Le commencement des cyber-armes

Djamel Metmati

Juillet 2013 – Article n°III.9

Si les Etats-Unis concourent à diffuser la cyber-guerre par la mise en ligne de documentation à vocation tactique et stratégique, force est de constater qu'ils produisent un effet d'entraînement pour les autres pays. Ce mouvement est double car il réunit des pays qui consentent au concept de la cyber-guerre et d'autres qui l'a qualifie encore de mythes. Ensuite, l'état de l'art en matière de cyber-attaques montrent deux dynamiques. La première traduit une réflexion stratégique où les attaques sont vues comme un phénomène découlant de la diffusion des réseaux. La seconde décrit l'émergence de cyber-attaques raisonnées et pensées comme une réalité dont les objectifs sont économiques, politiques et militaires.

Néanmoins, la cyber-attaque n'existe qu'à travers une arme. Or, celle-ci résulte d'une méthode particulière qui s'avère plus ou moins complexe dans la conception et l'exécution suivant les effets recherchés. La plupart des attaques actuelles s'apparente à la « gerra »[1] ou états de violence nés d'organisations ou de groupes non-étatiques. La diminution des conflits classiques laissent entrevoir une multiplication d'états de violence. Ce phénomène appuyé par le développement des réseaux dans le fonctionnement des sociétés et des économies annonce une redistribution de la violence selon des paramètres nouveaux.

Le cyber-space incarne ce processus en intégrant ces états de violence selon des modes opératoires inédits pour des effets identiques. La question est donc de connaître la manière dont le cyber peut être utilisé comme une arme. D'autant que le constat du théâtres des opérations réseaux conduit à un mélange de « gerra » avec une volonté des États à rétablir le principe du monopole de la violence légitime à travers des capacités offensives et défensives.

L'établissement du manuel de Tallinn, texte évoquant un droit international de la cyber-guerre, définit indirectement l'usage dans le cyber-space d'actions défensives et offensives à partir d'une réglementation dont l'ambition reste l'encadrement des champs du possible dans la militarisation du cyber-space. Ce qui signifie, au final, que des armes existent, que leurs actions combinées par une organisation étatique et non-étatiques participe à la modification de l'action de nature militaire par un transfert des logiques combattantes dans les réseaux.

Pour illustrer ce propos, les cyber-armes sont des processus issus de programmes informatiques crées ou existants qui répondent à des modes opératoires militaires dans les effets recherchés. Elles s'appuient sur des stratégies de sécurité nationale sur la base d'actions directes sur les réseaux ou combinées aux manœuvres des forces armées dans une dynamique de destruction/interception et détection/discrétion.

1 Frédéric Gros, États de violence. Essai sur la fin de la guerre. Paris, Gallimard, 2006, 310p.

I - Principes de conception

L'approche de Thomas Rid[2] et de Peter Mc Burney donne un cadre général mais restrictif de la cyber-arme sans en associer, dans sa dimension « réseau », les acteurs, les cibles de la cyber-opérations. Cette caractéristique, qui définit nos sociétés d'aujourd'hui, définit la cyber-arme en tout ce qui peut être utilisé comme une arme dans le cyber.

Ces deux auteurs définissent la cyber-arme par « *un code utilisé ou conçu afin de menacer ou de causer des dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants* [3]». Celle-ci est analysée selon trois niveaux de potentiels : faiblement potentiel[4], fortement potentiel[5] et une combinaison des deux premiers niveaux[6].

Ces échelles traduisent des attaques qui vont du déni de service jusqu'à la destruction d'ordinateurs[7]. Ainsi, la technologie reflète la puissance théorique de l'arme.
Néanmoins, les critères discriminants pour définir les potentialités dépendent également des effets voulus et du produit final attendu pour atteindre les cibles. Le niveau technique de l'arme n'en définit que sa puissance potentielle, qui ne sera avéré qu'en une mise pratique à partir d'une planification dans laquelle d'autres vecteurs interviennent.

Une cyber-arme est alors le produit du niveau technique associé à des cibles, multiplié par le réseau dans lequel elle doit manœuvrer. En ce cas, l'approche systémique dans la conception et l'exécution d'une arme lui donne sa forme, sa puissance, sa durée de vie sur une échelle de temps définie.

Comme une cyber-arme ne subsiste pas aux caractères évolutifs des armes défensives, la planification et la coordination demeurent essentielle pour saisir la « TAZ »[8], ceci pour déclencher une attaque à partir d'un point d'un faible qui peut être corrigé par la défense sur un temps plus court. La cyber-arme répond à un ensemble de critères à savoir : l'objectif, le « Find and fix », la technique, la tactique d'emploi, la « TAZ »[9] , la fin de partie.

Le résultat résulte d'une équipe de développeurs qui génèrent l'arme en fonction des vulnérabilités métiers identifiées à partir d'une cartographie du système adverse. Cette méthode répond à un processus de réalisation de l'attaque qui s'appuie tant sur la partie technique que sur la partie humaine. En amont, le rôle joué par le renseignement ouvert à partir du croisement d'informations de données insignifiantes par elles-mêmes donne, à la cyber-arme, sa typologie.

En récoltant les données sur une période déterminée correspondant à l'effet recherché par le stratège par rapport à un contexte particulier, le data-mining[10] permet la construction de l'attaque où le travail d'analyse préalable des potentialités liées à des vulnérabilités techniques et humaines font converger les cibles atteignables pour réaliser l'effet souhaité à un moment donné. Comme pour les principes régissant les réseaux ad hoc, la cyber-arme constitue un code mais s'insère dans une action existante et voulue vers l'objectif[11]. La cyber-arme se construit sur des vulnérabilités métiers et

2 Thomas Rid,Cyberwar will not take place. Hurst/Oxford University press, 2013.
3 Cette définition de Thomas Rid introduit l'aspect culturel et technique de la cyber-arme à travers l'utilisation de codes de même nature
4 Le déni de service.
5 Les virus type Flame.
6 Une attaque majeure est précédée par des coups de semonce marqués par du déni de service.
7 En 2012 le virus Shamoon a infecté la compagnie pétrolière saoudienne Aramco et provoqué la destruction de 35 000 ordinateurs.
8 Zone autonome temporaire : technique qui consiste à maîtriser à un moment donné les flux réseaux.
9 Hakim Bey
10 Technique consistant à faire converger des données multiples pour en déduire un sens caché.
11 L'exemple du virus Flame.

humaines en cherchant l'altération. Elle s'attaque aux points faibles des systèmes homme-machine mais également au point fort[12].

La perception système du point de vue de la défense n'est effectivement pas la même que la vision qu'en ont les attaquants. La confrontation des modes d'action ami et ennemi définit alors cette notion de points forts et de points faibles. Il en résulte un rapport de force entre des acteurs qui se mesure par des vulnérabilités. La différence de l'avantage des uns sur les autres tient alors à l'imagination et à la propension à frapper vite et fort en étant constamment en mouvement. En ce cas, la planification avec les scénarios possibles et mises à jour restent déterminants[13].

Une fois que les possibilités d'attaques émergent de cette analyse, la cyber-arme peut être pensée et conçue. Pour la réaliser, le marché des failles façonne les potentialités de la cyber-arme en permettant de compresser les délais de réalisation du programme d'attaque. Il reflète la technologie du moment et encourage les effets de destruction en les combinant d'autant que les sociétés délèguent une partie de leurs fonctionnements dans les réseaux[14]. Les ordinateurs, téléphones et tablettes sont devenus par exemple les chariots de supermarché des temps modernes.

Si la révolution industrielle du XIXème a entraîné une modification de l'armement vers un accroissement de la puissance de feu et la portée, la cybernétique d'aujourd'hui rend les armes encore plus puissantes en diminuant leurs volumes pour un même effet. Le cyber n'échappe pas à ce processus, les armes développées y sont d'autant plus puissantes que les réseaux se développent en s'interconnectant aux objets et aux personnes[15]. Des attaques « réseaux » rudimentaires contre des systèmes naissants émergent désormais des armes plus perfectionnées[16] nécessitant des équipes de développeurs. Leurs chefs les associent à une cyber-manœuvre qui peut, en fonction des circonstances, s'inscrire dans une opération militaire classique.

Dans le cas inverse, son action sur les réseaux répond à un choix politique où une entité étatique ou non étatique souhaite mener une opération à moindre coût pour un effet identique sans avoir à rendre de compte dans le cadre du droit international[17].

I I- Principes de réalisation

Qu'il appartienne à une organisation étatique et non étatique, au cyber-combattant de réaliser tactiquement ce qui est possible, à partir d'une stratégie voulue par un acteur organisé. A ce moment intervient la dimension technologique et organisationnelle de l'arme à travers l'objectif.

La cyber-arme résulte d'une stratégie indirecte ou directe en fonction de l'engagement, du type d'objectif choisi qui correspond à plusieurs registres du "pipe" à savoir : psychologie, information, physique, électronique. Celle-ci embrasse trois familles d'ennemis : les entités étatiques, les organisations vitales, les industriels et PME dans lesquelles se trouvent les cibles pour réaliser l'effet.

Le piège technologique de la cyber-arme est d'en faire un produit uniquement technique voir commercial à partir d'une faille identifiée provenant pour la plupart du marché des exploits. Au

12 L'open web application security permet de visualiser la nature des failles existantes sur le web.

13 Cette méthode consiste à hiérarchiser ces propres failles et les opportunités d'attaques par un travail d'analyse d'une cellule entièrement dédiée.

14 Les ventes sur le web ont progressé de 14% au premier trimestre.

15 D'après Thierry Berthier, la diffusion transversale des algorithmes a des effets sur chaque secteur d'activité humaine

16 Le virus sKywiper concentre des malwares, du keylogger, des configurations de fichiers différents, des infections par des partages locaux, des exploits de Stuxnets, des DLL.

17 Le cas de Flame sur les centrifugeuses iraniennes

contraire, aux développeurs de produire un algorithme de défense ou d'attaque s'inscrivant dans une coordination basée sur une vision de l'attaque.

L'aspect militaire représente un des volets les plus sophistiqués de la cyber-arme car il peut mobiliser des ressources étatiques que n'aurons jamais d'autres entités. D'autant que face aux menaces et aux risques, l'État est la première ligne de défense ou le premier échelon. Qu'elle soit efficace ou perméable, l'effet de l'arme suggère une dimension nouvelle de l'opération militaire. Que ce soit Flame, l'affaire Aramco ou encore des exercices navals simulant des attaques réseaux, elles répondent à une planification supposée et avérée.

En revanche, d'autres cyber-opérations usent des cyber-armes psychologiques par le discours et la rumeur, que renforce le vecteur médiatique. L'affaire Cahuzac révélée par Médiapart démontre que ce type d'arme produit un effet technique sur les réseaux[18] et prend également la forme d'une perturbation des rapports de force entre différentes acteurs uniquement par la psychologie sociale liée aux réseaux.

La production d'armes cyber ne vient donc pas exclusivement des États car l'économie de la cyber-défense en plein développement se construit à partir d'un marché dans lequel évoluent des sociétés de sécurité informatiques. Elles paraissent pour le moment les plus aptes à suivre et à proposer des solutions d'attaques et de défenses dans le cadre des individus, des entreprises et voire des administrations publiques.

La maitrise du code est une donnée clé pour la constitution d'une cyber-arme. Il détermine le niveau technique qui est fonction de la cible. Cette compréhension du code détermine l'effet des cyber-armes et les contre-mesures efficaces. Cette technologie s'appuie sur une économie souterraine du cyber armement[19] dont le monopole ne doit pas être contrôlé par des organisations criminelles.
A cet effet, les sociétés de sécurité n'apparaissent plus comme des illustrateurs de menaces. Ils disposent désormais d'un rôle de détection et de contre-mesures face aux cyber-armes. Une société comme HTTPCS détecte en moyenne 3000 failles/jour dont 30% de failles critiques ou très critiques.
Qui plus ait, comme une partie des armements militaires s'appuient sur des technologies duales, ce type de société s'insère dans le marché des industries d'armements classiques. Ainsi, Kaspersky[20] a détecté que le logiciel Skygrabber a permis l'interception, en 2012, d'un drone américain dans l'espace aérien iranien. Les États disposent donc de deux solutions. La première consiste à faire appel à ce genre de société pour développer leurs propres programmes d'attaques et de défense. La seconde conduirait à encourager des sociétés d'intérêt public sur le modèle des sociétés de défense pour s'assurer d'une force de frappe dissuasive et réactive propre à la défense des intérêts vitaux des États.
A l'avantage d'armes pré-existantes et non centralisées dans un cœur numérique, les cyber-combattants forment des profils variés dans la conception et l'exécution de l'arme. Une équipe de ce genre concentre des spécialistes réseaux, systèmes, des développeurs, des veilleurs, des analystes et un coordinateur assurant la cohérence de l'ensemble.

Dans la mesure où le cyber a un effet égalisateur entre les structures mises en réseau, les modes d'action virtuels tendent à prendre la forme de ceux pratiqués dans le monde réel à travers trois modes : l'agression, la chasse. Ils se pratiquent dans les réseaux ou en appui d'une opération militaire classique.

Pour lutter contre la supériorité de l'imagination de l'attaquant sur l'attaqué, l'arme offensives ou défensives répond à un but qui traduit un effet à obtenir sur les réseaux ou que le réseau permet sur la situation réelle. Elle se manifeste par la réalisation possible de la portée de l'arme à partir d'une "TAZ" qui se dessine pour l'attaque.

18 Mise en ligne d'informations ou modification de sites web.
19 Le web clandestin à travers le réseau Tor.
20 Société russe du nom de son inventeur.

Elle est alors discrète ou brutale suivant le mode opératoire utilisé. Si l'attaque peut n'avoir aucun effet "pipe[21]" par rapport à la perception que l'individu a de la machine ou du système, sa déclinaison sur d'autres styles d'emploi se forgent par l'effet de surprise. Aussi, l'agression, la chasse, la défense active s'inscrivent dans cet effet. Si l'arme cybernétique est par nature précise elle peut être autonome du fait des interconnexions réseau et des liens entre les individus les utilisant.

Pour qu'une arme puisse s'exprimer sur le réseau et par le réseau, elle s'inscrit dans un effet final recherché. L'attaque inspire des formes différenciées de mouvements et de types d'armes. L'agression décline une arme à fort potentiel qui vise une destruction ou une paralysie délibérée du fonctionnement d'une organisation. Dans ce cas, l'arme est le produit des vulnérabilités métiers du système attaqué. Ce qui suppose une cartographie technique et humaine précise de la cible. Le ralentissement du programme nucléaire par la destruction logique du rythme coordonné de rotation des centrifugeuses iraniennes par le virus Flame est construit à partir d'un programme sur des processus industriels dont le vecteur demeure l'individu.

La chasse est une posture de recherche de cibles pour multiplier les effets d'une action principale. Le programme correspondant s'attachera à récupérer des données pour les croiser avec d'autres. Le résultat permet de bâtir une attaque plus large ou fournit des éléments pour des frappes aériennes, des actions terrestres ou navals.

A ces déclinaisons s'ajoutent les théâtres d'opérations sur lesquels s'expriment les effets des armes. Que ce soit par le réseau ou sur les réseaux, la cyber-arme profite d'une « TAZ [22]» pour générer son effet. Dans ce contexte, l'attaque a le choix du moment et le défenseur le choix du lieu de l'affrontement. Celui-ci demeure libre à condition de disposer d'une défense en profondeur et active ainsi qu'une ligne sur laquelle il entend fixer sa défense[23].

La cyber-arme est donc un programme qui se caractérise par la maîtrise technique et l'organisation humaine. Pour autant, son effet dépasse les limites physiques des réseaux.
Il touche également à la psychologie des individus. Ce qui soulève plusieurs problématiques dont la principale consiste à l'idée d'une prolifération du cyber-armement et du rôle futur des sociétés de sécurité. Le développement quantitatif et qualitatif du nombre de cyber-attaques posent la question de leurs militarisations. Cette tendance induit l'introduction de cyber-armes tactiques dans la conduite des opérations conventionnelles. De ce fait, le cyber se greffe à d'anciennes pratiques militaires en les rendant plus performantes et innovantes dans la conception, la conduite et l'exécution d'une opération[24]. Elle viendrait en appui des armes létales qu'une transformation du droit international en cours changerait en une arme de destruction reconnue et acceptée.

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18
La chaire remercie ses partenaires

21 Psychologique, information, physique, électronique.
22 Zone autonome temporaire
23 Honeypoot, firewall,architecture réseaux redondantes.
24 Une saturation de la bande passante des réseaux tactiques ennemis peut, par exemple, contre-carrer sa capacité de manœuvre. Voir le concept CAC du corps de Marines.