IDN
INITIATIVES POUR LE DÉSARMEMENT NUCLÉAIRE

Juin 2018

La bombe nucléaire au bout du clavier

L'insécurité des systèmes d'armes nucléaires face aux risques cybernétiques

SOMMAIRE.

« L'arme nucléaire, c'est la fin acceptée de l'humanité ». Tels étaient les mots du scientifique naturaliste biologiste Théodore Monod en août 1999. Arme non conventionnelle, classée dans les armes de destruction massive, l'arme nucléaire a été une menace omniprésente pendant la Guerre Froide. Une prise de conscience quant à la dangerosité d'un potentiel hiver nucléaire intervient après la crise de Cuba. Des accords bilatéraux entre les Etats-Unis et l'URSS, puis des traités internationaux sont alors signés pour circonscrire la prolifération nucléaire, qu'elle soit horizontale (l'augmentation du nombre de pays détenteurs) ou verticale (le perfectionnement de l'arme nucléaire). Les stocks ont été réduits.

Pourtant, la menace d'une guerre nucléaire n'a jamais été aussi élevée qu'aujourd'hui. Symbole de sécurité nationale, la dissuasion prolongée demeure la pièce maîtresse des doctrines stratégiques de nombreux Etats. Les neuf Etats dépositaires du nucléaire militaire possèdent encore plus de 15 000 armes nucléaires et continuent d'augmenter leurs investissements pour l'amélioration de leurs forces nucléaires. Mais un tel système de défense ne paraît plus adéquat aux menaces géopolitiques actuelles. Le climat international n'apaise pas les tensions entre les Etats dotés de l'arme nucléaire, que ce soit entre la Fédération de Russie et l'Occident, les Etats-Unis et l'Iran ou encore l'Inde et le Pakistan. Dans le même temps, des groupes terroristes comme Al-Qaida ou l'Etat islamique ont exprimé leur désir d'acquérir des armes nucléaires.

La menace nucléaire est renforcée par l'avènement d'un nouvel environnement cybernétique. L'humanité est cernée de toutes parts par les nouvelles technologies et les objets connectés. Il y aurait actuellement 15 milliards d'objets connectés à Internet selon l'Institut de l'audiovisuel et des télécommunications en Europe (Idate), contre 4 milliards seulement en 2010. En 2020, il devrait y en avoir entre 50 et 80 milliards. Les objets connectés inondent désormais la société, que ce soit dans le domaine civil, industriel ou militaire. Cela augmente d'autant les enjeux liés à la sécurité du cyberespace et à la lutte contre une grande diversité de cybermenaces. L'individu, les entreprises, les organisations et l'Etat sont tous concernés par les nouvelles cybermenaces.

La dimension cybernétique a transformé les enjeux de sécurité concernant les organismes d'importance vitale (OIV) de l'Etat. Les armes nucléaires et les systèmes qui leur sont associés ne sont pas épargnés. Les dangers et les risques potentiels inhérentes aux armes nucléaires ne sont certes pas nouveaux. De multiples accidents se sont déjà produits : à Palomarès (Espagne, 1966), puis à Thulé (Groenland, 1968), des bombardiers ont perdu leur chargement nucléaire en plein vol. En 2009, deux sous-marins nucléaires lanceurs d'engin (SNLE) britannique et français chargés de près de deux cents ogives nucléaires entraient en collision. A plusieurs reprises, le monde a échappé de justesse à une explosion nucléaire militaire accidentelle.

L'avènement de l'ère du numérique augmente désormais les risques quant aux vulnérabilités préexistantes, et crée de nouvelles menaces. La fiabilité et l'intégrité des systèmes d'armes nucléaires dans toutes leurs actions sont aujourd'hui interrogées. Leur piratage, qui semblait hier impossible, est aujourd'hui devenu un risque réel. La menace est d'autant plus grande que les armes nucléaires ont été créées à une époque où l'informatique en était à ses balbutiements et que le risque cybernétique n'a pas été pris en compte dans l'architecture des systèmes et stratégies nucléaires actuelles. Et si les armes nucléaires sont censées être des ordonnances politiques plutôt que militaires, en maintenant la paix sans jamais être utilisées, les obstacles à leur utilisation s'érodent peu à peu.

Ce rapport a pour objectif d'analyser les risques que la numérisation des systèmes et l'utilisation de technologies émergentes font peser sur les systèmes d'armes nucléaires et les systèmes qui leur sont associés. Il s'agit également de déterminer de quelle manière ces évolutions technologiques pourraient remettre en question la stratégie nucléaire.

Chapitre 1
Qu'est-ce qu'une menace cybernétique ?

La menace cyber est partout et cible tout le monde. En 2015, le Panorama 2016 des risques globaux du Forum de Davos identifiait le cyber-risque comme le premier des risques technologiques. La révolution numérique, porteuse de vastes opportunités, induit également des risques, des menaces. Pourtant, le cyber est un sujet d'actualité, d'inquiétude et d'incompréhension. Le cyber-défi n'est que peu étudié et encore moins compris par tous. Il s'agit donc d'expliquer la vaste notion de cyber et de présenter le spectre tout aussi vaste des cybermenaces.

I. 'Cyber' : un concept polymorphe et incompris.

Si l'étymologie du terme 'cyber' remonte à la Grèce Antique, où '*kubernêtikê*' se traduisait par « *l'art de gouverner* », il n'apparaît que récemment dans la littérature contemporaine. En 1948, dans « *Cybernetics, or Control and Communication in the Animal and the Machine*[1] », Norbert Weiner étudie alors l'importance des systèmes chez les êtres vivants et les machines artificielles. Il considère que l'information doit pouvoir circuler librement entre les différentes classes et sociétés, sans entrave ou discrimination. La notion est ensuite popularisée par les romans de science-fiction qui décrivent alors un monde sombre et rempli d'outils cybernétiques.

'*Cyber*' est introduit dans le lexique de la sécurité nationale au début des années 1990, avec le développement de SIMNET – un champ de bataille virtuel utilisé par l'armée américaine – et la publication de l'ouvrage de John Arquilla et David Ronfeld, « *Cyberwar is Coming*[2] » en 1993. '*Cyber*' devient une expression générique pour relever les défis posés par les nouvelles vulnérabilités informatiques au sein des systèmes. C'est aujourd'hui une vaste notion qui regroupe les cybermenaces, le cyber-activisme, le cyberterrorisme, la cybercriminalité, ou encore le cyber-harcèlement. Il existe désormais plus de 150 mots ou expressions contenant le préfixe ou l'adjectif cyber.

Les risques cybernétiques touchant aux systèmes nucléaires sont antérieurs à l'exercice de définition de la menace. Déjà dans les années 1960, les responsables américains s'inquiétaient qu'un missile puisse être envoyé involontairement dans la mauvaise direction. La même année, une unité radar connectée au NORAD a confondu la lune avec une attaque

[1] WIENER Norbert, *Cybernetics or control and communication in the animal and the machine* (2nd edition), the M.I.T press, Cambridge, 1948.
[2] ARQUILLA John, RONFELD David, *Cyberwar is Coming*, 1993.

massive de missiles soviétiques. En 1980, le physicien Boris Rauschenbach avertissait que la sophistication croissante des systèmes d'armes nucléaires signifiait que l'existence de l'humanité devenait dépendante du matériel et des logiciels[3], et donc devenait vulnérables à des erreurs, des bugs informatiques.

Paradoxalement, c'est un film qui va véritablement entrainer une prise de conscience envers les menaces cybernétiques de la part de l'administration Reagan (1981-1983), aux Etats-Unis. Sorti en 1983, le film WarGames suit un jeune pirate informatique qui accède involontairement à distance à un supercalculateur militaire des forces armées américaines. Le programme WOPR (War Operations Plan Response) a pour but de prédire les résultats possibles d'une guerre nucléaire, et le pirate, croyant jouer à un jeu vidéo, obtient le lancement d'une simulation de guerre nucléaire et manque de déclencher une troisième guerre mondiale thermonucléaire. Les Etats-Unis prennent alors conscience que les ordinateurs du NORAD sont vulnérables aux pirates extérieurs. Cela donnera lieu à la publication d'une première directive le 17 septembre 1984, la NSDD-145, ou « National Policy on Telecommunications and Automated Information Systems Security, pour améliorer la cybersécurité des systèmes militaires américains.

Trente ans tard, le taux de pénétration de l'Internet dans la société est estimé à 50,1% au niveau mondial, 73,9% en Europe, et 83,8% en France[4]. Tout nouveau produit ou réseau numérique est une cible potentielle des cyber-malveillances. Plusieurs attaques ont eu une large résonnance internationale, comme celles de Targuet (2013), Sony (2014), Petya (2016) ou WannaCry (2017) en ce qui concerne le vol de données, ou l'attaque sur les centrales nucléaires iraniennes par le virus Stuxnet (2010). La révolution numérique avec la dématérialisation des données et l'introduction de technologies et de systèmes complexes ont provoqué des bouleversements majeurs à toutes les échelles de la société. Pourtant, en l'absence de données publiques et de statistiques significatives, le cyber-risque demeure un risque très difficile à cerner et à définir.

La notion de '*cyber*' peut être définie à la fois comme l'émergence d'un nouveau contexte numérique, et comme un nouvel ensemble d'outils, de dynamiques et d'armes. Andrew Futter, dans le cadre du nucléaire militaire, entend le cyber-défi comme touchant au commandement et au contrôle de toutes les technologies de l'information impliquée dans la gestion des armes nucléaires. Il opère dans les quatre domaines de l'environnement de

[3] FUTTER Andrew, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, Georgetown University Press, Washington DC, 2018.
[4] Ministère de l'Intérieur, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, *État de la menace liée au numérique en 2017*, Janvier 2017.

l'information : physique / mécanique – les infrastructures physiques et le matériel –, logique – les commandes indiquant au matériel quoi faire et les logiciels permettant la transmission, l'interprétation et le partage de l'information –, informationnel – les informations et les données que le système collecte, stocke, génère et utilise pour fonctionner – et humain / cognitif – les êtres humains et leurs interactions avec le matériel, les logiciels et l'information[5].

Les cyber-risques concerneraient l'ensemble des événements à caractère immatériel pouvant affecter un système d'information. Selon la définition de l'ONU, la cybercriminalité est une notion polymorphe, recouvrant tout comportement illégal faisant intervenir des opérateurs électroniques qui visent la sécurité des systèmes informatiques. Cela concerne à la fois les infractions classiques commises par le biais des nouvelles technologies – l'espionnage par exemple – et à la fois de nouvelles infractions, nées de l'essence même de ces nouvelles technologies. Enfin, le ministère de l'Intérieur français définit les cyberattaques comme des atteintes à des systèmes informatiques réalisées dans un but malveillant. Les cibles des cyberattaques sont diverses : des ordinateurs ou des serveurs, des équipements périphériques ou encore des appareils communicants tels que les smartphones ou les tablettes.

L'ANSSI, l'autorité nationale en matière de sécurité et de défense des systèmes d'information, définit la cybersécurité comme un « *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ». La cyberdéfense est entendue comme « *l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels* ».

II. Les cybermenaces : spectre, acteurs et attribution.

Depuis les premiers hackers apparus dans les années 1990, les cybermenaces ont largement évolué et ont vu leurs capacités augmenter. Elles englobent un spectre large d'activités, du simple piratage aux attaques de déni de service, de l'espionnage au sabotage. Selon Andrew Futter, les cybermenaces peuvent être regroupées en deux catégories. L'exploitation cybernétique se définit comme une activité de collecte de renseignements, ou comme des opérations conçues pour sonder et tester des systèmes auprès d'une cible ou de systèmes ennemis. Les cyberattaques sont des cyber-opérations conçues pour perturber, refuser, dégrader ou détruire les informations stockées dans des ordinateurs ou des réseaux. Les deux

[5] FUTTER Andrew, *Op. Cit*.

catégories se distinguent par l'intention et par le type de logiciel malveillant ou de charge utile impliquée[6]. Il existe en réalité quatre types de risques cyber : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.

Les moyens d'attaques sont aussi très divers, et nous proposons d'en présenter quelques-uns. Les malwares sont des programmes malveillants. Ils regroupent les virus – des segments de code exécutables greffés à un programme qui contaminent l'ensemble de l'ordinateur et pouvant le détruire –, les vers – des programmes autonomes se reproduisant d'un ordinateur à l'autre en utilisant les capacités et faiblesses d'un réseau –, et les chevaux de Troie, permettant la prise de contrôle de l'ordinateur infecté à distance et à l'insu de l'ordinateur afin de récupérer les données de l'ordinateur. Les rootkits donnent l'accès à tous les dossiers d'un ordinateur. Le spoofing introduit de fausses informations dans un système à l'insu du receveur.

Les spywares sont des logiciels introduits dans un système pour collecter des informations à l'insu de l'utilisateur, et de les transmettre à un tiers. C'est ce qu'on appelle plus communément les logiciels espions. Une bombe logique est un logiciel malveillant conçu pour causer des dommages à un système informatique et qui n'est déclenché que lorsque certaines conditions sont réunies. Le phishing a pour but de voler l'identité ou les informations confidentielles des utilisateurs par subterfuge. Les portes dérobées, ou backdoor, sont des accès dissimulés permettant à un utilisateur malveillant de se connecter à une machine de manière furtive. Enfin, les attaques Dos et DDos – déni de services et déni de services distribués – ont pour objectif la mise hors ligne ou l'impossibilité d'accès d'un serveur, et l'indisponibilité des services et ressources d'une organisation.

Le cyber-défi envers les systèmes d'armes nucléaires varie également selon le type d'acteurs impliqués. Les attaques peuvent provenir d'Etats-nations comme d'acteurs non-étatiques. La menace non-étatique est plurielle. Les systèmes d'armes nucléaires pourraient par exemple être la cible d'hacktivistes écologiques s'opposant au nucléaire. Leurs attaques prendraient alors la forme des 3D : DDos en fermant un service par exemple, Doxxing en révélant des informations confidentielles, et Defacement (vandalisme). Les opérateurs réseaux, ou hackers, chercheraient à prendre le contrôle des systèmes informatiques afin de coordonner des attaques et de distribuer des fichiers malveillants. Les groupes criminels organisés représentent une menace quant à leur capacité d'espionnage industriel. La plus grande menace provient aujourd'hui du cyberterrorisme nucléaire : un groupe terroriste pourrait avoir pour objectif de détruire ou exploiter des systèmes d'armes nucléaires afin de menacer la sécurité nationale, ou déclencher une guerre.

[6] *Ibid.*

Les attaques les plus sophistiquées semblent l'apanage d'une poignée d'Etats-nations dotés de capacités cybernétiques très avancées. Au contraire, les criminels, les hacktivistes ou les petits groupes préfèreront des attaques moins sophistiquées ou des nuisances. Il faut ici souligner que les cyber-armes et les cyberattaques particulièrement sophistiquées ne sont pas la meilleure arme des faibles. Si elles disposent sans aucun doute d'un pouvoir multiplicateur de force et égalisateur de puissance, il se pose des obstacles à leur développement et à leur utilisation, d'autant plus que les Etats peuvent menacer de mener des représailles. Pour reprendre les termes d'Andrew Futter, « *le potentiel destructeur des cyberattaques est inversement proportionnel au nombre d'acteurs capables de telles attaques et aux types de cibles pouvant être atteintes*[7] ». La nature de la menace cybernétique varie donc selon les enjeux, les intentions et les capacités des attaquants.

Mais l'une des principales difficultés de la menace cybernétique concerne la traçabilité des auteurs, et donc l'attribution des actions, élément nécessaire à toute stratégie de dissuasion. Il est extrêmement difficile de déterminer précisément et avec suffisamment de confiance l'attribution dans le cyberespace pour susciter une réponse. Les opérateurs disposent d'une multitude de techniques de brouillage pour empêcher les défenseurs d'identifier le point d'origine d'une attaque. De plus, l'attribution peut être compliquée par l'ingérence d'un tiers, par des attaques de pirates basés dans un pays donné mais qui ne travaillent pas pour son gouvernement. Andrew Futter propose de « *penser niveaux d'attribution*[8] », en prenant en compte les buts politiques, le contexte politique ou stratégique d'une attaque, et de réintroduire de la lenteur dans le processus afin de mener une enquête cyber-criminalistique approfondie.

Jason Healey, directeur de la Cyber Statecraft Initiative associée au think tank américain Conseil Atlantique, propose un « *spectre de la responsabilité de l'Etat*[9] », afin de déterminer l'attribution de la responsabilité d'une attaque particulière ou d'une campagne d'attaque avec plus de précision et de transparence. Le spectre attribue dix catégories :

1. State-prohibited : le gouvernement national aidera à arrêter l'attaque d'un tiers ;
2. State-prohibited-but-inadequate : le gouvernement national est coopératif pour arrêter l'attaque d'un tiers, mais en est incapable par manque de lois, de procédures, d'outils techniques ou de volonté politique ;
3. State-ignored : le gouvernement est au courant des attaques, mais ne veut politiquement prendre aucune mesure officielle. Il peut être d'accord avec les objectifs des

[7] *Ibid*.
[8] *Ibid*.
[9] HEALEY Jason, « Beyond Attribution: Seeking National Responsibility for Cyber Attacks », *Issue Brief*, Conseil Atlantique, Washington, DC, 2011.

assaillants ;

4. State-encouraged: les tiers contrôlent et dirigent l'attaque, mais le gouvernement national les y encourage ;
5. State-shaped : les tiers contrôlent et dirigent l'attaque, mais l'Etat fournit un certain soutien, comme une coordination informelle ;
6. State-coordinated : le gouvernement coordonne les attaques de tiers en suggérant des objectifs, un calendrier ou des détails opérationnels, ou en fournissant une assistance technique ou tactique ;
7. State-ordered : le gouvernement dirige les tiers mandatés pour mener l'attaque en son nom. Selon le droit international, tout attaquant sous le contrôle de l'Etat peut ici être considéré comme un agent de facto de l'Etat ;
8. State-rogue-conducted : les cyber-forces gouvernementales mènent l'attaque, à l'insu ou sans l'approbation du gouvernement national, qui peut les arrêter ;
9. State-executed: l'Etat, en tant qu'entité politique, contrôle et dirige directement l'attaque en utilisant ses propres cyber-forces ;
10. State-integrated: l'Etat intégrer des attaquants tiers et des cyber-forces gouvernementales avec un commandement et un contrôle commun. Le gouvernement contrôle les objectifs, le calendrier et le rythme de l'attaque, et les attaquants sont de facto des agents de l'Etat.

Selon Emilio Iasiello, « *le niveau de culpabilité attribué à l'état-nation servirait de guide pour le type et le niveau de réponse approprié, allant de l'ignorance de l'attaque initiale à la riposte de l'agresseur identifié*[10] ».

Les cybermenaces sont donc diverses et variées, et impactent tous les secteurs de la société. Cependant, les dangers qu'elles font peser sur les systèmes d'armes nucléaires sont particulièrement élevés.

[10] IASIELLO, Emilio, « Is Cyber Deterrence an Illusory Course of Action? », *Journal of Strategic Security*, Henley-Putnam University, n° 1, 2013, pp. 54-67

Chapitre 2
Le second âge nucléaire à l'épreuve des cybermenaces.

Les risques cybernétiques ont introduit de nouvelles vulnérabilités – entendues comme des faiblesses au niveau d'un élément d'un système industriel ou d'information – dans les systèmes d'armes nucléaires. Dans son rapport « *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences*[11] », le Département de sécurité internationale de la Chatham House a identifié 13 zones vulnérables aux cyber-risques, parmi lesquelles les différents systèmes de communication, les données télémétriques des missiles, les cyber-technologies dans les laboratoires et les installations d'assemblage, les informations météorologiques et de ciblage provenant de systèmes spatiaux ou de stations au sol, ou encore les systèmes autonomes robotisés dans l'infrastructure stratégique. Ces zones vulnérables possèdent toutes des vecteurs d'attaques par lesquels un acteur malveillant peut accéder à une information sensible ou créer de fausses informations. Nous allons ici en développer quelques-uns.

I. Le cyberespionnage.

Souvent considéré comme la deuxième profession la plus ancienne au monde, l'espionnage n'est pas un défi nouveau pour les systèmes d'armes nucléaires. Il s'est posé dès les premières conceptions de la bombe dans les années 1930 et 1940. Etaient recherchés par les Etats adverses des plans de conception, les capacités d'armes ennemies, des procédures opérationnelles ou encore des informations privées sur le personnel nucléaire. Le vol de secrets nucléaires a largement participé à la prolifération nucléaire. L'URSS, puis la Chine, le Pakistan, la Corée du Nord – ou même la France concernant la bombe H – ont pu obtenir l'arme nucléaire en partie grâce à l'espionnage nucléaire. Les risques, pendant le premier âge nucléaire (1945-1991), étaient principalement posés par des espions humains, des taupes ayant un accès direct et autorisé aux systèmes nucléaires. Les systèmes gouvernementaux ou militaires, comme les entrepreneurs de la défense ou des chercheurs étaient ciblés.

Depuis, le besoin d'acquérir des renseignements sensibles sur les systèmes nucléaires a dominé les relations stratégiques. Il a toujours été considéré plus facile d'obtenir des informations sur les divers systèmes, processus et personnels nucléaires plutôt que de mettre en

[11] UNAL Beyza, LEWIS Patricia, *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences*, International Security Department, Chatham House, Janvier 2018.

place des opérations pour saboter ou détruire les systèmes d'armes nucléaires par des moyens informatiques. Depuis le début des années 1980, la menace cyber a mis en péril la confidentialité des données. De plus en plus de données sont stockées et partagées sur des ordinateurs et des réseaux, permettant aux organisations un meilleur accès à l'information et donc un travail plus efficace. Mais ces évolutions sont à double tranchant : une plus grande quantité de données sont stockées en dehors du contrôle direct des gouvernements, et l'information est plus facilement accessible également pour les pirates. Le cyberespionnage est une menace omniprésente : elle représente aujourd'hui plus de 90% des cybermenaces.

Selon Andrew Futter, les ordinateurs sont tour à tour devenus un outil d'espionnage (en enfreignant les codes pour collecter des données), une cible d'espionnage (contenant des informations précieuses) puis un moyen d'espionnage (permettant de voler les secrets d'une autre machine)[12]. Le second âge nucléaire (depuis 1991) présente deux ensembles de défis. Pour le chercheur américain, un premier développement clé pour l'espionnage nucléaire est le recours croissant aux ordinateurs numériques pour le stockage des données. Du matériel scientifique et technique sur les essais nucléaires, des données de recherche et développement, des conceptions d'armes, des structures militaires, des doctrines sont stockées sur des réseaux. Cela rend l'accès à l'information plus aisé, même si ces ordinateurs sont séparés de l'Internet et des réseaux non-sécurisés. Une part importante des opérations d'espionnage nucléaire a impliqué des initiés ayant accès à des systèmes mal sécurisés en raison d'un manquement important en termes de cybersécurité et de cyber-hygiène. Le deuxième développement clé tient à la capacité d'accéder et de cibler les secrets nucléaires à distance. Cela concerne les attaques de phishing, l'exploitation de vulnérabilités ou un accès donné par un initié. Les attaques informatiques permettent d'exfiltrer les données sans infiltrer les humains dans des opérations très risquées. On a ainsi assisté à une hausse importante du nombre d'attaques à distance sur systèmes d'armes nucléaires.

Dans son ouvrage « *Hacking the Bomb: Cyber Threats and Nuclear Weapons* », Andrew Futter souligne également que l'espionnage cybernétique est loin d'être une menace homogène. Elle varie en fonction des acteurs et des intentions de ces derniers. Il peut s'agir d'un espionnage visant à accéder aux systèmes d'information nucléaire pour montrer que c'est possible, de la volonté de causer une nuisance en corrompant des fichiers, ou la volonté d'acquérir des connaissances et des renseignements sur ce qu'un Etat ou un acteur est en train de planifier. Un acteur peut aussi chercher des informations sur les capacités relatives des principaux programmes d'armement, à l'heure où les Etats cherchent à moderniser leurs forces nucléaires. Les systèmes peuvent être surveillés sur une période prolongée, et le

[12] FUTTER Andrew, *Op. Cit*.

cyberespionnage peut aussi concerner l'obtention d'information sur des personnes directement impliquées dans les processus nucléaires – c'est ce que l'on nomme l'ingénierie sociale. Le vol de secrets nucléaires peut aussi avoir comme objectif de compromettre ou neutraliser les systèmes clés utilisés ou en train d'être développés par un ennemi dans le cadre d'un conflit futur. Il peut également aider à la prolifération nucléaire, qu'elle soit verticale ou horizontale. Les systèmes peuvent être espionnés de manière ponctuelle ou prolongée.

Les cas de cyberespionnage nucléaire sont légions depuis la fin des années 1970. La première affaire serait le Projet Gunman lancé par l'URSS dans les années 1970 : les machines à écrire de l'ambassade des Etats-Unis à Moscou ont été équipées de petits appareils d'enregistrement numérique. Dans les années 1980, des pirates du groupe 414 se sont introduits dans les systèmes du Laboratoire national de Los Alamos (Etats-Unis) pour dérober des travaux classifiés sur la conception des armes nucléaires américaines. Les systèmes du Lawrence Berkeley National Laboratory en Californie ont également été violés par un hacker allemand travaillant pour le KGB soviétique dans le but de connaître les plans nucléaires de l'administration Reagan.

En 1999, un rapport commandé par le gouvernement américain accusait la Chine d'avoir volé une multitude de secrets militaires hautement sensibles pendant plus d'une décennie, entre 1983 et 1995[13]. En 2005, des hackers supposément liés à l'armée chinoise ont mené l'opération Titan Rain, infiltrant de nombreux systèmes informatiques militaires américains à la recherche de secrets nucléaires. En 2006, le Mossad israélien a placé un cheval de Troie dans l'ordinateur d'un haut responsable du gouvernement syrien, révélant l'ampleur du programme nucléaire militaire de la Syrie. En 2008, une clé USB infectée a été introduite dans une base militaire américaine au Moyen-Orient. Le virus, techniquement avancé, a contourné les protections séparant les réseaux sécurisés de l'armée d'Internet, infectant à la fois les réseaux classés et non-classés. Le logiciel malveillant s'est ensuite répliqué rapidement sur le réseau, infectant de nouvelles clés USB, puis de nouveaux ordinateurs.

La menace ne touche pas que les systèmes militaires. En 2011, un cheval de Troie a été découvert dans un courriel semblant provenir de la Maison Blanche et à destination des entrepreneurs impliqués dans la construction des sous-marins britanniques lanceurs d'engins Trident. Enfin, l'opération Jeux Olympiques (le programme qui produira Stuxnet) avait aussi essentiellement commencé comme une opération de renseignement et d'espionnage contre le programme nucléaire iranien. Les vers informatiques Flame et Duqu avaient été conçus pour

[13] US House of Representatives, *The Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China (The Cox Report)*, 1999.

obtenir des renseignements sur les systèmes et l'infrastructure nucléaire iranienne.

Cette liste est loin d'être exhaustive. Il est certain que tous les Etats ont été victimes de cyberespionnage, mais leur manque de transparence sur ces opérations ne permet pas d'en connaître les détails. Le cyberespionnage, ajoutés à la cyber-prolifération et au terrorisme mondial, représente une préoccupation sérieuse en matière de sécurité et de sûreté nucléaire. Mais le cyber peut aussi servir dans le cadre du contre-terrorisme, avec la possibilité de fournir de fausses informations à des proliférateurs potentiels. Cependant, il est très difficile de déterminer exactement ce qu'un attaquant tente de réaliser, car les méthodes et logiciels malveillants utilisés sont souvent communs à beaucoup de cyber-opérations, dont le sabotage.

II. Manipulation de l'information et cyber-handicap.

Selon Page Stoutland, ce n'est qu'une question de temps avant qu'une cyberattaque dévastatrice ne soit lancée envers un système d'armes nucléaires[14]. Que se passerait-il alors, si un pirate informatique usurpait les systèmes d'alerte pour faire croire à une attaque de missiles nucléaires, déclenchant une frappe de représailles ? Car c'est une réalité : les systèmes d'armes nucléaires peuvent être compromis par des cyberattaques. La cybermenace affecte les risques nucléaires principalement de deux façons : elle compromet les systèmes d'informations et d'alerte liés aux armes nucléaires, mais aussi les systèmes de commandement et de contrôle des armes nucléaires.

Andrew Futter souligne ainsi que le premier défi majeur aux systèmes d'armes nucléaires est la contamination et la manipulation (spoofing) de l'information sur laquelle les décisions nucléaires sont fondées. Il y a ici un double défi. Premièrement, les capteurs et les systèmes pourraient être trompés – et l'ont déjà été – soit par un faux positif, soit par un faux négatif[15]. En 1980 par exemple, l'échec d'une puce informatique du NORAD a provoqué un faux avertissement sur une attaque nucléaire entrante. En 1983, un ordinateur soviétique a identifié quatre missiles entrants : le système a confondu la réflexion des rayons du soleil sur les nuages avec le dégagement d'énergie produit au décollage de missiles, et l'humanité ne doit son salut qu'à l'analyse de Stanislav Petrov, officier de garde sur la base de Serpoukhov-15. Devant le faible nombre de missiles détectés, l'officier déduit que le système s'est trompé et décide de désobéir à la procédure en indiquant une fausse alerte à ses supérieurs. Plus récemment, en janvier 2018, une alerte au missile balistique déclenchée par erreur à Hawaï a

[14] STOUTLAND Page, *Growing Threat: Cyber and Nuclear Weapons Systems* [En Ligne] The Bulletin, 18 octobre 2017. URL : https://thebulletin.org/growing-threat-cyber-and-nuclear-weapons-systems11201
[15] FUTTER Andrew, *Op. Cit*.

semé un vent de panique sur l'île pendant 38 minutes, soit bien au-delà du temps nécessaire à la décision de représailles.

Deuxièmement, les pirates pourraient accéder directement aux systèmes de d'alerte ou de communication pour manipuler, contaminer, corrompre l'information au sein des réseaux, ce qui pourrait induire des erreurs de compréhension en temps de crise nucléaire. Les Etats-Unis comme Israël ont cherché à introduire des logiciels malveillants dans des systèmes de défense aérienne adverse par des méthodes électroniques pour couper les liaisons de communication militaire et les radars d'alerte précoce. Futter ajoute qu'il existe de nouvelles vulnérabilités concernant l'accès des systèmes à bord des satellites[16]. Les informations sur lesquelles s'appuient les systèmes nucléaires et leurs opérateurs représentent le vecteur de menace le plus direct, en temps de crise comme en temps de paix. En réalité, le seul fait de savoir que les systèmes nucléaires sensibles pourraient être compromis remet en cause la confiance en ces mêmes systèmes, indépendamment de l'ampleur ou de la nature de l'attaque.

Ici aussi, il existe plusieurs exemples. En 2015, un système de missile sol-air Patriot allemand aurait ainsi été piraté par des hackers, qui en ont pris le contrôle pendant une courte période de temps. De l'avis des analystes, ces systèmes de missiles comportaient deux points faibles : le système d'information entre le lance-missile et le système de contrôle, et une puce informatique responsable de la gestion du missile. Au milieu des années 1990, le Pentagone avait découvert une brèche importante dans ses systèmes de sécurité qui aurait permis à des hackers de prendre le contrôle de l'émetteur de la radio navale du Maine, donnant des ordres aux SNLE postés dans l'Atlantique. Lors du dernier essai du missile Trident II D5 britannique en juin 2016, le missile s'est dirigé à l'opposé de la direction prévue, ayant reçu des informations erronées. Par bonheur, le système du missile a reconnu l'erreur et s'est autodétruit.

Le deuxième défi, qui n'est pas nouveau, concerne le risque de cyber-handicap et de destruction pour les systèmes d'armes nucléaires[17]. Les capacités cybernétiques pourraient être utilisées pour les désactiver, les perturber ou les détruire, à travers des logiciels malveillants, des bombes logiques, des codages trafiqués, des chevaux de Troie introduits dans les logiciels, les systèmes ou les composants des armes nucléaires. En octobre 2010, l'armée américaine a par exemple perdu le contrôle de 50 de ses missiles nucléaires à longue portée Minuteman III à cause d'une panne informatique. La chaîne d'approvisionnement est particulièrement vulnérable : des vulnérabilités peuvent être introduites aux étapes de fabrication, d'approvisionnement et de maintenance. Selon le rapport de Beyza Unal et Patricia Lewis pour

[16] *Ibid.*
[17] *Ibid.*

la Chatham House[18], plusieurs aspects du développement des armes nucléaires – dont la production d'ogives – et la gestion des systèmes sont privatisés, et il y a donc un risque important d'introduction de vulnérabilités lors de la fabrication compromettant l'intégrité globale des systèmes d'armes nucléaires nationaux. Les entreprises privées sont dans un état constant de cyberattaques (General Dynamics, Lockheed Martin), et il y a une large culture du secret qui empêche une évaluation réelle des risques cybernétiques.

Par exemple, en 2012, des chercheurs britanniques ont découvert que des puces informatiques chinoises utilisées notamment dans les systèmes d'armes nucléaires contenaient un *backdoor* (porte dérobée) permettant la reprogrammation ou la désactivation à distance des puces. En 2014, les Etats-Unis ont à leur tour découvert des composants et des matériaux fabriqués en Chine dans les avions militaires Boeing et Lockheed et dans les missiles Raytheon[19]. Les missiles Unha-3 nord-coréens sont également particulièrement vulnérables à la cyber-infiltration du fait de l'externalisation de la production d'un certain nombre de leurs composants. Dans cette optique, la Russie n'utilisait jusqu'ici que des composants informatiques domestiques pour bâtir leurs infrastructures critiques. Les sites nucléaires sont aussi vulnérables. Une enquête du Télégramme en 2013 révélait d'incroyables failles dans la sécurité de l'Ile Longue, la base abritant les quatre sous-marins nucléaires lanceurs d'engins français. Le site n'était alors équipé ni de contrôles biométriques, ni de scanners pour véhicules[20].

Il s'agit ici de dénoncer le problème de transparence des Etats dotés de l'arme nucléaire sur la sécurité et la sûreté de leurs arsenaux nucléaires comme de leur complexe militaro-industriel. Il est légitime de supposer que de nombreux incidents sont cachés à la fois au grand public et aux adversaires étatiques.

[18] UNAL Beyza, LEWIS Patricia, *Op. Cit.*
[19] DUNN Will, *Can Nuclear Weapons be Hacked?* [En Ligne] New Statesman, 07 mai 2018. URL : https://www.newstatesman.com/spotlight/cyber/2018/05/can-nuclear-weapons-be-hacked
[20] LE TELEGRAMME, Ile Longue. *Les incroyables failles dans la sécurité* [En Ligne] Le Télégramme, 11 juin 2013. URL : https://www.letelegramme.fr/ig/generales/fait-du-jour/ile-longue-des-failles-dans-la-securite-11-06-2013-2132250.php#7LdM2xQTcRHTzk4R.99

Chapitre 3
Vers un troisième âge nucléaire ?

Les menaces cybernétiques sont devenues une composante importante des conflits. Les cyberattaques seront utilisées aux côtés des armes conventionnelles dans tous les conflits futurs, et le nouvel environnement cyber est susceptible de brouiller les relations nucléaires internationales. Il change la dynamique des conflits et des crises, en augmentant le risque de perception erronée, d'incompréhension et d'erreurs. Surtout, les capacités cybernétiques des Etats modifient la composition des systèmes d'armes conventionnels et nucléaires, et mettent à mal les principes de dissuasion nucléaire.

I. Modernisation des systèmes, intelligence artificielle et armes conventionnelles avancées.

Dans l'esprit de tous, la modernisation des armes nucléaires, des systèmes de commandement et de contrôle et des infrastructures est synonyme de sécurité et de sûreté. C'est pourtant loin d'être le cas. Bien sûr, les nouvelles technologies aident à la fonctionnalité, à la prise de décision en temps réel et au traitement des données. Elles offrent des options pour se prémunir contre les risques de recourir à une technologie statique, et pourraient créer de nouveaux types de défense. Cependant, les nouveaux ordinateurs et codes complexes rendent les systèmes moins sûrs, plus difficiles à protéger et donc plus faciles à compromettre.

Andrew Futter souligne quatre raisons à cela[21]. La première est qu'un recours accru à des systèmes d'informations de plus en plus complexes pour les opérations nucléaires augmente la possibilité d'erreurs, de défaillances des systèmes, d'accidents ou de résultats imprévus. Deuxièmement, avec la complexité des systèmes, les problèmes deviennent plus difficiles à diagnostiquer et à résoudre. Seule une poignée de programmeurs est capable de comprendre ces systèmes, ce qui rend presque impossible la capacité à déterminer si un système est exempt de bugs, d'interférences malveillantes ou de backdoors. Troisièmement, les systèmes nucléaires et conventionnels sont de plus en plus liés et dispersés géographiquement. Une opération cyber contre une cible conventionnelle pourrait ainsi être interprétée à tort comme une attaque contre un système nucléaire. Quatrièmement, le recours croissant à des technologies commerciales disponibles sur le marché crée d'importants risques. Plusieurs Etats dotés de l'arme nucléaire comptent en effet sur des technologies commerciales et des composants achetés à l'étranger pour des opérations nucléaires sensibles, car ils sont incapables fabriquer des composants de haute-technologie et des puces informatiques. La modernisation doit donc être un équilibre, et

[21] FUTTER Andrew, *Op. Cit*.

pas la bonne chose à faire a priori.

Le développement des capacités cybernétiques a aussi un effet transformateur sur les autres systèmes d'armes. On assiste au développement d'armes intelligentes, ce qui aura un impact sur les pensées et les stratégies nucléaires. On parle ici des défenses antimissiles balistiques – une notion qui s'est largement normalisée –, des capacités de guerre anti-sous-marine, des capacités de frappe de précision à longue portée ou encore des armes antisatellites. Ces nouvelles technologies peuvent alors offrir des possibilités de dissuasion par déni : conçues pour intercepter les missiles ou les ogives après le lancement, elles sont aussi utilisées pour empêcher les systèmes d'armes nucléaires de fonctionner comme prévu. Cela amène des questions importantes pour la sécurité, la réflexion et la stratégie nucléaire. D'abord, la propagation de défenses antimissiles performantes interroge sur la capacité des Etats à viser les cibles adverses vulnérables, notamment dans le cas des dyades nucléaires. Ensuite, les technologies avancées sont utilisées dans un rôle de contre-force non-nucléaire contre les armes nucléaires, les véhicules de livraison ou les systèmes de commandement et de contrôle associés avant même que les armes soient utilisées, alors que ce rôle était auparavant dévolu aux armes nucléaires. Se pose également une question quant à la course aux technologies à double usage : il y a ici un problème de différenciation entre les armes nucléaires et les armes non-nucléaires basées sur des missiles balistiques ou de croisière. Les armes anti-sous-marines et antisatellites ont aussi un fort potentiel déstabilisateur. Les Etats-Unis développent enfin des armes nucléaires tactiques de puissance limitée – qui sont en réalité plus puissantes que Hiroshima ou Nagasaki – et destinées à détruire des installations précises.

L'intelligence artificielle est aussi en débat. Une course à l'intelligence artificielle s'est ouverte entre les Etats-Unis, la Chine et la Russie pour une utilisation comme machine de guerre, dans des systèmes autonomes sophistiqués capables d'apprendre par eux-mêmes à effectuer des tâches spécifiques. L'armée américaine développe aujourd'hui un projet (principalement tourné contre la Corée du Nord) pour parvenir à anticiper les lancements de missiles nucléaires depuis des lanceurs mobiles[22]. La Russie a quant-à-elle annoncé au début du mois de mars qu'elle développe une torpille nucléaire autonome. Celle-ci, armée d'une ogive nucléaire, serait lancée depuis l'Océan Arctique, et pourrait parcourir des centaines de kilomètres pour atteindre sa cible en manœuvrant de façon autonome pour échapper aux défenses sous-marines adverses[23].

[22] STEWART Phil, *Deep in the Pentagon, a secret program to find hidden nuclear missiles* [En Ligne] Reuters, 05 juin 2018. URL : https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J

[23] GROLL Elias, *How AI Could Destabilize Nuclear Deterrence* [En Ligne] Foreign Policy, 24 avril 2018. URL : http://foreignpolicy.com/2018/04/24/how-ai-could-destabilize-nuclear-deterrence/

Quels sont alors les risques de cette nouvelle technologie ? Dans un rapport publié en 2018, la société de conseil RAND Corporation a présenté les conclusions de plusieurs spécialistes en intelligence artificielle et en sécurité nucléaire[24]. Certains sont optimistes, et considèrent que l'intelligence artificielle permettra un meilleur fonctionnement et un perfectionnement des armes nucléaires. De leur avis, elle ne changera pas la stratégie militaire, mais aidera à une meilleure prise de décision. A l'inverse, de nombreux chercheurs évoquent le potentiel déstabilisateur de l'intelligence artificielle pour la stabilité nucléaire et stratégique. L'intelligence artificielle va d'abord renforcer les capacités de renseignement des Etats les plus avancés, ce qui va affaiblir la dissuasion nucléaire. De plus, si l'intelligence artificielle va accélérer la prise de décision dans les crises nucléaires, cela augmente d'autant plus le risque d'erreurs générées par les ordinateurs. Par exemple, que se serait-il passé si, en 1983, une machine intelligente avait remplacé le lieutenant-colonel soviétique Petrov ? Aurait-elle été capable de reconnaître une fausse alerte ? Surtout que ces intelligences artificielles seront vulnérables au hacking ou à la manipulation. Dans la prise de décision nucléaire, l'intelligence artificielle n'aurait alors pour effet que d'affaiblir volontairement l'autonomie et la capacité d'appréciation du décideur. La RAND Corporation prévient : « *L'intelligence artificielle pourrait être déstabilisante d'un point de vue stratégique. Pas parce qu'elle fonctionne trop bien, mais parce qu'elle fonctionne juste assez bien pour nourrir l'incertitude*[25] ».

L'intelligence artificielle et les nouvelles armes conventionnelles avancées introduiront donc de nouveaux risques, de nouvelles menaces dans les systèmes d'armement nucléaire. Selon Andrew Futter, il faut ainsi prévoir un environnement stratégique où les armes nucléaires pourraient être compromises, la dissuasion pourrait échouer, et le seuil d'utilisation serait abaissé[26].

II. Vers la fin des principes de dissuasion nucléaire.

La nouvelle menace cyber fait peser des risques importants sur le principe même de dissuasion nucléaire. Elément clé des futurs conflits, les cyber-capacités offensives, dont l'avantage est à l'attaquant plutôt qu'au défenseur, auront pour effet d'augmenter les tensions en temps de crise, et cela pourrait avoir des conséquences importantes pour la stabilité stratégique, nécessitant de repenser les concepts nucléaires établis.

Les risques qui pèsent sur les systèmes de commandement et de contrôle nucléaire, ainsi que sur les systèmes d'information et d'alerte précoce pourraient rendre inopérant l'ordre

[24] GEIST Edward, LOHN Andrew J., « How Might Artificial Intelligence Affect the Risk of Nuclear War? », *Security 2040*, RAND Corporation, 2018.
[25] *Ibid*.
[26] FUTTER Andrew, *Op. Cit*.

nucléaire en cas de crise. Dans le cas de l'intelligence artificielle comme des cyberattaques, la seule existence de tels moyens d'attaque pourrait saper la confiance entretenue envers les systèmes d'armes nucléaires et remettre en question la capacité nucléaire de seconde frappe. Craignant de plus avoir la possibilité de mener des représailles, les Etats pourraient se sentir si vulnérables qu'ils mèneraient des actions préemptives. Les risques sont d'autant plus grands que plusieurs des Etats dotés de l'arme nucléaire maintiennent leurs forces nucléaires en état d'alerte permanent, et que les temps de lancement sont de plus en plus réduits. C'est ainsi que, dans son article « *Could U.S.-Russia Tensions Go Nuclear?* », Bruce Blair expliquait en 2015 que la Russie avait réduit son temps de lancement, et qu'un missile pouvait être envoyé en seulement 20 secondes. Pour les Etats-Unis, le temps de lancement est d'une minute pour les missiles terrestres, 12 pour les missiles sous-marins[27]. Les décisions sont donc prises sans recul, dans la précipitation.

La stabilité stratégique est donc remise en question par le nouvel environnement cybernétique. Il y a une préoccupation croissante concernant la capacité des Etats à cibler les armes nucléaires et les systèmes de commandement et de contrôle nucléaire par des cyberattaques. Futter explique que les Etats-Unis ont déjà commencé à intégrer de telles opérations dans leur réflexion et leur réflexion[28]. La plus grande inquiétude des analystes est la possibilité d'inclure les capacités de cyberattaques dans le concept de frappe globale des Etats-Unis, soit d'attendre des cibles partout dans le monde après un très court préavis. Le problème est qu'il sera difficile pour les Etats-Unis de convaincre les autres Etats que leurs capacités cyber ne seront pas utilisés contre eux. Les russes notamment considèrent les cyberattaques sur leurs systèmes d'armes nucléaires comme une des plus grandes menaces stratégiques. Le développement de capacités cybernétiques offensives pourraient alors bouleverser l'échelle traditionnelle de l'escalade : les Etats pouvant être vulnérables à tout moment par leurs ennemis, étatiques ou non, on entre alors dans un « *état permanent de rivalité*[29] ».

Selon Futter, ces évolutions pourraient avoir de graves conséquences sur la dissuasion nucléaire fondée sur la capacité de seconde frappe et sur la peur de destruction mutuelle assurée. La potentielle utilisation des capacités cybernétiques comme précurseurs pour retarder les systèmes avant de mener une attaque stratégique introduit le risque que les systèmes puissent être compromis et donc ne fonctionnent pas comme prévu. Les Etats réintroduiraient alors la possibilité d'effectuer des frappes préventives contre les armes nucléaires ou les systèmes associés. Cela aura aussi un impact sur la probabilité d'un futur accord de réduction des

[27] BLAIR Bruce, *Could U.S.-Russia Tensions Go Nuclear?* [En Ligne] Politico, 27 novembre 2015. URL : https://www.politico.com/magazine/story/2015/11/russia-us-tensions-nuclear-cold-war-213395
[28] FUTTER Andrew, *Op. Cit*.
[29] MAZAAR Michael J., « Rivalry's new face », *Survival*, n°54, vol. 4, 2012, p. 83-106.

armements nucléaires, ainsi que sur la prolifération nucléaire, car toute réduction des armements pourrait accroître l'influence des cybermenaces. Cela compromettrait la flexibilité nucléaire et la certitude que les armes nucléaires pourront toujours être utilisées. Les armes cybernétiques représentent donc un risque de contre-pouvoir sérieux et croissant. On s'oriente alors vers un dilemme de sécurité cybernétique, où les Etats dotés de l'arme nucléaire doivent supposer que leurs infrastructures de sécurité nationale soient ciblées, y compris les systèmes d'armes nucléaires. Cela entraine une incitation croissante des Etats nucléaires à adapter leurs politiques nucléaires vers une dissuasion préventive fondée sur la dissuasion par déni plutôt que la dissuasion par punition. Le caractère sacré des normes nucléaires est en passe d'être entièrement réévalué[30].

Il l'est d'autant plus qu'à l'avenir, les armes nucléaires pourraient jouer un rôle dans la prévention et la dissuasion de cyberattaques stratégiques, visant des infrastructures civiles critiques ou les forces armées. En 2013, un rapport publié par l'US Defense Science Board explicitait que « *la dissuasion [américaine] est obtenue grâce à des cyber-offensives, des capacités conventionnelles protégées et ancrées à des armes nucléaires*[31] ». En 2011 déjà, dans leur Stratégie internationale pour le cyberespace, les Etats-Unis certifiaient qu'ils utiliseraient tous les moyens nécessaires pour répondre aux cybermenaces[32]. Cela inclue-t-il les armes nucléaires ? La publication de la Nuclear Posture Review de l'administration Trump en février 2018 le laisse à penser[33]. Elle permet l'utilisation de l'arsenal nucléaire américain pour répondre à un large éventail d'attaques dévastatrices non-nucléaires, dont les cybermenaces, contre les infrastructures critiques des Etats-Unis, comme le réseau électrique par exemple[34]. Il y a donc un abaissement du seuil nucléaire.

La Russie aurait une position similaire, et aucun Etat doté de l'arme nucléaire n'a exclu explicitement une réaction nucléaire à une cyberattaque majeure. La France est également concernée. En 2015, François Hollande, alors président, disait implicitement dans son discours prononcé à Istres qu'une cyberattaque portant atteinte aux intérêts vitaux de la France pourrait être concernée par la dissuasion[35]. Il n'a pas été contredit par l'ex-ministre de la Défense Jean-Yves Le Drian en décembre 2016. Un rapport d'information pour le Sénat déposé le 23 mai 2017 appuie également cette position : selon les rédacteurs du rapport, la doctrine nucléaire

[30] FUTTER Andrew, *Op. Cit*.
[31] Department of Defense of the United States, Defense Science Board, *Task Force Report: Resilient Military Systemps and the Advanced Cyber Threat*, janvier 2013.
[32] Office of the President of the United States, *International Strategy for Cyberspace*, 2011.
[33] Department of Defense of the United States, *Nuclear Posture Review*, 05 février 2018.
[34] SANGER David E., BROAD William J., *Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms* [En Ligne] New-York Times, 16 janvier 2018. URL : https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html
[35] HOLLANDE François, *Discours sur la dissuasion nucléaire*, Istres, 19 février 2015.

française est « *suffisamment flexible pour prendre en compte ce type de configuration : ce ne sont pas les moyens mais la nature de l'attaque (« ciblant des intérêts vitaux ») et son origine étatique qui sont prises en compte*[36] ». Les doctrines nucléaires sont donc peu à peu revues et adaptées aux nouvelles menaces cybernétiques, et il est peu dire qu'une telle évolution est dangereuse pour le régime de non-prolifération nucléaire.

[36] PINTAT Xavier, LORGEOUX Jeanny, TRILLARD André, ALLIZARD Pasacal, HAUT Claude, « La nécessaire modernisation de la dissuasion nucléaire », *Rapport d'information n°560* au nom de la Commission des Affaires Etrangères de la Défense et des forces armées, 23 mai 2017.

La conclusion est évidente : les armes nucléaires, symbole de sécurité nationale et de stabilité internationale, ne sont désormais plus sûres. Les vulnérabilités, menaces et risques cybernétiques dans le domaine des systèmes et structures d'armes nucléaires remettent en question le principe même de dissuasion nucléaire : la cyber-insécurité dans les systèmes d'armes nucléaires compromet la confiance dans les capacités et infrastructures militaires nucléaires, créant une incertitude pour les décideurs. Et, à défaut d'accepter l'abandon de l'armement nucléaire, les Etats dotés de l'arme nucléaire et la communauté doivent au moins prendre un certain nombre de mesures pour réduire le danger pesant sur la survie de l'humanité.

Il y a d'abord une nécessité pour tous de comprendre pleinement le cyber-défi et les risques qu'il entraîne pour un futur environnement stratégique cyber-nucléaire. Pour cela, la communauté internationale doit s'accorder sur des définitions qui s'imposeraient à tous sur les notions de 'cyber', 'cyberguerre', 'cyber-opérations' et autres. Il s'agit également d'établir des règles cyber-nucléaires globales. La communauté internationale doit établir des limites aux représailles militaires des cyberattaques. Cela pourrait passer par la détermination d'un seuil minimum de gravité et par la fourniture de preuves pour l'engagement de représailles militaires. Cela passera aussi, à l'image des armes nucléaires, par une limitation des capacités de cyber-attaques, ou par des normes de non-utilisation.

Les doctrines nucléaires doivent aussi être réévaluées. Tous les Etats doivent adopter la politique de non-utilisation en premier, et empêcher tout comportement qui pourrait conduire à une escalade nucléaire. Des inquiétudes se forment également quant à l'utilisation future de l'intelligence artificielle dans les systèmes nucléaires. Pour le Général John Hyten, il faudra créer des garanties pour que les humains demeurent pleinement ancrés dans le processus de décision nucléaire à l'heure où les systèmes pilotés par des intelligences artificielles seront pleinement opérationnels[37]. Le seuil d'utilisation nucléaire doit aussi être relevé, avec par exemple l'interdiction de missiles de croisière à armement nucléaire ou de missiles tactiques de courte-portée (Corée du Nord et Iran). Allonger les temps de décision en temps de crise est également nécessaire, notamment pour les dyades nucléaires proches géographiquement.

En matière de cybersécurité, les Etats doivent être plus transparents concernant leurs mesures de base de cybersécurité. Surtout, une véritable culture du partage de l'information doit se développer. Il y a d'abord une nécessité d'inclure l'expertise du secteur privé en matière de cyber dans les stratégies de défense nationale, ainsi que le monde académique et les think-tank. Les Etats dotés de l'arme nucléaire doivent ensuite communiquer entre eux concernant des informations non-classifiées ou le partage de données sur des menaces mutuelles. La mise

[37] STEWART Phil, *Op. Cit.*

en place d'une ligne de cybersécurité entre les Etats-Unis et la Russie en 2013 est une évolution particulièrement importante en ce sens.

Des mesures de cybersécurité doivent aussi être mises en place. Il s'agit de développer une analyse des scénarios possibles en matière de cyber-risques, leur probabilité et la capacité de survie des forces nucléaires. Des tests de résistance ou encore des exercices de simulation en « red timing » de haut niveau doivent être menés régulièrement. Il faut également s'assurer qu'un nombre certain et nécessaire de personnes soit en mesure de comprendre les systèmes informatiques complexes pour pouvoir les diagnostiquer et résoudre les problèmes. Patricia Lewis et Beyza Unal proposaient aussi le développement de hotlines internationales d'incidents cybers, et l'établissement d'équipes nationales d'intervention chargées de la protection des systèmes de contrôle industriel dans les complexes d'armes nucléaires.

Des mesures de cyber-hygiène doivent aussi être développées. Cela passe par une meilleure défense de réseau, une architecte de sécurité des systèmes solides. La redondance des systèmes est préconisée – c'est-à-dire que si un composant tombe en panne, le système continue de fonctionner avec des composants de sauvegarde – et les risques cybernétiques doivent être pris en compte dans la conception, la fabrication et la maintenance des systèmes nucléaires. Il doit y avoir une gestion plus robuste de la chaîne d'approvisionnement, notamment quant aux composants étrangers. Pour pallier aux failles induites par l'innovation technologique, il s'agit aussi de former le personnel à de meilleures pratiques en matière de cybersécurité. En ce sens, il faut noter que, selon un rapport de la Nuclear Threat Initiative (NTI) en janvier 2016, la France se place à la pointe en matière de cybersécurité face à une éventuelle cyber-attaque[38].

Il s'agit également de sécuriser les matières nucléaires, et empêcher les acteurs non-étatiques d'accéder aux connaissances, équipements et matériaux nucléaires. Des ponts doivent être ici créés entre le nucléaire militaire et le nucléaire civil. Le renforcement de la sûreté nucléaire doit être global, et des mesures de sécurité et de garanties doivent être prises pour le nucléaire civil. Il s'agirait aussi d'interroger le processus de gestion des déchets nucléaires et des sources radioactives.

Enfin, doit se développer le principe de cyber-résilience. La résilience d'une organisation se traduit par l'évaluation et l'intégration du risque dans le processus de planification stratégique. En matière de risque cyber, il s'agit de mettre en place une politique d'anticipation et de prévention des risques adaptée, de prévoir un plan de continuité d'activités en temps de crise, ou encore d'analyser les retours d'expérience.

[38] NTI, « The 2016 NTI Nuclear Security Index: Theft and Sabotage », *Building a Framework for Assurance, Accountability, and Action*, 3e édition, janvier 2016.

BIBLIOGRAPHIE

❖ ARQUILLA John, RONFELD David, *Cyberwar is Coming*, 1993.

❖ BLAIR Bruce, *Could U.S.-Russia Tensions Go Nuclear?* [En Ligne] Politico, 27 novembre 2015. URL : https://www.politico.com/magazine/story/2015/11/russia-us-tensions-nuclear-cold-war-213395

❖ BORRIE, John, CAUGHLEY, Tim, WAN, Wilfred (dir.), Understanding Nuclear Weapon Risks, UNIDIR, 2017.

❖ CIMBALA, Stephen J., « Nuclear Deterrence and Cyber: The Quest for Concept », *Air & Space Power Journal*, mars-avril 2014.

❖ Department of Defense of the United States, Defense Science Board, *Task Force Report: Resilient Military Systemps and the Advanced Cyber Threat*, janvier 2013.

❖ Department of Defense of the United States, *Nuclear Posture Review*, 05 février 2018.

❖ DUNN Will, *Can Nuclear Weapons be Hacked?* [En Ligne] New Statesman, 07 mai 2018. URL : https://www.newstatesman.com/spotlight/cyber/2018/05/can-nuclear-weapons-be-hacked

❖ FUTTER Andrew, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, Georgetown University Press, Washington DC, 2018.

❖ GEIST Edward, LOHN Andrew J., « How Might Artificial Intelligence Affect the Risk of Nuclear War? », *Security 2040*, RAND Corporation, 2018.

❖ GROLL Elias, *How AI Could Destabilize Nuclear Deterrence* [En Ligne] Foreign Policy, 24 avril 2018. URL : http://foreignpolicy.com/2018/04/24/how-ai-could-destabilize-nuclear-deterrence/

❖ HEALEY Jason, « Beyond Attribution: Seeking National Responsibility for Cyber Attacks », *Issue Brief*, Conseil Atlantique, Washington, DC, 2011.

❖ HOLLANDE François, *Discours sur la dissuasion nucléaire*, Istres, 19 février 2015.

❖ IASIELLO, Emilio, « Is Cyber Deterrence an Illusory Course of Action? », *Journal of Strategic Security*, Henley-Putnam University, n° 1, 2013.

❖ LE TELEGRAMME, Ile Longue. *Les incroyables failles dans la sécurité* [En Ligne] Le Télégramme, 11 juin 2013. URL : https://www.letelegramme.fr/ig/generales/fait-du-jour/ile-longue-des-failles-dans-la-securite-11-06-2013-2132250.php#7LdM2xQTcRHTzk4R.99

❖ MAZAAR Michael J., « Rivalry's new face », *Survival*, n°54, vol. 4, 2012.

❖ Ministère de l'Intérieur, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, *État de la menace liée au numérique en 2017*, Janvier 2017.

❖ NTI, « The 2016 NTI Nuclear Security Index: Theft and Sabotage », *Building a Framework for Assurance, Accountability, and Action*, 3e édition, janvier 2016.

❖ Office of the President of the United States, *International Strategy for Cyberspace*, 2011.

❖ PINTAT Xavier, LORGEOUX Jeanny, TRILLARD André, ALLIZARD Pasacal, HAUT Claude, « La nécessaire modernisation de la dissuasion nucléaire », *Rapport*

d'information n°560 au nom de la Commission des Affaires Etrangères de la Défense et des forces armées, 23 mai 2017

❖ SANGER David E., BROAD William J., *Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms* [En Ligne] New-York Times, 16 janvier 2018. URL : https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html

❖ STEWART Phil, *Deep in the Pentagon, a secret program to find hidden nuclear missiles* [En Ligne] Reuters, 05 juin 2018. URL : https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J

❖ STOUTLAND Page, *Growing Threat: Cyber and Nuclear Weapons Systems* [En Ligne] The Bulletin, 18 octobre 2017. URL : https://thebulletin.org/growing-threat-cyber-and-nuclear-weapons-systems11201

❖ UNAL Beyza, LEWIS Patricia, *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences*, International Security Department, Chatham House, Janvier 2018.

❖ US House of Representatives, *The Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China (The Cox Report)*, 1999.

❖ WIENER Norbert, *Cybernetics or control and communication in the animal and the machine* (2nd edition), the

M.I.T press, Cambridge, 1948.