ANNUAIRE FRANÇAIS DE RELATIONS INTERNATIONALES

2016

Volume XVII

PUBLICATION COURONNÉE PAR
L'ACADÉMIE DES SCIENCES MORALES ET POLITIQUES

(Prix de la Fondation Edouard Bonnefous, 2008)

Université Panthéon-Assas
Centre Thucydide

LES DEUX PHASES DE LA CYBERGUERRE

PAR

JACQUES TOURNIER (*)

La littérature sur le sujet atteste que la question de la cyberguerre est difficile à conceptualiser. Et il semble que cette difficulté tient pour une grande part à la nature composite et quelque peu insaisissable du cyberespace.

Certes, le cyberespace revêt d'abord et évidemment la dimension d'une réalité objective : il renvoie à cet ensemble singulier formé par la mise en réseau des machines qui produisent, traitent et exploitent des données numériques et dans lequel on comprend également les flux que permettent leurs interconnexions ainsi que les opérations qui s'y déroulent, soit en réponse à des impulsions données par les humains avec lesquelles elles sont interfacées, soit automatiquement pour avoir été programmées à cet effet.

LE CYBERESPACE COMME MILIEU

Le cyberespace est plus qu'une entité caractérisée par une certaine unité matérielle avec laquelle les hommes entretiendraient un rapport d'extériorité objectivable. Il est aussi un « milieu » dans lequel ils baignent, milieu qui est néanmoins hétérogène par rapport aux milieux naturels qui constituent le cadre spatial dans lequel s'inscrit le déploiement de l'humanité. En effet, même s'il a sans doute la propriété d'être un espace commun, le cyberespace, qui relève par essence du registre de l'artefact, n'a pas d'existence autonome par rapport aux êtres humains. Sans les innombrables interactions qui le relient en permanence aux hommes, il ne fonctionnerait plus et ne connaîtrait pas cette expansion incessante aux ramifications protéiformes qui viennent l'inscrire toujours plus profondément dans la texture du monde qu'ils construisent.

En outre, non content d'innerver une partie continuellement croissante du substrat matériel des activités humaines – tout au moins dans les pays les plus avancés –, le cyberespace tend à devenir une espèce de soubassement immanent au développement immatériel des sociétés – ce qui achève de lui conférer la dimension d'une totalité métaphorique de notre monde et d'en brouiller passablement les contours. Environnement instrumental, sphère d'interactions qui abolit le temps et l'espace entre

(*) Haut fonctionnaire, ancien rapporteur général du Livre blanc sur la défense et la sécurité nationale (2013).

les hommes, miroir numérique de nos sociétés, voire matrice de plus en plus déterminante de leur auto-engendrement : de fait, c'est bien sous de multiples visages que le cyberespace se présente à la prise de la guerre.

Que le cyberespace soit rapidement devenu un relais propice à l'expression de la violence des hommes n'a rien que de très normal, dès lors qu'à l'instar de la plupart des objets techniques forgés par ces derniers les potentialités *a priori* bénéfiques que recèle sa nature première d'outil n'ont pas manqué d'être exploitées ou asservies à des fins moins heureuses. En outre, l'infinie variété de ses domaines d'application lui a donné de pouvoir être le vecteur, voire le théâtre de la transposition, dans le langage du numérique, de la plupart des agissements auxquels les pulsions agressives ou les passions belliqueuses entraînent aussi bien les individus que les groupes qu'ils forment, des associations malfaisantes aux Etats-nations. Cela, en parfaite résonance avec les multiples facettes de la conflictualité contemporaine, marquée par la banalisation diffuse de ses modalités instrumentales et la dilution du spectre des acteurs qui s'y livrent.

Toutefois, dans la mesure où le cyberespace semble être de plus en plus consubstantiel à la trame des sociétés humaines, le caractère mimétique de la violence qui s'y déploie rend tentant de le considérer, notamment du point de vue de la guerre, comme une espèce d'avatar du monde réel, où serait duplicable l'ensemble des paradigmes auxquels obéit la dynamique des conflits armés conventionnels, mais, au-delà, dont la prégnance et la centralité diffuse pourraient augurer qu'il devienne le foyer de substitution ou sinon principal de la guerre. Et on se prend à imaginer que si la guerre s'avérait effectivement susceptible d'être circonscrite au seul théâtre du numérique, la dimension de létalité qui lui est inhérente pourrait en être largement extirpée, cependant que l'immanence du cyberespace aux sociétés humaines n'en permettrait pas moins d'obtenir les effets recherchés par la guerre, à savoir plier ou soumettre la volonté de l'adversaire aux fins poursuivis par l'attaquant.

En l'état actuel, cette absorption, par le cyberespace, de la totalité du spectre de la guerre demeure du registre de la fiction. Force est en effet de constater que, jusqu'à présent, les actes de cyberviolence participant manifestement d'une intention politique n'ont guère produit, y compris pour les plus importants, d'effets coercitifs déterminants dans le monde réel. Tout au plus, pour ceux d'entre eux qui sont restés confinés au seul domaine du cyber – Stuxnet, Shamoon, l'Estonie –, ont-ils provoqué des perturbations dont l'impact a été de l'ordre de la gêne ou de l'entrave temporaires, mais surtout pas celui de la contrainte irrésistible. Quant aux autres – Géorgie, bombardement par Israël de la centrale Al-Kibar –, ils n'ont jamais été qu'une composante à fonction facilitatrice insérée dans un dispositif militaire constitué pour mener des opérations des plus classiques.

Deux caractéristiques principales

De fait, les actions hostiles qui, dans ou à travers le cyberespace, sont rattachables au registre de la guerre présentent deux caractéristiques principales ayant vraisemblablement pour effet d'en circonscrire la portée stratégique.

La première de ces caractéristiques procède de la dimension aussi subreptice que furtive de l'action de guerre dans le cyberespace : qu'elle soit véhiculée à la vitesse de la lumière ou déclenchée par un virus dormant installé de longue date, on ne voit pas venir l'attaque, pas plus qu'on ne peut voir d'emblée d'où elle vient réellement ; en outre, toute riposte frontale consistant à détruire par une contre-offensive cyber la source de l'agression est non seulement quasi impossible, faute de pouvoir la désigner, mais elle ne sert à rien dans la mesure où la capacité de frappe de l'agresseur est immédiatement périmée dès lors qu'elle a donné à l'attaqué d'identifier et de remédier à la vulnérabilité par où il a été saisi. A quoi s'ajoute le fait que l'évolution continue du cyberespace oblige les attaquants à faire preuve d'une très grande mobilité pour trouver de nouvelles vulnérabilités à la place de celles qui ont été entre-temps traitées. Enfin, le mode de fonctionnement propre à la cyberguerre interdit à quiconque de découvrir à des fins dissuasives les armes qu'il pourrait avoir forgées, sauf à en dégrader, voire à en ruiner complètement les potentialités, dès lors qu'il offre de la sorte à ses adversaires la connaissance et donc la possibilité de résorber les vulnérabilités visées par ces armes.

La seconde caractéristique réside dans la très grande technicité requise pour forger des cyberarmes véritablement pointues, c'est-à-dire susceptibles de pénétrer dans des systèmes complexes et d'y provoquer d'importants dommages. Cette réalité est le pendant du niveau toujours plus élevé de la protection dont les pays capables de maîtriser les technologies informatiques s'emploient à pourvoir les systèmes qui représentent pour eux des enjeux d'importance vitale. Autrement dit, s'il ne paraît pas très difficile de porter des attaques sur la partie largement ouverte de la couche supérieure du cyberespace (défacement de sites « grand public », DoS ou *Denial of service attack*) – attaques dont les conséquences sont plus embarrassantes que destructrices, la possibilité de mener une attaque capable de causer des dommages substantiels sur un système complexe suppose une préparation experte de très haut niveau et de longue haleine.

Un très lourd investissement est donc le préalable à la fabrication de telles armes, dont l'emploi est généralement limité à une cible donnée et voué à un usage unique et qui, au surplus, n'offre pas de garantie absolue quant aux effets collatéraux de dissémination et de contamination susceptibles d'être le corollaire de sa mise en œuvre. Il en résulte que seuls les pays avancés semblent être en mesure d'aligner le potentiel approprié de ressources, notamment humaines, en vue de se doter d'une capacité significative de cyberarmes actives et efficaces. Juste retour des

choses, en quelque sorte, puisque ces pays sont les plus concernés par la problématique des risques de cyberattaques compte tenu de la dépendance toujours accrue de leur fonctionnement global aux systèmes d'information.

Topologie du cyberespace du point de vue de la guerre

Ces deux caractéristiques centrales de la cyberconflictualité ont un effet déterminant sur la formation de ce qui peut être appréhendé comme la topologie du cyberespace du point de vue de la guerre.

Car, en l'état actuel des choses, il y a lieu en effet de considérer que la question de la cyberguerre peut être d'autant mieux cernée qu'on admet l'existence de deux espaces dissociés et néanmoins tangents ouverts au déploiement de la cyberconflictualité : d'une part, celui où foisonnent les attaques dépourvues de portée destructive significative et qu'on qualifierait volontiers comme un espace du « tout-venant » de la cyberagression ; d'autre part, celui où sont susceptibles de se déployer les cyberarmes au potentiel réellement destructeur et qui a la structure d'un espace discret, dans la mesure où, même s'ils ne sont pas identifiés, tant les acteurs que les armes y sont *a priori* dénombrables, parce que relativement concentrés.

Comme on peut le constater aisément, la cyberconflictualité relevant du registre du « tout venant » reste circonscrite à la sphère du cyberespace, où elle se déploie selon des modalités qui l'apparentent à l'action clandestine. Les agressions y sont opérées à visage couvert et relèvent de l'ordre du coup de main subversif, de la *razzia* de données, du raid ou de l'incursion à des fins de sabotage de systèmes appartenant à la couche informationnelle du cyberespace. Pour reprendre l'expression opportune de Christian Malis, le cyberespace est bien devenu, sous cet angle, le théâtre multiforme et largement aveugle d'une « *guérilla cybernétique endémique mondiale* » (1), dont on peut inférer, sans trop se tromper, que s'y pressent toutes les catégories possibles d'acteurs, des *hackers* individuels aux grandes puissances en passant par les collectifs d'activistes ou les groupes terroristes.

Le fait est que le grouillement des cyberattaques de ce type est un facteur d'intranquillité, en particulier pour les pays les plus « info-dépendants », puisqu'ils ne peuvent jamais complètement connaître les vulnérabilités de tous leurs systèmes et le niveau de risque qui peut en résulter. Cela, d'autant plus que certaines de ces attaques sont effectivement capables de provoquer des perturbations dérangeantes ou d'être la cause de déprédations embarrassantes. Dans le même temps, on voit bien que cette « guérilla » reste ce qu'elle est, que ses opérations demeurent en deçà d'un seuil où les dommages occasionnés seraient véritablement destructeurs, à une échelle telle que le terme de « guerre » serait en l'espèce approprié.

(1) Christian Malis, *Guerre et stratégie au XXIe siècle*, Fayard, 2014.

Pour ce qui est des acteurs infra-étatiques, il est probable que le non-franchissement de ce seuil procède de la difficulté à élaborer des armes au pouvoir de pénétration et de dévastation suffisantes pour produire des effets d'ampleur commensurable à celle des attentats au retentissement international. En revanche, il ne fait pas de doute que, pour les puissances les plus avancées, cette limitation résulte de la retenue qu'elles s'imposent dans l'expression de leur violence intrinsèque et de l'attention qu'elles prêtent à en maîtriser les possibilités d'escalade. Et on voit bien que, sous l'empire du gel de la guerre auquel a conduit la possession d'armes nucléaires, le cyberespace offre un terrain d'expansion à cette soupape qu'est pour elles l'action clandestine, c'est-à-dire à cette façon de passer à l'acte en mode mineur ou encore, si on veut bien passer l'expression, de se « faire des coups en douce » – sachant qu'il est implicitement admis que ces pratiques s'inscrivent aussi dans une dynamique de tests réciproques dont la dialectique des volontés finit, au moment où la tension devient trop forte, par arrêter la ligne toujours provisoire d'équilibre (*cf.* Chine/Etats-Unis).

Selon toute vraisemblance, le franchissement de ce seuil ne peut que marquer le basculement dans un conflit d'une toute autre portée que celle à laquelle restent circonscrites ces myriades d'assauts et de raids clandestins qui traduisent, dans le cyberespace, l'ordinaire quotidien de la rivalité des nations. Car on ne voit pas comment une cyberagression de « vive force » pourrait rester associée à la perspective d'une conflictualité exclusivement confinée dans le cyberespace. Il semble en effet inévitable que l'élévation du niveau de frappe dans le cyberespace ne puisse qu'occasionner – ou, le plus souvent, accompagner – ce qui constitue bel et bien un « changement de phase », c'est-à-dire le passage à une conflagration classique où le cinétique retrouve toute sa place et où le cyber ne représente plus qu'une modalité parmi d'autres des opérations de combat.

Les réalités invitent de fait à considérer qu'il a y bel et bien un point de bascule ou encore une rupture de continuité entre l'espace enclos de la « *cyber-guérilla endémique* » et celui où le cyber devient un instrument de la guerre – au sens de l'action véritablement coercitive et dévastatrice. L'infirmation de cette discontinuité topologique supposerait de pouvoir prouver qu'il existe des cyberarmes de destruction massive capables de mettre instantanément un pays par terre, y compris en le privant de toute capacité cinétique de seconde frappe. Car, en bonne logique, seule l'existence de telles cyberarmes serait de nature à faire de la cyberbataille l'*ultima ratio* de la guerre – ce qui, au stade où nous en sommes, relève de la pure fiction, mais n'en participe pas moins d'un fantasme assez commun : celui de l'arme ultime qui, en l'espèce, pourrait à elle seule subvenir à la guerre, avec en outre l'avantage immense d'épargner aux êtres humains les horreurs du « feu qui tue ».

Tant qu'on en n'est pas là – le sera-t-on jamais ? -, il semble raisonnable de considérer le cyberespace comme le moyen de forger de nouvelles

armes de guerre répondant à certaines fonctionnalités : celle d'une salve en premier, visant à affaiblir ou à paralyser les systèmes informatiques critiques du dispositif militaire adverse ; celle d'un amplificateur des capacités de guerre électronique permettant de garantir, voire démultiplier, les effets de l'action cinétique ou encore de protéger les forces armées et de faciliter leurs mouvements en créant autour d'elles une espèce de phénomène de « super-cavitation » par aveuglement de l'adversaire ou par annihilation temporaire de ses capacités de réaction. Autrement dit, des armes qui constituent de nouvelles façons, certes sophistiquées et adaptées à l'âge du numérique, de traiter des fonctionnalités classiques telles que la frappe dans la profondeur ou l'appui tactique aux combattants.

De la cyberguerre a l'emploi de la force armée

Cette dualité de phase pose en fait la question de savoir dans quelle mesure l'action hostile dans le cyberespace peut devenir le facteur déclenchant d'une guerre nécessairement vouée à « faire parler le feu ». C'est précisément la problématique cruciale à laquelle renvoie l'économie de la déclaration qui a été publiée par les alliés de l'Organisation du Traité de l'Atlantique-Nord (OTAN) lors du sommet du Pays de Galles de 2014, à la suite des attaques dont l'Estonie avait été victime. Selon les termes de cette déclaration, les cyberattaques sont désormais reconnues comme l'une des circonstances justifiant l'invocation – et donc la mise en œuvre – de l'article 5. Autrement dit, dans le sillage de la doctrine américaine énoncée en 2011 et des travaux qui ont débouché en 2012 sur le Manuel de Tallinn, a été ainsi acté ce principe d'un seuil de bascule dans l'ordre de la « vraie » guerre, principe dont l'application concrète reste encore entourée d'une très importante zone de flou. Car on peut aisément mesurer comme il est difficile de quantifier le niveau de gravité à partir duquel une attaque cyber est considérée comme le point de décrochage qui vient réintroduire un lien de continuité entre le cyber et le conventionnel, voire le nucléaire.

A supposer en théorie que la question se pose un jour concrètement, on peut augurer que la réponse ne butera pas forcément sur le problème de l'attribution : hors les cas d'action de groupes terroristes – dont il reste à prouver qu'elles peuvent ou pourront atteindre une capacité cyber à infliger des dommages dévastateurs –, ce qui serait au pire une sorte de « Pearl Harbor cyber » ne peut qu'être le résultat d'une montée de tension entre des acteurs étatiques somme toute assez identifiables, puisque, une fois encore, seuls ne devraient être potentiellement concernés que les pays les plus avancés au plan technologique.

Et toujours d'un point de vue théorique, on peut concevoir que le véritable obstacle à la cristallisation de ce seuil résidera essentiellement, tout au moins chez les Occidentaux, dans la difficulté qu'ils éprouvent aujourd'hui à envisager la possibilité de s'engager dans une guerre interétatique contre des adversaires dont les capacités militaires sont d'un niveau comparable

aux leurs. Car de toute façon, à ce stade – et c'est bien là ce que signifie la déclaration de Newport –, il ne faudra pas compter sur le cyber pour faire l'économie du cinétique. Peut-être ne s'agit-il là, effectivement, que d'un problème théorique, dès lors qu'il apparaît que le jeu de la dissuasion, aussi bien nucléaire que conventionnel, reste sans aucune espèce de doute le véritable verrou qui retient les puissances d'ouvrir, y compris avec une clef cyber, la boîte de Pandore d'où peut surgir la guerre.

Il reste aussi que l'un des moyens de ne pas avoir à se poser cette question difficile se trouve dans l'efficacité de la cyberdéfense qu'on met en œuvre. Car, après tout, malgré la paranoïa à laquelle incline aisément le caractère invisible du monde du cyber et malgré l'avantage qu'on y prête aux attaquants, il est sans doute loisible de penser qu'une bonne protection des systèmes critiques constitue la voie la plus appropriée pour s'assurer que l'impact des cyberattaques subies restera circonscrit à un niveau acceptable. Autrement dit, la physionomie de la cyberguerre invite à conclure qu'un effort sur ce plan est sans conteste primordial pour s'éviter d'effleurer ou, pire, d'avoir à franchir le seuil critique à partir duquel l'expression irrésistible de la conflictualité entre les hommes et les peuples revêt le funeste visage de la guerre.