Sous la direction de
Stéphane Taillat,
Amaël Cattaruzza et Didier Danet

La cyberdéfense

Politique de l'espace numérique

2e édition

ARMAND COLIN

Illustration de couverture : Vectorfusionart / Shutterstock
Mise en page : Nord Compo

Armand Colin est une marque de
Dunod Éditeur, 11 rue Paul Bert, 92240 Malakoff

ISBN 978-2-200-63422-3

Composition réalisée par Nord Compo

263422 - (I) - OSB 80 - NOC - CMU
dépôt légal : février 2023
Achevé d'impression par Dupli-Print

www.dupli-print.fr

Imprimé en France

Sommaire

Introduction

Amaël Cattaruzza, Didier Danet et Stéphane Taillat

Pourquoi ce manuel ?

L'espace numérique est désormais un champ bien établi des relations internationales. La plupart des États en ont fait une priorité de leurs stratégies de sécurité nationale. Des superpuissances économiques y affirment leur volonté de contrôler les stocks et les flux de données aussi bien que de produire et mettre à disposition l'information qui éclaire les citoyens dans les choix démocratiques. Des associations de défense des libertés publiques déploient des ressources inusitées pour faire face à la montée de normes sécuritaires qui empiètent plus ou moins gravement sur des libertés fondamentales. Des groupes criminels ou para-étatiques se livrent à des activités d'espionnage industriel, de sabotage, de chantage… qui portent atteinte à des intérêts individuels mais aussi nationaux… L'espace numérique est donc un espace d'expression du pouvoir et de la force, un espace de tensions culturelles, politiques, militaires, économiques… bref un espace en construction permanente des relations internationales contemporaines.

Il était donc naturel de se demander si cet espace nouveau n'est qu'un espace de plus ou s'il se différencie en tout ou partie de l'espace physique qui forme le cadre traditionnel des relations internationales. En est-il un sous-ensemble, soumis aux mêmes paramètres et aux mêmes principes d'action ou un champ nouveau pour lequel il convient de produire de nouvelles théories, de nouveaux concepts et de nouveaux outils ? Le fait qu'il soit un pur artefact en fait-il un domaine spécifique, étranger au monde physique où règnent les frictions des distances et de la durée ? Comment gérer la continuité et l'imbrication de l'espace physique et de l'espace numérique et les inévitables questions découlant de leur nécessaire articulation ?

La multiplicité et l'hétérogénéité des acteurs, la place particulière de la dimension technique, la particularité du cadre espace/temps, l'acuité particulière de certaines questions (attribution des attaques, seuil et formes de la légitime défense, compatibilité des actions offensives avec les principes du droit

international humanitaire…) donnent une première indication. Le jeu des relations dans l'espace numérique appelle à revisiter les acquis fondamentaux des relations internationales et, plus largement, des sciences sociales du politique. L'espace numérique est un espace à part dont les caractéristiques fondamentales produisent un cadre renouvelé pour le jeu des rivalités et des coopérations entre acteurs stratégiques. Il ne s'agit pas de dire que rien de ce qui constitue la théorie, les concepts et les outils des relations internationales ne saurait y avoir de valeur explicative ou prescriptive. Bien au contraire, il s'agit de partir de cet acquis, de s'en nourrir, pour développer une analyse originale, capable de rendre compte du caractère global et complexe de l'espace numérique et des affrontements de pouvoir qui s'y expriment.

En ce sens, il est impossible aujourd'hui de s'interroger sur ce nouveau domaine, ou champ d'action, que constitue le cyberespace sans s'intéresser de près à ce qui le constitue, à savoir son caractère technique. Cet espace repose nécessairement sur des infrastructures physiques, des matériels technologiques plus ou moins avancés, qui redessinent les relations entre acteurs sur la scène internationale. Il s'inscrit aussi dans tout un jeu de normes, de codes, de langages machines, qui conditionnent profondément les modes d'action en son sein. Ce serait donc une gageure de penser que l'on puisse aujourd'hui réfléchir aux nouveaux enjeux internationaux posés par le cyberespace sans prendre en compte ces aspects techniques.

Pour autant, il n'y a pas, ici comme ailleurs, de déterminisme technologique qui induit de manière mécanique l'action des acteurs. Ce domaine technique nécessite donc d'être approché sous un angle social et politique à plusieurs niveaux :

– *sur le plan des stratégies et des représentations qui en sont à l'origine* : comment oublier, par exemple, que la création d'Internet dépend d'une volonté politique ? En l'occurrence, celle-ci était incarnée dès la fin des années 1960 par le programme Arpanet (*Advanced Research Projects Agency Network*), développé par la *Defense Advanced Research Projects Agency* (DARPA), agence du département de la Défense des États-Unis, qui aboutit à la mise en place du premier réseau informatique mondial ;

– *sur le plan des interactions et des jeux d'acteurs qui l'animent au quotidien* : un ensemble de stratégies, de coopérations, de concurrences ou de rivalités sont ainsi lisibles dans chacun des sous-domaines qui le constituent (voir, par exemple, toutes les questions concernant le problème de la gouvernance d'Internet, de la souveraineté numérique, ou encore celui de la concurrence internationale féroce qui émerge pour devenir *leader* de certaines technologies – comme c'est le cas aujourd'hui dans le secteur de l'intelligence artificielle) ;

– *sur le plan des réalisations et des pratiques qu'il rend possible* in fine : ce constat peut être décliné évidemment dans l'ensemble des activités humaines, qui sont toutes aujourd'hui concernées par le développement des technologies numériques. Dans le domaine de la guerre et des conflits, qui est plus particulièrement l'objet de cet ouvrage, l'usage des cyberattaques et des cyberarmes a, par exemple, transformé de manière générale l'ensemble des opérations militaires (comme l'ont démontré les opérations russes de 2008 en Géorgie et depuis 2014 en Ukraine).

De fait, force est de constater que les organisations militaires ont été profondément bouleversées par la numérisation et qu'elles sont toujours en train de se redéfinir autour de ces nouveaux outils. Qu'est-ce que le *leadership* à l'heure d'Internet et des réseaux sociaux ? Quelle place accorder aux technologies de l'information et de la communication (TIC) dans la reconfiguration actuelle des forces ? Qu'est-ce qu'un théâtre d'opération numérique ? Quel encadrement éthique et juridique pour ces nouvelles activités ? Tant de questions auxquelles cet ouvrage propose de réfléchir autour d'un constat qui en constitue le fil d'Ariane : l'idée que le social et le politique doivent être placés au cœur de l'analyse pour mieux saisir l'ensemble du spectre stratégique qu'implique ce nouveau domaine technique.

Définir le cyberespace et l'espace informationnel

Cela s'applique à la définition même du cyberespace, et plus largement de l'espace informationnel. De fait, nombreuses sont les définitions qui ont déjà été formulées de ces notions et il ne s'agit donc pas ici d'ajouter une nouvelle proposition à cette pyramide, mais plutôt de faire un panorama de l'ensemble des champs mobilisés pour construire ces définitions. Ce faisant, notre but est de montrer en quoi l'appréhension du cyberespace dépend des représentations dont il fait l'objet et en quoi ces représentations modèlent sa réalité et influencent les relations, les comportements et les pratiques des acteurs qui l'utilisent.

Commençons par une définition de base, celle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans son rapport « Défense et sécurité des systèmes d'information. Stratégie de la France » paru en 2011, le cyberespace est décrit comme « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées ». Cette approche est essentiellement technique. L'accent est posé sur les machines, leur interconnexion mondiale et la communication ainsi rendue possible via la numérisation des données. Cette approche évoque exclusivement le domaine de l'ingénieur et suppose une forme de « neutralité » définitionnelle qui évacue a priori toute dimension politique. Une telle définition paraît donc sous-entendre que les problèmes de sécurité dans le cyberespace ainsi que les solutions qui s'y rapportent ne sont que d'ordre technique. En caricaturant un peu, nous pourrions donc entendre « laissez aux ingénieurs le soin de traiter de toutes les questions touchant au cyberespace puisqu'ils sont les seuls à le comprendre ».

Bien évidemment, une telle approche a ses limites. Derrière ce semblant de neutralité, cette définition occulte un des aspects les plus fondamentaux du cyberespace qui est sa dimension humaine et politique. Derrière les machines se trouvent des utilisateurs et des acteurs, avec leurs stratégies individuelles et collectives. Une stratégie de sécurité et de défense dans le cyberespace ne peut donc pas se restreindre aux seuls aspects techniques et doit également prendre en compte l'environnement social et politique dans lequel s'insère l'ensemble

des échanges et des activités rendus possibles par Internet. Il faut donc s'intéresser à des définitions plus larges permettant d'appréhender le cyberespace comme les interactions humaines qui l'animent. Mais l'exercice est ardu tant les propositions abondent. Certains ont ainsi pu désigner le cyberespace comme un *environnement*, d'autres comme un *domaine*, un *milieu* ou un *moyen*. Ces multiples dénominations se répercutent également dans la littérature stratégique et dans les différentes doctrines militaires qui ont été formulées sur ces questions.

Or, loin d'une simple querelle de termes, chacune de ces propositions induit une représentation spécifique du cyberespace qui peut appeler à des types d'action différents en termes opérationnels. En clair, les mots utilisés ne sont pas de simples descriptions du cyberespace, mais participent à modeler sa réalité, par les représentations et les comportements qu'ils provoquent chez les concepteurs et les usagers du Net. Ainsi, les images et les métaphores véhiculées par le vocabulaire couramment appliqué au cyberespace, empruntées tantôt au champ sémantique de la mer (« surfer sur Internet », « naviguer », être attaqué par des « pirates informatiques », etc.), à celui de l'air (*cloud computing*, etc.) ou encore au monde biologique (« infection » des ordinateurs par des « virus », etc.) influent sur nos manières de penser et d'agir. Cette subordination du cyberespace aux représentations et aux usages a d'importantes conséquences. De fait, nous ne pouvons pas le considérer comme un bloc homogène et uniforme, mais il faut plutôt le voir comme une multitude de cyberespaces : chaque acteur, chaque usager construit son « espace » en fonction de son utilisation, de ses représentations, de ses intérêts. Il édifie aussi ses propres menaces et ses propres risques. En clair, un État ne construit pas le même cyberespace qu'une entreprise privée ou qu'un simple individu. Chacun développe son propre « univers numérique », inscrit dans des représentations et des pratiques, qui induisent des vulnérabilités distinctes pour chaque acteur considéré. Aussi, l'étude des acteurs doit être au centre de l'analyse stratégique du cyberespace et de l'espace informationnel.

Acteurs, discours et pratiques

Découlent de ce qui précède des interrogations renouvelées concernant l'articulation entre acteurs, et plus particulièrement entre acteurs non étatiques et étatiques, entre sphères privées et publiques, entre enjeux de sécurité interne et de sécurité externe, enfin entre échelles internationale, régionale, locale et transnationale. En effet, si les relations internationales sont depuis déjà plusieurs décennies profondément ébranlées par l'émergence de nouveaux acteurs toujours plus influents qui perturbent les traditionnelles relations interétatiques, cela est particulièrement vérifiable dans le cas du cyberespace. En effet, sa structure actuelle met en jeu de puissants acteurs privés (comme l'ensemble connu aujourd'hui sous l'acronyme de GAFAM [Google, Apple, Facebook, Amazon, Microsoft]) et toute une gamme d'acteurs individuels (hackers, cybercriminels, etc.) ou collectifs (groupes d'influence comme Anonymous) qui concurrencent depuis l'origine l'action des États dans ce domaine. L'exemple

du *Dark Web* illustre l'ampleur des contournements possibles de l'appareil étatique par l'intermédiaire du cyberespace et l'impossibilité fondamentale d'un contrôle effectif et certain de cet outil.

En un sens, cette configuration multi-acteurs selon différentes échelles et en fonction d'interactions de plus en plus rapides, de plus en plus diverses et de plus en plus intenses nécessite de repenser le champ de la politique internationale. Celui-ci ne peut plus être modélisé uniquement comme un système clos formé de quelques unités (les grandes puissances) dont les interactions potentiellement conflictuelles produisent un fragile équilibre des puissances. Il n'est pas non plus suffisant de s'en tenir à la vision d'une société internationale où les normes et les institutions configurent les interactions entre les États, lesquelles produisent ces normes en retour. Avec l'intégration du domaine numérique au cœur du champ politique, les relations internationales comprennent non seulement les États et la société transnationale mais articulent un nombre croissant d'échelles entre le niveau mondial et le niveau national. Se dessine alors un système adaptatif complexe caractérisé par : la production d'effets non linéaires par les acteurs ; des propriétés émergentes résultant des interactions entre eux et entre ceux-ci et l'environnement international ; une plus grande fluidité des modèles de comportement du système dans son ensemble, ce qui génère une incertitude plus importante. Celle-ci porte à la fois sur le degré d'ambiguïté dans l'interprétation des événements et sur le degré de prévisibilité des comportements.

En tant que critère principal de la politique internationale, la puissance se trouve donc relativisée, diffusée, reconfigurée, privatisée ou contournée. Il en découle la nécessité de repenser la stratégie des États dans un contexte où cette densité dynamique globale se traduit par leur difficulté croissante à formuler des objectifs et à mettre en œuvre des politiques cohérentes.

De la sécurité informatique à la sécurité nationale

Dans ce cadre, le développement des technologies de l'information et de la communication et l'intégration de l'espace numérique à un nombre toujours plus croissant d'activités économiques, politiques et sociales a accompagné un processus de *sécuritisation* du cyberespace. Celui-ci peut être compris comme l'érection des problèmes posés par la sécurité informatique (à l'encontre de la disponibilité, la confidentialité et l'intégrité des données, des systèmes et des réseaux) en enjeux existentiels de sécurité. Ce processus a dépendu des discours et des pratiques produits par un ensemble d'acteurs comprenant les gouvernements, les agences en charge de la sécurité et les entreprises de sécurité informatique.

Ainsi a émergé un champ de la sécurité comprenant à la fois des objets à protéger (les infrastructures critiques, définies selon des critères divers), des menaces (acteurs étatiques, groupes de hackers, risques d'effondrement) et des mesures à adopter en urgence aux échelles individuelle, organisationnelle,

nationale et internationale (organisation de la cyberdéfense, actions défensives, préemptives et préventives, nécessité d'une coopération internationale voire multi-acteurs).

Néanmoins, ce processus ne correspond pas totalement aux présupposés des théories de la *sécuritisation*, lesquelles insistent sur le rôle des acteurs politiques capables de mobiliser des ressources et de faire prévaloir leurs interprétations. Les gouvernements, à commencer par celui des États-Unis, ont certes joué un rôle instrumental dans le développement initial des discours sur la cybersécurité et la cyberdéfense. Cependant, en raison de la multitude des acteurs concernés, individuels ou collectifs, comme de la complexité du système constitué par le domaine numérique, le champ de la sécurité est caractérisé par l'émergence de nouveaux enjeux, de nouvelles menaces et de nouveaux dispositifs selon des logiques distribuées et non linéaires. Par leurs rapports publics, les sociétés de sécurité informatique ont institutionnalisé la manière de concevoir les menaces. Menaces persistantes avancées (*Advanced persistent threats*, APT), *Diamond Model*, *Kill Chain*[1] configurent ainsi l'organisation comme les opérations des acteurs malveillants. L'interaction entre médias traditionnels et nouveaux médias est également à l'origine de représentations sécuritaires propres : de la propagande informatique à la génération de mobilisation en ligne en passant par le développement d'applications par le bas. En retour enfin, l'émergence de nouvelles technologies et de leurs usages alimente les discours et les pratiques sécuritaires, qu'il s'agisse de l'Internet des objets ou des enjeux liés aux intelligences artificielles.

La déclinaison du champ de la sécurité du niveau individuel jusqu'au niveau international engendre des propriétés émergentes qui se nourrissent des interactions entre les acteurs et leurs enjeux selon ces différentes échelles. En raison de son caractère transnational et global, le domaine numérique semble donc particulièrement sensible aux enjeux internationaux qu'il peut susciter. D'une part, les États sont confrontés à la question de la gouvernance du réseau global Internet, dans des logiques classiques de coopération et de compétition où se jouent les relations de puissance. Néanmoins, la difficulté à cadrer des enjeux communs et à intégrer les acteurs non étatiques pourtant parties prenantes de cette gouvernance suscite davantage de conflits. D'autre part, la construction du cyberespace comme espace politique de confrontation, de rivalités et de conflits nourrit chez les gouvernements nationaux des postures alimentant des dilemmes émergents de sécurité qui sont autant d'obstacles à la poursuite de coopérations nécessaires face à des enjeux communs. La nature existentielle des enjeux explique la prédominance de ces dynamiques et la tendance à la politisation des questions techniques et opérationnelles. C'est notamment le cas pour les questions liées à la dissuasion des attaques numériques ou l'inscription de ces dernières dans le champ du droit des conflits armés.

1. Le terme APT désigne des acteurs organisés menant des campagnes numériques de longue durée, le *Diamond Model* et la *Kill Chain* sont deux modèles permettant d'analyser les attaques, les acteurs malveillants ou leurs modes d'action.

Les aspects politiques, organisationnels et opérationnels de la cyberdéfense

Le terme de cyberdéfense est d'un usage malaisé. D'une part parce qu'il se comprend essentiellement dans le cadre français. L'usage otanien de *cyber defence* renvoie certes à une conception opérationnelle, mais sur un plan strictement défensif. Il est plus pertinent de mettre le terme de cyberdéfense en parallèle avec celui de *cyberwarfare* usité aux États-Unis. D'autre part parce qu'il ne se limite nullement à une posture défensive. Le gouvernement français a admis la nécessité de mesures actives voire offensives en octobre 2015 avant de communiquer sur les éléments publics de la Lutte Informatique Offensive (LIO) en janvier 2019 et sur la Lutte Informatique d'Influence (L2I) en octobre 2021. En revanche, le cadre général de la politique étrangère qui sous-tend les politiques de sécurité et de défense peut effectivement être défini comme la poursuite de la stabilité, justifiant de le caractériser comme défensif.

Par cyberdéfense, il faut donc entendre une certaine conception de l'action sur, dans ou à travers les réseaux numériques et les activités qu'ils soutiennent. Cette conception est premièrement opérationnelle, en ce qu'elle souligne la nécessaire intégration de cette dimension dans l'accomplissement de ses tâches par une organisation. Elle est deuxièmement stratégique car elle prend en compte une dialectique toujours possible contre un adversaire. La cyberdéfense n'est donc pas nécessairement militaire au sens strict, mais son assimilation au combat ou à l'affrontement des volontés renforce la part prise par les institutions militaires et les agences de renseignement dans sa conception et sa mise en œuvre. D'autre part, pour des raisons juridiques aussi bien que politiques, la cyberdéfense est plutôt l'apanage des États, même si elle s'appuie à des degrés divers sur le secteur privé.

En dépit d'une grande diversité dans ses modalités, l'organisation de la cyberdéfense par les États suit une logique croissante d'autonomisation vis-à-vis des autres dimensions de leur action. Deux distinctions doivent être opérées afin de catégoriser les modèles organisationnels selon les États. La première concerne le champ d'application de la cyberdéfense : s'agit-il d'agir uniquement sur le plan des réseaux numériques ou également dans les champs sociopolitiques ? Le cas américain se rapprocherait du premier modèle, tandis que les cas russe ou chinois le seraient davantage du second. Une seconde distinction concerne le degré d'intégration des acteurs non étatiques et du secteur privé : s'agit-il plutôt d'assurer la coopération avec ce dernier ou de développer son intégration ? Là encore, les cas cités plus haut correspondent respectivement au premier et au second modèles. Cette catégorisation est néanmoins fluctuante dans la mesure où les modèles tendent à converger pour inclure une approche globale de la cyberdéfense.

Comprise comme une approche particulière de la conflictualité, la cyberdéfense est également dépendante des discours et des représentations technoscientifiques liées à la guerre et à la manière de la faire. Elle s'inscrit en effet dans les développements du régime cybernétique développé durant la guerre froide. En ce sens, la cyberdéfense est héritière des réflexions, des pratiques

et des mises en œuvre liées aux soucis du commandement et du contrôle à l'ère nucléaire, à la « révolution dans les affaires militaires » (*Revolution in Military Affairs*, RMA) et à la numérisation du champ de bataille. Néanmoins, le domaine numérique suit un développement différent en direction d'un rôle croissant de l'organisation en réseau, de la prise en compte des propriétés émergentes des systèmes complexes et de la production d'effets non linéaires par les acteurs. En ce sens, le principal défi politique, organisationnel et opérationnel consiste à intégrer ces évolutions.

La gestion de crise en cyberdéfense

La politique de cyberdéfense remplit de nombreuses fonctions. Elle structure l'espace numérique et les jeux d'acteurs qui s'y développent, elle contribue à produire et organiser un corpus normatif, elle affirme une volonté politique et un projet collectif, elle vise à dissuader, le cas échéant, les comportements ou les projets susceptibles de s'y opposer… Il lui revient en particulier d'anticiper et de faire face aux « crises » susceptibles de se produire dans l'espace numérique.

Depuis que l'espace numérique a émergé, la littérature populaire aussi bien que les écrits académiques ou professionnels se complaisent dans l'évocation du cataclysme numérique, du « Pearl Harbor digital », du « Cyber 9/11 ». Du film *Wargames* au non moins célèbre *Cyberwar is coming !* de John Arquilla et David Ronfeldt, l'espace numérique est celui de tous les dangers, de la menace terroriste sur les infrastructures vitales à celle du « *geek* » dont l'habileté à la fois monstrueuse et fascinante peut conduire à déclencher une guerre nucléaire apocalyptique. La fin du monde, du moins celle du monde développé, est à l'ordre du jour.

Il était donc naturel que prospère sur ce discours alarmiste une dilection particulière pour la gestion des crises dans l'espace numérique. Avant même qu'elle ne devienne une obligation légale pour un nombre substantiel de secteurs d'activité et d'opérateurs économiques, la création et la mise en place de dispositifs et de procédures *ad hoc* se sont multipliées chez tous les acteurs : administrations et entreprises, collectivités locales et institutions communautaires… La gestion de crise est désormais l'affaire de tout un chacun. Certes, nul ne saurait se plaindre de cette prise en compte de la menace et de la volonté de renforcer la résilience de nos systèmes et de nos sociétés. On peut tout autant regretter l'occasion manquée d'une véritable réflexion sur la notion de « crise » dans l'espace numérique, sur ses caractéristiques propres, sur la transposabilité des théories, des concepts et des outils de la gestion des crises dans l'espace physique, sur la primauté accordée à la dimension technique, sur l'équilibre entre experts et décideurs en situation de crise, sur la pertinence des approches de type *risk management*, sur la conception du « château fort » qui guide encore souvent la philosophie de la gestion de crise numérique…

Fort heureusement, les attaques ou les accidents qui se sont produits jusqu'ici dans l'espace numérique et auxquels les victimes ont résisté de manière généralement satisfaisante ne présentaient pas toutes les caractéristiques d'une crise au sens propre du terme mais plutôt celles des « incidents ordinaires ».

L'utilité des dispositifs et des procédures de « gestion de crise » est donc réelle dans cette hypothèse mais il est difficile de porter un jugement définitif sur leur pertinence et leur efficacité dans l'hypothèse de véritables situations de « crise ». Le moment est peut-être le bon, maintenant que les dispositifs de gestion de crise sont en voie de généralisation, de réfléchir à la question.

Organisation de l'ouvrage

Appréhender une réalité politico-stratégique mais aussi technique, sociale ou économique aussi complexe que celle des rapports de pouvoir et de puissance multi-acteurs qui s'expriment dans l'espace numérique suppose des choix difficiles et arbitraires quant à la problématique et au plan à retenir. Les auteurs se sont ralliés à une approche systémique qui leur paraît scientifiquement utile et pédagogiquement éclairante. La logique générale en est la suivante : les politiques de cyberdéfense sont faites d'activités tendant à la réalisation d'une finalité politico-stratégique voulue et mise en œuvre par une organisation publique encastrée dans un réseau complexe d'acteurs et appelées à évoluer dans le temps.

Toute politique de cyberdéfense se décline en une série de décisions et d'actions prises par des acteurs hétérogènes dans le domaine de l'espace numérique. La politique de cyberdéfense est donc faite d'activités spécifiques dans un champ complexe d'infrastructures, d'acteurs individuels et collectifs, de logiciels et de contenus. L'analyse de la cyberdéfense ne saurait être conduite sans commencer par une tentative de cartographie de l'espace numérique, tentative toujours délicate du fait de la complexité et de la turbulence qui le caractérisent. Dans cet espace coopétitif, fait de relations de coopération et de rivalité inextricablement mêlées, la politique de cyberdéfense des États est orientée vers une finalité globale : garantir la souveraineté de la Nation dans le cyberespace. Pour ce faire, les États qui le peuvent s'assignent des objectifs, déploient des politiques et se dotent des capacités d'intervention appropriées. L'une des particularités majeures de ces politiques de cyberdéfense par rapport aux autres politiques visant à l'affirmation de la souveraineté nationale tient sans doute à la diffraction de la notion et des acteurs qui entrent en jeu. Qu'est-ce qu'une souveraineté nationale dans un espace dont il est fréquemment dit qu'il ne connaît pas de frontière et que les distances y sont abolies ? Quelle peut être l'emprise de l'État sur l'espace numérique lorsqu'il doit composer avec des acteurs privés qui conçoivent et produisent l'infrastructure technique ou les possibilités de création et d'échange dans cet espace ? Quelle est l'effectivité de ses décisions lorsqu'elles sont soumises à une totale mobilité des acteurs et des opérations ? La cyberdéfense est par essence globale ; elle s'inscrit dans un environnement contraignant qui circonscrit les ambitions et les capacités d'action de tous les acteurs, y compris les plus puissants d'entre eux, les États : politique, socio-économique, technique, culturel, légal. Plus que les autres politiques de sécurité et de défense, la cyberdéfense est le lieu de la coconstruction, des nécessaires équilibres entre des principes antagonistes d'égales valeurs, des interactions dynamiques, de la gestion de systèmes sociotechniques, politiques et économiques complexes, d'où son originalité et son intérêt.

Partie 1

Le contexte global de la cyberdéfense

Il serait faux d'imaginer que l'espace numérique puisse être appréhendé comme un domaine essentiellement technique et neutre dont la fonction stratégique pourrait être minorée. Cette idée de l'implication géopolitique et stratégique du cyberespace pourrait presque aujourd'hui paraître comme une évidence au regard de l'attention permanente dont cet environnement fait l'objet dans les médias, les ouvrages plus ou moins spécialisés, les textes et les doctrines militaires actuels. Pourtant, au début des années 2000, ce thème semblait encore exotique et réservé aux ingénieurs. Dans les milieux stratégiques, si la guerre en réseau était déjà un objet d'étude, Internet dans sa dimension civile, et en tant qu'espace social, était peu abordé et ne constituait pas une priorité. Force est de constater que cette situation a changé. À l'instar des États-Unis et de l'Organisation du traité de l'Atlantique Nord (Otan), la France a placé, depuis le Livre blanc de 2008, la sécurisation du cyberespace au premier rang des sujets de défense.

Or penser la cyberdéfense impose d'abord de resituer l'espace numérique dans un contexte global. Il n'est pas possible aujourd'hui de dissocier de façon très nette les enjeux de défense de ceux de la sécurité. Une cyberattaque de grande ampleur sur des infrastructures nationales est tout aussi préoccupante pour un État que des menaces plus diffuses, comme celle de la propagande qui se joue sur les réseaux sociaux et qui peut, dans les cas les plus extrêmes, conduire à des actes criminels ou terroristes. Aussi, il n'est pas possible non plus d'isoler, au sein de l'espace numérique, un champ qui serait spécifiquement technique et un autre (ou plusieurs autres) d'ordre social, économique, politique ou juridique. Des exemples, comme l'attaque par déni de service subie par l'Estonie au printemps 2007[1], montrent au contraire l'imbrication toujours plus fine de ces différents champs. En effet, si la dimension technique était évidente du fait de la nature de l'attaque, les dimensions politiques (relations avec la Russie et avec les minorités russes), économiques (pertes financières importantes pour le pays) et sociales (blocages d'institutions étatiques et d'infrastructures financières) étaient tout aussi prégnantes.

Nous traiterons cette problématique en trois chapitres. Dans un premier temps, il s'agit pour nous de montrer en quoi *le cyberespace est également une construction sociale et politique* qui peut être abordée par le prisme des outils traditionnels de la géopolitique et des relations internationales. De fait, s'il apparaît à première vue comme un espace essentiellement virtuel, ce domaine repose en réalité sur des infrastructures tout à fait tangibles qui permettent d'en dresser une approche géostratégique. Par ailleurs, si l'environnement numérique semble relativement récent, les pratiques conflictuelles qui se déroulent en son sein ne sont pas en tant que telles de pratiques nouvelles et elles s'inscrivent donc dans la pensée stratégique plus ancienne.

1. Le 27 avril 2007, l'Estonie avait dû faire face à des cyberattaques de grande ampleur, en provenance de Russie, ciblant plusieurs infrastructures administratives, bancaires ainsi que des organes de presse du pays. La méthode utilisée était celle dite du « déni de service » : un nombre considérable de requêtes avaient été envoyé par des « *botnets* », ou « ordinateurs-zombies », pour saturer les serveurs. Cette situation faisait suite à des tensions avec les minorités russophones du pays, en raison de la décision symbolique prise par le gouvernement de retirer du centre-ville de Tallinn un ancien monument aux morts soviétiques de la Seconde Guerre mondiale.

Un deuxième chapitre est consacré aux *dimensions sociales du combat cybernétique* (caractère sociotechnique du cyberespace, aspects socioculturels de la cyberdéfense). Il montre en particulier en quoi des notions classiques comme celles de vulnérabilités ou de menaces (et les réponses à y apporter) doivent être analysés et conçues en articulant de manière dialectique des processus techniques et des dynamiques sociales en permanente évolution.

Enfin, le troisième chapitre est consacré aux *aspects juridique et stratégique de la conflictualité dans l'espace numérique*. De fait, tant dans le domaine du *jus in bello* que dans celui *jus ad bellum*, des normes et des textes ont émergé aujourd'hui au niveau international et commencent à faire autorité, tandis que certaines questions (celle des cyberarmes entre autres) restent encore en débats. Une généalogie de la notion de cyberdéfense est également proposée, en resituant ce concept dans la réflexion stratégique des dernières décennies.

Chapitre 1

La construction politique de l'espace numérique

L'espace numérique : les promesses de l'aube

Jean-Fabrice Lebraty

En septembre 2022, malgré un contexte international turbulent et sombre, cinq entreprises américaines, connues sous l'acronyme GAFAM, cumulaient, à elles seules, une capitalisation de près de 8 000 milliards de dollars – sans parler des NATU (Netflix, Airbnb, Tesla et Uber) et des BHATX (Baidu, Huawei, Alibaba Group, Tencent et Xiaomi). Le poids économique de ces géants illustre le fait qu'année après année, malgré une grande volatilité et des chutes brutales, les entreprises du numérique deviennent des acteurs majeurs dans l'ensemble du monde. Ainsi, le terme de cyberespace, imaginé par William Gibson en 1982, semble s'imposer ici. À l'instar des grappes de satellites du projet Starlink qui permettent un accès Internet à l'ensemble de la planète depuis l'espace, les zones dépourvues d'accès filaire pourraient rejoindre un espace numérique ou, plus exactement, des espaces numériques, grâce aux investissements dans les métaverses réalisés par Meta (anciennement Facebook), ainsi que d'autres acteurs, qui contribueraient à proposer non pas un cyberespace, mais bien des cyberespaces. Ainsi, il se pourrait que nous ne soyons seulement qu'à l'aube du développement de ce concept de cyberespace.

Ces premières lignes pourraient sembler être tirées d'un roman de science-fiction des années 1950. Pourtant, elles recouvrent des faits avérés

à ce jour[1]. Il n'y a donc pas de magie ou de fantaisie dans ce cyberespace actuel et proche. Néanmoins, le mélange entre discours politiques, blogs, messages sur les réseaux sociaux et séries télé contribue à générer une certaine confusion dans les esprits des spectateurs, mais aussi dans ceux de certains acteurs confrontés à cette transformation numérique.

Dès lors, le but de ce chapitre est de tenter de faire un tri entre ce qui apparaît envisageable rationnellement, ce qui semble être merveilleux mais peut quand même se réaliser – comme pouvaient l'être certaines couvertures du magazine *La Science et la Vie*, créé en 1913 – et ce qui relève de l'éternel fantasme – comme a pu l'être le film *Terminator*. En résumé, dans ce chapitre, nous allons nous poser cette question : quelles pistes de réflexion plausibles pouvons-nous poser pour fonder des stratégies intégrant cyber et organisations ?

Cette question possède un intérêt théorique, mais également managérial. Tout d'abord, un intérêt théorique car elle pose la question de savoir si les modèles académiques que nous utilisons actuellement seront toujours adaptés au contexte futur. Plus en avant, elle peut également remettre en cause les paradigmes sur lesquels sont bâtis ces modèles. Prenons, par exemple, les modèles de stratégie de Porter (1996) ou de Kim et Mauborgne (2010). Le but est de conserver une situation dominante, supposant ainsi que l'on est déjà dominant. L'asymétrie engendrée par le numérique peut remettre en cause cette position de domination. Enfin, cette question présente également un intérêt managérial fort. En effet, en accord avec le célèbre ouvrage *Grandeur et décadence de la planification stratégique* (Mintzberg, 1994), il convient plus que jamais d'éviter de bâtir des plans considérés comme de véritables carcans à l'adaptation. Il s'avère tout aussi essentiel pour les organisations d'avoir une idée du contexte futur pour prendre des décisions et conserver une certaine liberté de manœuvre.

Pour répondre à la question posée, nous reviendrons dans un premier temps sur deux caractéristiques actuelles favorisant des innovations de rupture. Puis, nous décrirons trois de ces innovations qui devraient s'imposer dans les prochaines années, avant de proposer sept scénarios en nous fondant sur la série dystopique *Black Mirror* et celle plus réaliste *Mr. Robot* pour mettre en avant des enseignements quant au futur potentiel en matière de cyber. Enfin, nous proposerons l'idée d'un changement de paradigme qui pourrait s'avérer salutaire, même si quelque peu douloureux à suivre.

Un contexte propice aux innovations de rupture

La croissance exponentielle de l'Internet ne peut être considérée comme un phénomène linéaire. Le franchissement de seuils a conduit l'environnement mondial à se transformer (Gladwell, 2000). Le développement de la

1. L'auteur souhaite indiquer que cette deuxième version, qui s'inspire de la proche science-fiction, doit être complétée par le suivi des scénarios du projet *Red Team* qui, lui ; se fonde sur la vraie et fondamentale science-fiction.

globalisation a été poussé par le développement de l'Internet. En effet, l'arrivée d'un protocole unifiant l'ensemble des échanges numériques mondiaux a permis la circulation de millions de containers eux aussi standardisés au niveau international.

Malgré la standardisation du protocole, l'Internet tend à se fracturer. D'ailleurs, le magazine *Wired* de novembre 2020 proposait comme titre de couverture le néologisme *splinternet*, jouant ainsi sur les mots *split* (scinder) et Internet. Ainsi, il existe, par exemple, un Internet occidental aux côtés d'un Internet chinois. Mais, pour chacun de ces mondes, des tendances structurelles identiques s'observent.

Un exemple permet d'illustrer une des transformations induites par l'Internet depuis 1995. Alors que les modèles commerciaux traditionnels de vente poussaient les entreprises à se centrer sur un nombre limité de types de produit – dans le but de tenter d'uniformiser les goûts des consommateurs afin de réduire la variété de la demande et, ainsi, de se faire une marge plus grande –, l'Internet a permis de générer du profit sur la vente de millions de produits différents avec des stocks très faibles pour chacun d'entre eux. C'est le modèle de la longue traîne, brillamment mis en place par Amazon (Anderson, 2006)[1]. Aujourd'hui, Amazone propose plus de 12 millions de produits en son nom et 350 millions au nom de vendeurs indépendants, tout en ayant en moyenne moins de dix articles par référence en stock et en vendant plusieurs milliards de produits par an. L'Internet permettant aux utilisateurs d'accéder à des marchandises dans le monde entier, chacun d'entre eux peut y trouver le produit spécifique qu'il désire. Le concept de personnalisation de masse a émergé des pratiques du commerce en ligne. Airbnb aurait pu aussi ici servir d'exemple puisque le site propose 7 millions de chambres différentes dans plus de 100 000 villes dans le monde. Ajoutons que le management d'un grand nombre de produits variés n'a été rendu possible que grâce à une optimisation de l'usage du matériel informatique. Ainsi, il faut comprendre la notion de *cloud computing*, qui est une technique d'équilibrage des charges entre un grand nombre de machines qui appartiennent à un même ensemble. Cette optimisation a été le moteur ayant permis la montée en charge (scalabilité) et l'augmentation rapide de l'offre tout en lissant les coûts.

Reprenons le cas d'Amazon pour illustrer une autre caractéristique du marché électronique mondiale dont les implications sont encore plus grandes : la participation des utilisateurs. En 1995, la majorité des transactions ne concernait que les parties prenantes de celles-ci et comprenait un nombre très faible d'échanges. Par exemple, un vendeur offrait un produit à un acheteur et la réception du produit clôturait la transaction. Certes les systèmes de carte de fidélité existaient déjà, mais ils ne permettaient pas un gros volume d'interactions. Or, l'entreprise Amazon s'est retrouvée face à un défi : celui de donner des informations sur les millions de produits qu'elle proposait. Trois solutions s'offraient alors à elle. La première consistait à demander aux fabricants de décrire leurs propres produits. Cependant, cette solution posait

1. https://www.sec.gov/Archives/edgar/data/1018724/000101872417000011/amzn-20161231x10k.htm (consulté le 25 octobre 2022).

le problème de l'intégrité du fabricant qui aurait pu enjoliver les qualités de ses marchandises. La deuxième aurait été que l'entreprise Amazon teste elle-même les produits et donne son avis sur ceux-ci. Mais cette solution interne coûteuse n'aurait pas résolu le problème de la confiance, les clients ayant pu penser qu'Amazon aurait pu favoriser des produits pour son bénéfice propre, plutôt que pour celui des acheteurs. Enfin, la troisième solution aurait été de demander à un cabinet indépendant externe à Amazon d'évaluer les produits et de publier les résultats de ses tests. Cependant, cette solution aurait été bien trop onéreuse, surtout au regard du modèle de la longue traîne et des millions de références concernées. Aussi, l'entreprise Amazon a-t-elle utilisé une quatrième solution : celle du *crowdsourcing* (Lebraty et Lobre, 2015). Ce sont les clients qui donnent leurs avis sur les produits qu'ils ont achetés. Ainsi, pour Amazon, le bénéfice est triple : un coût faible, une confiance assez élevée et une fidélisation de la communauté de clients en la faisant participer à la vie du site. Cette participation des utilisateurs, aussi appelée phénomène 2.0 dès 2005 par Tim O'Reilly[1], a constitué le point de départ de l'essor des réseaux sociaux sur lesquels des milliards d'individus postent du contenu à chaque instant. L'essor des réseaux sociaux depuis 2006 a conduit à modifier les perceptions. L'effet d'un simple tweet peut largement dépasser le cadre d'une application informatique. Ainsi, la dynamique des communautés d'utilisateurs authentiques ou non sur les différents réseaux sociaux constitue un critère important du monde cyber. La crise de la Covid-19 en a d'ailleurs constitué un excellent terrain d'étude (Boulet et Lebraty, 2020).

Ainsi, dans le contexte actuel, le monde numérique permet de proposer à chacun une offre adaptée tout en laissant la possibilité à chaque membre de la foule de participer ou non. Les flux sont donc bidirectifs, générant alors un système complexe dont l'évolution est délicate à prédire. Pourtant, à court terme, quatre innovations de rupture dessinent selon nous un nouveau contexte qui conditionne les modes d'actions, tant au niveau individuel qu'organisationnel.

Quatre innovations de rupture déterminantes

Évoquées depuis plusieurs années, quatre technologies sont en pleine phase d'adoption et devraient, dans un futur proche, arriver à maturité tout en réalisant des synergies avec leur environnement, mais également entre elles, conduisant aux fondements du contexte de notre proche futur.

La première innovation de rupture est constituée par le développement de l'impression 3D. Comme l'explique brillamment Chris Anderson (2012), la grande force des imprimantes 3D et des machines à découpe laser réside dans le fait de parler la même langue ou, du moins, de savoir lire différents formats de fichier mondiaux. De notre point de vue, le développement de la fabrication 3D recèle un potentiel aussi important que celui de l'Internet en 1995. Ainsi,

1. http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (consulté le 25 octobre 2022).

après la standardisation des conteneurs et celle du protocole de communication Internet, vient la standardisation des modèles de conception assistée par ordinateur. Après la démocratisation de l'accès au virtuel se profile l'universalité de l'accès à la production de biens physiques. Notons, d'ailleurs, que le fait que chacun puisse fabriquer directement un produit à amener à la création d'une notion : les personnes qui réalisent ces objets sont appelées les faiseurs ou les *makers*. Anderson (2012, p. 21) précise les trois principales caractéristiques de ces *makers* :

1. les *makers* utilisent des technologies numériques pour créer des prototypes et des produits finis ;
2. l'esprit d'une communauté virtuelle de faiseurs réside dans le partage des modèles et des idées et dans la collaboration entre membres ;
3. le fait d'utiliser des formats de fichier standards pour les modèles permet à tous ceux qui le souhaitent d'envoyer leur création à une entreprise qui se chargera de la fabrication de ce modèle. D'une certaine manière, l'esprit de l'*open source* se retrouve chez les *makers*.

Un exemple d'intérêt sécuritaire peut être mis en avant. En effet, en octobre 2012, le magazine *Wired* indiquait que Cody Wilson, un étudiant en droit de 25 ans à l'université du Texas, proposait de mettre en ligne un modèle permettant de fabriquer un pistolet avec une imprimante 3D. En décembre 2012, le même magazine classait ce jeune étudiant parmi les 15 personnes les plus dangereuses de la planète. En mai 2013, le premier prototype a été testé et le modèle largement diffusé. Dix-huit mois plus tard, le prototype a été amélioré et l'on a assisté à une prolifération d'armes de poing et d'épaule de plus en plus innovantes. Un site recensant l'ensemble des modèles disponibles existe d'ailleurs (https://defcad.com/), ce qui peut paraître quelque peu effrayant.

La seconde innovation émergeante provient de la rapide expansion du nombre d'objets connectés. L'Internet des objets (IoT en anglais) existe déjà et cette nouvelle toile devient, jour après jour, plus forte. Que ce soit de simples capteurs d'humidité ou de plusieurs mesures corrélées, comme les produits de santé proposés par la marque Withings, qu'ils soient à destination du grand public ou à celle des industriels, les objets en circulation sont tellement nombreux qu'il est difficile de les chiffrer. Cependant, on estime actuellement que leur nombre est de l'ordre de la dizaine de milliards. Bien évidemment, ces capteurs nécessitent de bénéficier d'un écosystème de création, comme il en existe d'ailleurs près de Toulouse (Bessagnet *et al.*, 2021), et d'une architecture complète et sécurisée (Wu, 2021). L'ensemble des données collectées permet de nouvelles applications (comme la voiture autonome, par exemple) et une meilleure compréhension et maîtrise de son environnement par une analyse des données (Fortino *et al.*, 2019). Ainsi, l'IoT contribue à redessiner les espaces de manœuvre et donc le champ des possibles.

La troisième innovation de rupture réside dans la montée en puissance de la *blockchain* (BC). Connue du grand public, grâce notamment aux envolées du Bitcoin, une BC se définit comme un registre ouvert et distribué, qui permet d'enregistrer les transactions entre deux parties d'une manière sécurisée, vérifiable et permanente. Aujourd'hui, ce livre n'est plus statique mais peut être