de l'Intelligence Nationale dirige « l'intelligence service », il combat le terrorisme, il contrôle les mouvements sociaux, il conduit un service contre l'espionnage industriel. Il s'agit de protéger les industries nationales des actes délictueux des concurrents étrangers.

Les bombardements français en Syrie posent ainsi plusieurs problèmes, au regard de l'utilisation du combat numérique que le droit international ne semble guère avoir encore maîtrisé[70]. Il s'agit de combiner la cyber compétence avec les autres armes disponibles sur le théâtre d'opérations. Ensuite, comment aborder la « judiciarisation » croissante des conflits et l'adaptation du droit aux nouvelles menaces en provenance des « zones grises » ? Enfin, comment justifier et qui décide dans la lutte informatique intensive engagée par l'Etat-Major contre les ennemis ? Dans ce contexte, la France attaque, elle ne se limite plus aux tâches défensives dans l'utilisation de cette arme nouvelle, laquelle renforce les moyens de coercition non seulement sur les théâtres d'opération sur terre, en mer, dans l'air, ou dans l'espace extra atmosphérique, grâce à l'utilisation du cyberespace et du numérique. Elle suit dans cette démarche le gouvernement des Etats-Unis décidé à mener des « cyber attaques », accompagnant ou non, les moyens conventionnels d'action.

Le gouvernement américain a engagé une procédure contre Apple pour contraindre cette société à respecter une décision de justice lui demandant de l'aider à recueillir les informations disponibles dans l'iPhone d'un terroriste. C'est l'une des premières interventions publiques de ce type qui soit connu, notamment parce que le gouvernement a dû aller en justice pour obtenir ce droit face au refus du PDG, Timothy Cook, qui souhaite préserver la sécurité des consommateurs d'Apple. Le gouvernement américain a clairement demandé de construire une « porte d'accès cachée sur l'iPhone », disponible lorsque la sécurité de l'Etat est concernée. Ce n'est sans doute qu'un des premiers soubresauts des conflits à venir. Il est intéressant de constater que les autres fabricants américains n'ont jamais fait état d'une telle demande, ce qui peut laisser supposer soit que le combat vient seulement de s'engager, soit que celui-ci a déjà été remporté par l'Etat, dans le plus grand secret. Sur ce point Apple a été soutenu par Facebook et Twitter, alors que Bill Gates et McAfee soutiennent le FBI.

La responsabilité de la NSA dans les attentats du 11 septembre 2001 est engagée. « Nous ne savions pas que nous savions ». C'est la faillite du

[70] Alonso, P. (2015), Existe-t-il un droit de la cyberguerre ? Libération, 3 novembre.

renseignement américain, celle de la surveillance massive de la NSA et de son complice britannique GCHQ. Le CIA, le FBI et la NSA sont au banc des accusés. Dorénavant, l'objectif est de savoir et d'empêcher les autres de savoir, grâce au cyber renseignement. La « cyber attaque » n'est pas toujours bien définie et si elle est exprimée ou prouvée elle provoque de graves effets diplomatiques. Il s'agit non seulement d'être informé par tous les moyens (infiltration des systèmes et vol de données), il s'agit aussi d'introduire des « malware » qui infectent les données des ennemis, adversaires, concurrents, voire parfois amis. De nombreux virus permettent à celui qui les a lancés de disposer d'un temps d'avance sur les autres acteurs concernés, juste avant que celui-ci ne les découvre et s'en guérit. La guerre électronique suppose la recherche constante de la maîtrise de l'information et la protection ses infrastructures les plus vulnérables. La guerre cybernétique est envisagée. Depuis 2010, les Etats-Unis disposent officiellement de l'USCYBERCOM, un commandement interarmées de combat, sous la Direction de l'US Strategic Command. Il exerce une fonction essentielle de protection militaire, mais aussi une mission de sécurité nationale en protégeant les réseaux informatiques et leurs infrastructures. Avec les TAO (hackers) et les Five Eyes (alliance avec l'Australie, le Royaume-Uni, la Nouvelle-Zélande et le Canada), il est chargé de traiter les questions relatives à une guerre cybernétique, avec l'essor des instruments de surveillance, la capacité de destruction des réseaux ennemis et le contrôle en temps réel de toutes les opérations de « cyber attaque » et de « cyber »défense ».

Les services nationaux responsables de la gestion de l'intelligence économique sont aussi concernés, car ils doivent à la fois protéger le pays contre la prédation de son héritage technologique ou économique, entreprendre une guerre de l'information pour gêner un rival, mais aussi savoir ce qui se fait dans les autres pays afin d'anticiper les sauts épistémologiques ou de prévoir l'émergence de nouveaux types de concurrence ou de forces de pays ennemis et même amis. Il a pu être mis en évidence que les VPN d'entreprises qui servent à protéger les données confidentielles ont pu être exfiltrées à distance par la NASA[71].

Dans le domaine de la « cyber guerre », les Etats-Unis ne jouent pas encore en maître. De nombreux pays sont engagés dans ce nouveau terrain de bataille où il s'agit non seulement de savoir mais aussi d'influencer, de tromper, de manipuler. Une longue et coûteuse préparation des armes doit être engagée, sans être certain de disposer d'avantages décisifs sur les pays ennemis, adversaires ou concurrents. En août 2012, 30.000 ordinateurs d'Aramco ont été infectés, sans doute une opération lancée par Téhéran. Les attaques sont très coûteuses pour ceux qui en subissent les effets, il en est de même de la chasse

[71] Kallenborn, G. (2016), La NASA a pu déchiffrer les données secrètes d'entreprises pendant des années, 01net.com, 19 Août. http://www.01net.com/actualites/la-nsa-a-pu-dechiffrer-les-donnees-secretes-d-entreprises-pendant-des-annees-1027725.html

aux hackers. La guerre des câbles, facteur de liberté d'action, est engagée. La Chine met en exploitation en 2016 une boucle de communication quantique de plus de 2000 kilomètres, ce qui est considérable. Ce système n'est pas susceptible d'être piraté du fait de l'utilisation de la « cryptographie quantique ». L'Europe et le Brésil pensent aussi s'organiser à terme dans cette voie. Cette méfiance à l'égard des Etats-Unis devient généralisée.

Cependant, les armes « cyber technologiques » sont encore dominées par les Etats-Unis. Elles permettent d'échapper à l'éventualité d'une destruction nucléaire ou d'engager des conflits longs et très couteux. Elles se distinguent par la souplesse de son action ciblée, par sa violence apparente réduite ainsi que par son caractère clandestin. Les guerres s'expriment de moins en moins dans l'ordre militaire, l'ensemble de la population d'un pays, son économie, sa sociologie, sa diplomatie, sont concernés. Au regard de la force de ces instruments de conflits, les Etats-Unis redoutent les systèmes d'espionnage de la Chine et de la Russie (qui dispose probablement d'un Cyber Command)[72]. Dans ce domaine, l'innovation est une question de survie politique, militaire et économique. Or, la Chine semble aujourd'hui avoir une avance significative dans le cryptage des informations, en lançant le 16 août 2016 un satellite de communication quantique destiné à tester l'envoi de clés hyper sécurisées. Les Etats-Unis ont pris du retard du fait de « l'instabilité des financements ». Dans le même temps, un groupe de pirates, The Shadow Brokers, a dérobé des outils d'espionnage informatique du groupe Equation de la NSA, ce qui a été confirmé par la firme russe Kapersky, spécialisée dans la sécurité informatique. La Russie est accusée d'être responsable d'être responsable de ce piratage, mais Moscou nie cette implication. Cette course aux armements peut soulever deux problèmes, la menace d'un système militaire extrémiste et même la création d'un système totalitaire privé[73].

Bibliographie

AAAS (2016), Historical Trends R&D Budget and Policy Program, http://www.aaas.org/page/historical-trends-federal-rd

Bensahel, L., Fontanel, J., Corvaisier-Drouart, B. (2009), Les organisations non gouvernementales Collection Librairie des Humanités, L'Harmattan, Paris. 2009.

Bensahel-Perrin, L., Fontanel, J. (2010), L'intelligence économique, un facteur de sécurité internationale, Economie politique de la Sécurité Internationale (Ed. Jacques Fontanel), L'Harmattan.

Biad, A. (2015), Traité sur le commerce des armes, PSEI, Numéro 2, , mis en ligne le 21 novembre 2015, URL : http://revel.unice.fr/psei/index.html?id=671

Cars, H.C., Fontanel, J. (1987), Military Expenditure Comparisons, in "Peace, Defence and Economic Analysis", Editors, C. Schmidt, F. Blackhaby,The International Economic Association, Mac Millan, London

Cornetta C. (2015), Economists for Peace & Security, Newsletter, Volume 27, Issue 1, March.

[72] La Russie a créé un consortium unifié e construction des appareils de précision pour équiper son armée de systèmes modernes de communication et de gestion de combat. .Demesse (2016), Op.Cit. p. 353.

[73] Delesse (2016), Op.Cit. p. 381.

Coulomb, F., Fontanel, J. (2000), Disarmament in the Next Millenium, Defence and Peace Economics, Volume 11

Coulomb, F. et Fontanel, J. (2003), Disarmament: A century of economic thought. Defence and peace economics, vol. 14, no 3, p. 193-208.

Coulomb, F., Fontanel, J. (2005), An economic interpretation of French military expenditure, Defence and Peace Economics, 16(4),

Coulomb, F., Fontanel, J. (2006), Le coût du nucléaire en France et son avantage comparatif, in Pascallon (Ed.), La sécurité de la France, Economica, Paris,

Coulomb, F., Bensahel, L., Fontanel, J. (2007), The concepts of economic war and economic conflicts in a global market economy, in « Arms, War, and Terrorism in the global economy today, LIT Verlag, Hamburg.

Deger, S., Smith, R. (1983), Military expenditure and growth in less developed countries ; Journal of Conflict Resolution, Vol.27,n°2.

Delesse, C. (2016), NSA. National Security Agency. Taillandier, Paris.

Dunne, P., Smith, R. (1990), Military expenditure and unemployment in the OECD, Defence Economics, Vol.1, n°1.

Eurostat (2015), Dépenses de R&D, http://ec.europa.eu/eurostat/statistics

Fontanel, J. (1980). Le concept de dépenses militaires. Défense Nationale

Fontanel, J. (1982). Military Expenditure and Economic Growth: France, Morocco. report written for the United Nations, New York.

Fontanel, J., & Smith, R. (1985). Analyse économique des dépenses militaires. Stratégique, Fondation, Paris

Fontanel, J. Smith, R.P. (1987), The creation of an International Disarmament Fund for Development, in "Defence, Security and Development" (Deger, S. et West R., Ed.), Francis Pinter, London, June

Fontanel, J, Smith, R. (1990), The impact of strategy and measurement on models of French military expenditures, Defence Economics, Vol.1, n°4.

Fontanel, J. (1990), The economic effects of military expenditure in Third World Countries, Journal of Peace Research, Vol. 27, n° 4, November 1990.

Fontanel, J., & Smith, R. (1991). A European defence union?. Economic Policy,13(3)

Fontanel, J. (1991), Third World Economic Consequences of the East-West Disarmament Process, Edited by Serge SUR, in Disarmament Agreements and Negociations. The Economic Dimension. United Nations Institute for Disarmament Research (UNIDIR), Darmouth, Aldershot, Brookfield, USA, 1991 (32 pages).

Fontanel, J., Ward, M. (1993), Military Expenditures, Armaments and Disarmament, Defence Economics, Vol. 4

Fontanel, J. (1993), La gestion économique du désarmement. Dix principes positifs. in "Economistes de la Paix", Presses Universitaires de Grenoble, PUG, 1993

Fontanel, J. (1993), Economistes de la Paix", Presses Universitaires de Grenoble, PUG, 1993

Fontanel, J, Hébert, J-P. (1997), The French policy of "Grandeur", Defence and Peace Economics, Vol. 8 (1),

Fontanel, J., Smith, R. (1993), Le couple désarmement-développement dans la pensée économique, in "Economistes de la Paix, PUG, 1993,

Fontanel, J. (1994), The Economics of Disarmament. A Survey, Defence and Peace Economics, Vol. 5, n° 2,

Fontanel, J. (1995), The economics of disarmament, in Handbook of Defense Economics, Vol.1. (Hartley and Sandler eds), North Holland, Elsevier Sciences, Amsterdam, 1995.

Fontanel, J. (1995), La conversion économique du secteur militaire, Economie Poche, Economica n° 12

Fontanel, J. Borissova, I, Ward, M. (1995), The principles of arms conversion in the case of Russia, Defence and Peace Economics, 1995, 6.3.

Fontanel, J., Matelly, S. (2000), Le coût des dividendes de la paix, Mondes en développement, Tome 28, année 2000, n° 112, pp. 59-73.

Fontanel, J. (2002), Disarmament : A century of economic thought, Defence and Peace Economics,Tome 28

Fontanel, J., Ward, M. (2002), A hard look at the costs of peace, World Economics, Vol.3, n.2, April-June .

Fontanel, J., Samson, I. (2008), The economic determinants of military expenditures, in « War, Peace and Security » (Fontanel, Chatterji Eds.), Emerald London,

Fontanel, J., Fontanel, M. (2013), Les BRICS, un concept statistique devenu une force politico-économique, in « Basculement économique & géopolitique du monde. Poids et diversité des pays émergents » (Mohammed Matmati Ed.). L'Harmattan, Paris.

. Fontanel, M, Fontanel, J. (2013), L'intelligence économique, une activité d'intérêt public et privé, in Entrepreneuriat, PME durables et réseaux sociaux (Thierry Levy-Tadjine et Zhan Su), en l'honneur du Professeur Robert Paturel, CEDIMES, L'Harmattan Paris,

Fontanel, J. (2015), La base des données des dépenses militaires recueillie par l'Organisation des Nations Unies : origine et évolution. *United Nations Standardized Instrument for Reporting Military Expenditure (*2015) In Paix et sécurité européenne et internationale, http://revel.unice.fr/psei/ ,

Gewin, V. (2016), Climate Change Adds Urgency To Push to Save World's Seeds, Yale – Environment 360 – Report – April 21, http://e360.yale.edu/feature/climate_change_adds_urgency_push_save_worlds_seeds/2985/

Guilhaudis, J-F. (2015), Désarmement, PSEI, Numéro 1, 17 août 2015, URL : http://revel.unice.fr/psei/index.html?id=357.

Guilhaudis, J-F. (2015) , « Les Alliances collectives(Inf.2/1-11). », PSEI, Numéro 1, 17 août 2015, URL : http://revel.unice.fr/psei/index.html?id=351

Guilhaudis, J-F. (2015), « Puissances et impuissances, acteurs de la sécurité et de l'insécurité internationale.(A1-A83) », PSEI, Numéro 1, 17 août 2015, http://revel.unice.fr/psei/index.html?id=333.

Harbulot, C. (sous la direction de), 2016, La France peut-elle vaincre Daech sur le terrain de la guerre de l'information, Rapport d'alerte, Préface Alain Juillet, Ecole de guerre économique, Paris

Hartley, K., Sandler, T. (1994), Handbook of Defence Economics, Vol.1. Elsevier, North Hollland. Coulomb (2004), Economic theories of Peace and War, Routledge, London and New York.

Hartung, W. (2015), Economists for Peace & Security, Newsletter, Volume 27, Issue 1, March.

IHEST (2014) La recherche aux Etats-Unis, http://www.ihest.fr/la-mediatheque/international/etats-unis-science-innovation/la-recherche-aux-etats-unis

Kallenborn, G. (2016), La NASA a pu déchiffrer les données secrètes d'entreprises pendant des années, 01net.com, 19 Août. http://www.01net.com/actualites/la-nsa-a-pu-dechiffrer-les-donnees-secretes-d-entreprises-pendant-des-annees-1027725.html

Kaufman, R. (2015), Economists for Peace & Security, Newsletter, Volume 27, Issue 1, March 2015.

Leontiev, W., Duchin, F. (1983), Military spendings. Facts and figures. Worlwide implications and Future Outlook, Oxford University Press, Oxford.

Lichtenberg, F. (1988), Governmeng subsidies to Private Military R&D Investment : DOD's IR&D Policy, NBER Working Papers 2745, National Bureau of Economic Research, Inc.

Lioger, R. (2016), La guerre des civilisations n'aura pas lieu. Coexistence et violence au XXIe siècle,CNRS Editions. Paris.

Malizard, J. (2013), Opportunity costs of Defence : an Evaluation in the case of France, Defence and Peace Economics 26(3), pp. 247-259.

Malizard, J., Guilhaudis, J-F. (2015), Dépenses de défense et de sécurité, PSEI, http://economie-defense.fr/depenses-de-defense-et-de-securite-julien-malizard-j-f-guilhaudis/

Mampaey L., Serfati, C. (2004), « Les groupes de l'armement et les marchés financiers : vers une convention 'guerre sans limites' ? », in Chesnais F. (ed.), La finance mondialisée. Racines sociales, et politiques, configuration, conséquences, Paris, La Découverte, p. 223-251.

Melman, S. (1970), Pentagon Capitalism : The Political Economy of War, New York, McGraw-Hill.

MIT (2015), The future postponed. Why declining Investment in Basic Resaerch Threatens a U.S. Innovation Deficit. A Report by the MIT Committee to Evaluate tyhe Innovation Deficit, April 2015.

PWC (2015), 2015, global innovation 1000. Innovation's New World Order, Strategy&, 15 October. http://www.strategyand.pwc.com/media/file/2015-Global-Innovation-1000-Fact-Pack.pdf

Sargent, J.F. (2015), Federal Research and Development, FY2016, Congress Research Service, November 10, 7-5700, www.crs.gov, p.10.

Schmidt, C. (1987), The Economics of Military Expenditures, Mac Millan Press, London.

Sharp, G. (1994) " La défense par actions civiles. Une proposition pour la défense nationale". Préface Jacques Fontanel, PUG, Grenoble, 1994.

Sharp, G. (2009), De la dictature à la démocratie : Un cadre conceptuel pour la libération, Collection « La Librairie des Humanités, L'Harmattan, Paris.

Sheehan, N. (2003). Le maintien de la paix pour le développement. In J. Fontanel (Ed.), Civilisations, globalisation, guerre. Discours d'économistes. Collection Débats, Presses Universitaires de Grenoble.

Sheehan, N. (2013) La réforme ou « reconstruction » du secteur de la sécurité : outil fondamental pour la consolidation de la paix dans les pays post-conflits, in Liber Amicorum, hommage en l'honneur du Professeur Jacques Fontanel, L'Harmattan, Paris

Shkaratan, O., & Fontanel, J. (1998). Conversion and personnel in the Russian military-industrial complex. Defence and peace economics, 9(4)

SIPRI Yearbook (2009), Armaments, disarmament, and internatinal security, Oxford, Stockholm, Oxford University Press.

UNIDIR (1992), Aspects économiques du désarmement, le désarmement en tant qu'investissement, UNIDIR, A/47/346, 27 Août, Genève.

Wojcik, D.E., Michaels, P.J. (2015), Is the Government Buying Science or Support ? A Framework Analysis of Federal Funding- Induced Biases, Cato Working Paper, n°29. April 30.
http://www.cato.org/publications/working-paper/government-buying-science-or-support-framework-analysis-federal-funding