Études de l'Ifri

Focus stratégique 100

CYBERARMES

La lutte informatique offensive dans la manœuvre future

Jean-Baptiste FLORANT

Janvier 2021

Laboratoire de Recherche sur la Défense

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-0286-1

Comment citer cette publication :
Jean-Baptiste Florant, « Cyberarmes : la lutte informatique offensive dans la manœuvre future », *Focus stratégique*, n° 100, Ifri, janvier 2021.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Auteur

Le capitaine de frégate **Jean-Baptiste Florant** est chercheur au Laboratoire de Recherche sur la Défense (LRD) où il travaille sur le cyber et la guerre de l'information. Il est également doctorant au Centre de Recherche en Gestion (CRG-I3) de l'École Polytechnique, où il conduit des recherches sur la supériorité informationnelle et décisionnelle. Officier d'active de la Marine nationale, il est breveté d'état-major et diplômé en arabe de l'Institut national des langues et civilisations orientales (INALCO). Spécialisé dans le domaine du renseignement, il a été projeté en Europe orientale, en Afrique et au Moyen-Orient. Il a commandé une unité relevant du commandement de la Cyberdéfense de 2015 à 2019.

Comité de rédaction

Résumé

La lutte informatique offensive est un domaine relativement nouveau des opérations militaires. En raison de la numérisation croissante des sociétés et des forces armées, elle offre des capacités d'action inédites tant au niveau stratégique que sur le champ de bataille, contribuant ainsi à la supériorité opérationnelle des armées qui la maîtrisent. Sa mise en œuvre repose toutefois sur une architecture civilo-militaire complexe nécessitant un degré élevé de coordination entre les chaînes de production industrielle des armements, de renseignement, de commandement et de contrôle des opérations. Dans cette perspective, la manœuvre de demain devra prendre en compte les effets des cyberarmes, tout en intégrant leurs spécificités techniques et opérationnelles afin d'en tirer pleinement profit sur le champ de bataille.

Abstract

Offensive cyberspace operations are a relatively new realm of military operations. Due to the vulnerabilities of increasingly digitalized societies and armed forces, they allow unprecedented operational capabilities at both the strategic and battlefield levels. They therefore appear as a factor of operational superiority for the armed forces. Nevertheless, their implementation is based on a complex civilian-military architecture requiring a high level of coordination between the cyberweapons industrial production chain, the comprehensive intelligence process and the command and control chain. Hence, future military operations will have to consider the effects of cyberweapons, while integrating their technical and operational specificities for an optimal efficiency on the battlefield.

Sommaire

INTRODUCTION 9

L'ÉMERGENCE D'UN NOUVEAU DOMAINE DE LUTTE 13

Une numérisation massive de la société et des armées 13

L'avènement de la société digitale 13

La révolution numérique dans les armées 15

Des premières attaques à la cyberdéfense 17

Aux origines du hacking, une vieille pratique 17

Des opérations clandestines aux opérations militaires 18

Vecteurs et types d'attaque 21

DES OPÉRATIONS STRATÉGIQUES AU CHAMP DE BATAILLE 25

Trois cyber-opérations au XXIe siècle 25

Olympic Games : une opération stratégique très ciblée 25

Orchard : la LIO au service de la neutralisation des défenses aériennes 27

Glowing Symphony : une cyber-opération interalliée au niveau d'un théâtre entier 29

Quelles leçons en tirer pour la manœuvre ? 31

Les enjeux de l'hyperconnectivité 31

La convergence cyber-électronique 32

Le rôle central du renseignement 34

L'écrasement des niveaux opérationnels 35

Les cyberarmes, un levier stratégique 35

La LIO, un engagement persistent ? 36

FORGER LES CYBERARMES DE DEMAIN 39

Des contextes d'engagement diversifiés 39

Actions cyberoffensives contre un adversaire irrégulier 39

Emploi des cyberarmes en zone grise 40

La LIO dans un conflit de haute intensité 41

Comment intégrer les cyberarmes aux opérations militaires ? 43

Diffuser une culture de LIO dans les forces..... 43

Créer des cellules mixtes Cyber-GE-IO dans les états-majors interarmées de théâtre..... 44

Rapprocher la LIO de la guerre électronique et du renseignement d'intérêt cyber 45

Développer une doctrine de défense active 46

Maintenir le contrôle opérationnel au niveau stratégique 47

CONCLUSION 49

Introduction

En janvier 2020, Guillaume Poupard, actuel directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) prédisait que : « les conflits de demain vont être numériques, tous les grands États s'y préparent, à la fois en attaque et en défense[1] ». De fait, alors que jusqu'en 2019 la France se refusait à reconnaître publiquement des capacités offensives dans le domaine du cyber[2], elle s'est depuis dotée d'une doctrine officielle de lutte informatique offensive (LIO) pour encadrer « les actions entreprises dans le cyberespace produisant des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données[3] ». Cette doctrine est venue renforcer la posture, assumée depuis 2008, de lutte informatique défensive (LID) qui vise à « anticiper, détecter et réagir face aux risques, aux menaces et aux cyberattaques dont les systèmes d'information font l'objet[4] ».

Si les aspects défensifs de la lutte informatique ont fait l'objet de très nombreuses analyses, notamment en ce qui concerne la cybersécurité et la cyberdéfense, sa dimension offensive est moins souvent abordée. Pourtant, comme l'a signifié la ministre des Armées Florence Parly le 18 janvier 2019 : « la France emploie et emploiera l'arme cyber dans ses opérations militaires ». Il n'est toutefois pas aisé de définir ce qu'est une « cyberarme ». David Singer, journaliste au *New York Times* et spécialiste des questions de défense, la considère comme « l'arme parfaite[5] ». D'autres y voient l'apogée de l'art de la guerre imaginé par Sun Tzu, permettant de « vaincre sans combattre[6] ». Dans cette perspective, cette étude s'attachera à expliciter ce qu'est une cyberarme et ce qui la distingue des autres armes, afin de saisir les raisons pour

1. F. Schmitt et F. Dèbes, « 'Les conflits de demain vont être numériques, tous les grands États s'y préparent', dit le patron de l'ANSSI », *Les Échos*, 21 janvier 2020.
2. Toutefois, *Le Livre blanc sur la défense et la sécurité nationale* souligne dès 2008 la nécessité de développer une stratégie cyber de défense active comprenant des actions offensives. *Le Livre blanc sur la défense et la sécurité nationale*, Paris, Odile Jacob, 2008, p. 53.
3. « Doctrine militaire de lutte informatique offensive », Ministère des Armées, janvier 2019.
4. « Politique ministérielle de lutte informatique défensive », nr.101000, Ministère des Armées, décembre 2018.
5. D. E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the CyberAge*, New York, Crown, 2018.
6. « Être victorieux dans tous les combats n'est pas le fin du fin ; soumettre l'ennemi sans croiser le fer, voilà le fin du fin », dans J. Lévi (trad.), « Expéditions punitives », *in L'Art de la guerre,* Paris, Pluriel, 2015.

lesquelles les opérations cyberoffensives tendent à s'imposer dans les rapports de force.

Il est d'usage de représenter le « cyberespace[7] » en trois couches. La première est une couche physique, qui comprend les infrastructures, les équipements de traitement automatisé et les objets (câbles, serveurs, ordinateurs, etc.). Les données numériques et les moyens de les transmettre dans les réseaux (protocoles, applications, interfaces, etc.) constituent la deuxième couche, dite logique, du cyberespace. La troisième couche, inhérente à tout espace de communication, est la couche sémantique, qui englobe les utilisateurs, les échanges en temps réels, les réseaux sociaux et les contenus qui y circulent.

Bien qu'elles soient susceptibles de produire des effets dans toutes les strates, les cyberarmes se déploient principalement dans la couche intermédiaire du cyberespace. Ce sont des armes constituées de lignes de code informatique, silencieuses et insidieuses, qui pénètrent les réseaux de télécommunications et les systèmes d'information, en altèrent les données et la confidentialité, les effacent, les remplacent, les dérobent et en déroutent les flux.

Ces attaques invisibles ont pourtant des conséquences bien réelles. En témoignent des opérations majeures telles qu'*Olympic Games* menée contre le programme d'enrichissement d'uranium en Iran, ou, plus récemment, *Glowing Symphony* destinée à lutter contre les réseaux de Daech au Levant. Si ces opérations ont mis en lumière les possibilités d'usage de l'outil cyber, elles ont aussi mis en exergue les difficultés à l'associer aux autres composantes de la puissance militaire.

Pendant plus de deux décennies, les cyberattaques ont été cantonnées à des opérations clandestines, qu'elles aient été menées à des fins d'espionnage (renseignement), de sabotage (destruction ou altération de contenu) ou de subversion (propagande, désinformation, etc.). Leur intégration au sein des opérations proprement militaires est récente, puisqu'elle remonte à la création des commandements de cyberdéfense au tournant des années 2010. Il convient désormais de réfléchir à la manière d'intégrer les cyberarmes à leur juste place dans la manœuvre de demain.

7. Nous reprenons ici la définition du cyberespace donnée par les autorités françaises comme « l'espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées », cité dans *Journal officiel de la République française*, n° 0219 du 19 septembre 2017.

Alors que le cyber apparaît désormais comme un domaine de lutte incontournable (I), il convient de revenir sur la manière dont il a été investi, à la fois au niveau politico-stratégique et au niveau tactico-opératif (II). Une analyse prospective permettra enfin de faire émerger des recommandations sur la manière d'intégrer la lutte informatique offensive aux opérations militaires (III).

L’émergence d’un nouveau domaine de lutte

Il n’est pas possible d’envisager la lutte informatique offensive comme une capacité opérationnelle à part entière, permettant d’obtenir des effets militaires sur l’adversaire, sans analyser au préalable le cadre qui l’a vue naître et faite évoluer. Si la prise en compte de la menace cyber s’est d’abord imposée par le biais de la cybercriminalité, répandre un code malveillant à des fins d’escroquerie et lancer une cyberattaque contre des systèmes d’information, de commandement ou d’armes ennemis sont deux entreprises radicalement différentes d’un point de vue technique. Passer de l’un à l’autre requiert des avancées technologiques, organisationnelles et doctrinales considérables, qui sont pourtant souvent sous-estimées.

En effet, bien plus qu’un simple utilisateur, un groupe armé ou un État est capable de défendre ses systèmes pour réduire sa « surface d’attaque », c’est-à-dire son exposition à la menace. Il en découle une hausse du seuil de sophistication des attaques pour atteindre ce type de cibles. En parallèle, cependant, la dépendance au numérique des sociétés et des organisations comme des forces armées ne cesse de croître et s’accompagne logiquement d’une extension du risque cyber. Du point de vue des assaillants, cette évolution donc présente des opportunités offensives immenses.

Une numérisation massive de la société et des armées

L’avènement de la société digitale

De la naissance de l’informatique moderne à l’avènement d’Internet, la révolution numérique a transformé en profondeur non seulement la conception, la production et la consommation des biens et des services, mais également la manière de communiquer entre les individus et les groupes humains. Par « révolution numérique », on entend la rupture technologique qui a permis de transformer chaque information en une combinaison de données pouvant être stockées, traitées et transmises. Ce phénomène est né dans les années 1980 avec l’apparition de l’informatique personnelle, puis s’est développé grâce à l’accès généralisé

aux réseaux interconnectés à partir des années 1990, que l'on a appelé « Internet[8] ».

À l'échelle globale, la numérisation des sociétés humaines est un phénomène d'une ampleur et d'une rapidité sans précédent. Si l'usage du télégraphe puis du téléphone analogique a mis plus de deux siècles à s'imposer dans le monde occidental uniquement, la communication numérique a, quant à elle, conquis près des deux tiers de l'humanité en moins de cinquante ans. Dans les années 1990, la diffusion de l'informatique personnelle s'accompagne de celle d'Internet, généralement limité à 56 kilobits par seconde (kbit/s) et passant par les réseaux téléphoniques classiques. La téléphonie mobile dite « 2G » (pour deuxième génération ») se développe aussi, permettant de passer du signal analogique au signal numérique transmettant jusqu'à 40 kbit/s grâce à un réseau d'antennes relais idoines. Au début des années 2000, alors que l'ADSL démocratise les connexions filaires « haut débit » dans les entreprises et les foyers, la 3G multiplie au moins par quatre le débit de données accessibles depuis un téléphone mobile. Elle permet notamment l'accès au web, à la messagerie et même aux flux vidéo à partir de nouveaux terminaux, les *smartphones*. Les années 2010 sont celles de l'essor de la 4G, qui atteint des débits de l'ordre de 30 megabits par seconde (Mbit/s) en moyenne tandis que la fibre optique offre des accès jusqu'à 1 gigabit par seconde (Gbit/s) à une part grandissante de la population urbaine[9]. La décennie 2020 consacrera enfin la 5G qui autorisera des débits « mobiles » de 100 Mbit/s et permettra de prendre le contrôle à distance d'objets connectés grâce à des temps de latence extrêmement faibles, de l'ordre d'une milliseconde – contre 30 à 40 secondes pour la génération actuelle.

En 2020, près de 60 % de la population mondiale est connectée à Internet, soit 4,5 milliards de personnes parmi lesquelles 3,8 milliards disposent de comptes sur les réseaux sociaux, soit une augmentation de 9 % en un an (+ 325 millions). Le nombre d'objets connectés avoisine pour sa part les 50 milliards d'unités[10]. La moitié du temps passé sur le réseau Internet se fait désormais *via* des appareils mobiles dont disposent

8. Le premier message transmis au sein d'un réseau interconnecté de plusieurs ordinateurs, *via* le réseau téléphonique, a eu lieu en octobre 1969. Ce réseau était constitué des universités de Californie (UCLA), de l'institut de recherche de l'université de Stanford, des universités de l'Utah et de Santa Barbara (ARPAnet, pour Advanced Research Project Agency net).

9. M. Burhan *et al.*, « IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey », *Sensors*, vol. 19, n° 9, 2018.

10. Cité dans O. Becht et T. Gassilloud (rapporteurs), *Rapport sur les enjeux de la numérisation des armées*, Rapport n° 996, Paris, Commission de la Défense nationale et des forces armées, Assemblée nationale, mai 2018.

5,19 milliards d'individus[11]. Désormais, toutes les activités quotidiennes sont numérisées : les communications privées comme personnelles, les médias (qu'ils soient sociaux ou classiques), les communications, mais aussi une part grandissante des échanges financiers et commerciaux ainsi que des démarches administratives (factures, comptes bancaires, impôts, état civil). Ce phénomène s'inscrit dans un mouvement plus général de « dématérialisation », qui atteint également la documentation et les activités des États, des entreprises, et des individus. Bien que l'Estonie ait été pionnière en la matière, la France a suivi ce modèle avec le « Plan France numérique 2020 » élaboré dès 2011, qui prévoyait une disparition du papier dans la décennie suivante. L'Internet des objets constitue une étape supplémentaire en ce sens, puisqu'il « numérise » et connecte des activités liées au monde physique et donc non intégralement dématérialisables, qu'il s'agisse d'un réfrigérateur, d'une voiture, d'un thermostat, etc.

La machine, et avec elle ses capacités de calcul et de mémoire, est désormais un intermédiaire incontournable pour transmettre l'information sous forme de données numériques, sur des ordinateurs, des tablettes, des *smartphones* voire des objets connectés. En effet, cette tendance exponentielle à la numérisation ne s'arrêtera pas là. L'exploitation opérationnelle de la 5G et de l'Internet des objets devrait être possible d'ici deux à cinq ans. Elle concernera d'abord les infrastructures Télécoms des zones urbaines fortement peuplées et aux activités économiques denses, telles que les zones portuaires et aéroportuaires. Les *smart cities* et les *smart ports* devraient alors devenir emblématiques de l'hyper-connectivité urbaine. Ces innovations représentent toutefois un défi considérable dans le domaine de la cybersécurité, car l'avènement de la 5G s'accompagnera de la généralisation de l'Internet nomade, dont les architectures de sécurité sont à ce stade bien plus vulnérables.

La révolution numérique dans les armées

Les forces armées, et plus largement les institutions de défense et de sécurité nationale, n'ont évidemment pas échappé à la transformation numérique. Elles se sont très tôt engagées dans l'informatisation de leurs systèmes, puis dans la numérisation de leurs données. Comme le souligne Antoine Lefébure, « au départ, l'informatique sert à faire la guerre. Et d'abord à la gagner[12] ». Le premier calculateur électronique est en effet apparu dès 1947 aux États-Unis pour évaluer des trajectoires d'obus, après

11. E. Sojae, « Digital Report 2020 », *We Are Social*, 30 janvier 2020, disponible sur : https://wearesocial.com.
12. A. Lefébure, « Informatique communication et militaire », *Réseaux*, vol. 4, n° 17, 1986, p. 1.

avoir été développé à l'université de Pennsylvanie sur des crédits militaires[13].

Dans les 1970-1980, la révolution dans les affaires militaires (RMA) est amorcée par les États-Unis comme une stratégie capacitaire de compensation (*offset strategy*) de la supériorité quantitative soviétique par des capacités de frappes de précision dans toute la profondeur du champ de bataille. Celles-ci exigent alors une capacité de renseignement massif, en particulier un complexe reconnaissance-frappe informatisé lié à un centre de commandement et de contrôle adapté. C'est l'avènement du C4ISR, c'est-à-dire *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*, pour mettre en cohérence l'ensemble. Lancé dès 1969 par la *Defense Advanced Research Projects Agency* (DARPA), en partenariat avec l'université de Los Angeles (UCLA) et de Stanford, le réseau de systèmes d'information ARPAnet (futur Internet) est développé en parallèle pour faciliter la communication des données entre les nombreux ordinateurs du Département de la Défense.

Après la Guerre du Golfe, ce modèle de la RMA poussé par *l'Office of Net Assessment* du Pentagone, s'est imposé dans toutes les armées. Le concept de « *network centric warfare* » de la fin des années 1990 témoigne en outre de la prise en compte très rapide par les forces armées américaines du rôle central de la donnée et de l'importance de la capacité à la traiter et à la diffuser en réseau pour la manœuvre.

Côté français, les systèmes d'armes ont été dotés de composants électroniques et informatiques à partir des années 1980. Des projets tels que le programme nucléaire de défense *Simulation* (1996-2010), le programme *Rafale*, et l'expérience dès la fin des années 2000 de la numérisation de l'espace de bataille (NEB) pour l'armée de Terre, ont contribué à l'acculturation des forces aux technologies digitales. Aujourd'hui, le programme SCORPION (pour « synergie du contact renforcée par la polyvalence et l'info-valorisation ») va encore plus loin, puisqu'il doit permettre l'avènement du combat info-valorisé. Désormais, tous les équipements – qu'il s'agisse de véhicules blindés, de frégates ou d'avions – disposent d'une interface numérique et sont connectés entre eux ainsi qu'au poste de commandement. D'ailleurs, cette interconnexion continuera à prendre de l'ampleur avec la croissance du multi-domaine. Comme le rappelait l'amiral François Moreau, alors sous-chef d'état-major chargé des plans et des programmes de l'état-major de la Marine nationale, « la Marine opère des systèmes numérisés depuis trente ou quarante ans »,

13. *Ibid.*, p. 41.

bien que la numérisation ait subi une accélération récente avec la frégate multi-missions (FREMM) et la frégate de taille intermédiaire (FTI)[14].

Des premières attaques à la cyberdéfense

Qu'elle concerne la société dans son ensemble ou les armées en particulier, la révolution numérique s'est évidemment accompagnée d'effets négatifs. Chaque gain de productivité permis par l'informatisation est contrebalancé par des risques, voire des menaces. Les premières cyberattaques ont ainsi émergé presque en même temps que le cyberespace.

Aux origines du hacking, une vieille pratique

Le *hacking* consiste à pénétrer un système d'information ou un réseau, sans y être autorisé, dans le but de se renseigner, d'y dérober des données, de les falsifier, de les effacer, ou de saboter ce même système pour le neutraliser ou en prendre le contrôle. De fait, l'attaque d'un système d'information et de communication le détourne de son objectif de départ. Il s'agit plus précisément d'une altération du code initial visant *in fine* à modifier le message transmis et la possibilité d'une exploitation efficiente du système d'information. Le premier *hack*, ou ce qui peut être considéré comme tel, pourrait remonter à l'attaque du réseau télégraphique optique d'État (télégraphe Chappe) entre Paris et Bordeaux par deux escrocs, les frères Blanc, en 1834, qui en ont détourné le signal morse à leur profit, portant préjudice à l'intégrité des données transmises[15].

Avec l'avènement de l'informatique moderne, de nombreuses cyberattaques ont vu le jour. Les techniques de *hacking* ont d'abord inspiré des cybercriminels attirés par la perspective de gains toujours plus importants et une prise de risques relativement faible. Mais ces modes opératoires se sont progressivement étendus aux opérations clandestines puis militaires. Figure emblématique du *hacking* de la fin du XXe siècle, l'informaticien de génie Kévin Mitnick a défié pendant vingt ans les services de sécurité américains. S'il s'attaquait essentiellement à des sociétés d'informatique ou de télécommunication, il est également

14. Cité *in* O. Becht et T. Gassilloud, *Rapport sur les enjeux de la numérisation des armées, op. cit.* p. 12.
15. J.-M. Pottier, « L'Affaire des télégraphes, ou la première cyberattaque de l'Histoire », *Retronews*, 10 octobre 2018, disponible sur : www.retronews.fr. Cette histoire, connue sous le nom d'« Affaire des télégraphes » se déroule en France sous la monarchie de Juillet. Deux hommes d'affaires bordelais, les frères Louis-Joseph et François Blanc, cherchant à obtenir à des informations financières en provenance de la bourse de Paris avant la Bourse de Bordeaux, mettent en œuvre une attaque dite de l'« Homme du Milieu », qui consiste à intercepter le flux d'information entre un expéditeur et un destinataire, et éventuellement de corrompre ce contenu, sans que ni l'un ni l'autre ne s'en aperçoive.

soupçonné d'avoir tenté de pénétrer le système du Pentagone *via* le réseau ARPAnet au début des années 1980. Les systèmes d'information militaires et stratégiques étant des objectifs de choix, leur protection est rapidement devenue une priorité. Ainsi, au sein des armées, la cyberdéfense, qui n'en portait pas encore le nom, s'est, dans un premier temps, imposée par la lutte défensive.

Des opérations clandestines aux opérations militaires

Si la lutte informatique active s'est considérablement développée depuis les années 1990, elle a vu émerger son pendant proprement militaire au fur et à mesure que les armées et les services de renseignement ont décelé des vulnérabilités dans les systèmes informatiques d'adversaires, avérés ou potentiels, et ont compris que celles-ci permettaient de prendre un avantage opérationnel. En outre, les cyberattaques subies par les États dans les années 2000 ont donné lieu à la mise en place de stratégies plus offensives.

Parmi les opérations clandestines qui ont marqué l'Europe ces dernières années, on peut retenir la cyberattaque ayant visé Bics – une filiale de l'opérateur belge de télécommunications Belgacom – qui a défrayé la chronique après les révélations du lanceur d'alerte et ancien sous-traitant de la National Security Agency (NSA), Edward Snowden[16]. Selon le magazine allemand *Der Spiegel*, qui a eu accès aux documents mis en ligne par l'informaticien américain alors en cavale à Hong Kong, cette opération est imputable au Government Communications Headquarter (GCHQ), le service gouvernemental britannique en charge du renseignement électromagnétique et de la sécurité des systèmes d'information. Baptisée « *OP Socialist* », cette opération visant apparemment à pénétrer les institutions européennes s'est appuyée sur un *malware* très élaboré – *Regin* – qui se faisait passer pour un logiciel légitime de Microsoft[17]. À ce type d'opérations de niveau stratégique, menées avec un objectif clair de renseignement par des moyens clandestins, sont venues s'ajouter de nouvelles opérations aux objectifs purement militaires.

16. Cette cyberattaque de Belgacom est, d'après *Libération*, révélée par le quotidien belge néerlandophone *De Staandard* le 16 septembre 2013. Cf. A. Guiton, « Belgacom, ou les aléas du piratage entre amis », *Libération*, 2 novembre 2018.
17. R. Gallagher, « The Inside Story of How British Spies Hacked Belgium's Largest Telco », *The Intercept*, 13 décembre 2014.

L'intégration des cyberattaques au sein des opérations proprement militaires est concomitante à la création des commandements militaires de cyberdéfense. Aux États-Unis, le Cyber Command (CYBERCOM) a vu le jour en 2010, tandis que le Royaume-Uni ne s'est doté d'une National Cyber Force qu'en 2020. Cette entité mixte entre le ministère britannique de la Défense et le GCHQ est entièrement dédiée aux opérations cyberoffensives. En France, le commandement de la cyberdéfense (COMCYBER) a été créé en 2017 et placé sous l'autorité du chef d'état-major des armées (CEMA).

L'architecture française de LIO à des fins militaires repose sur un écosystème complexe dans lequel le COMCYBER s'appuie sur trois acteurs clés. D'une part, la division Maîtrise de l'information de la Direction générale de l'armement (DGA-MI) est en charge du développement des capacités, c'est-à-dire de l'ingénierie technique des cyberarme offensives[18]. D'autre part, pour planifier et conduire les opérations cyber qui sont du ressort des armées, le COMCYBER dispose, depuis le mois d'octobre 2015, d'un centre opérationnel de cyberdéfense (CO-Cyber) intégré au sein du centre de planification et de conduite des opérations (CPCO)[19]. Cet outil spécifique permet au CEMA de mener soit des opérations cyber en appui aux forces, soit des opérations autonomes.

Enfin, le troisième pilier est constitué par les services de renseignement qui apportent un appui essentiel et déterminant aux opérations en fournissant les éléments techniques et opérationnels nécessaires à la connaissance de l'environnement opérationnel, des vulnérabilités de l'adversaire, de son comportement et de ses intentions avant, pendant et après la manœuvre, comme c'est le cas dans toute opération militaire[20]. S'il s'agit d'une attaque proprement dite, par exemple d'un sabotage visant à la neutralisation d'un système, le renseignement précède, accompagne et exploite l'action de destruction. La manœuvre renseignement est donc centrale, en ce qu'elle conditionne la réussite de l'opération. En effet, l'efficacité de la LIO repose en grande partie sur une analyse très poussée de la cible et de son environnement technique et humain, afin d'en saisir les vulnérabilités et la manière de les exploiter pour obtenir l'effet recherché par l'opération. C'est ce que l'on nomme la

18. « Doctrine militaire de lutte informatique offensive », Ministère des Armées, janvier 2019, p. 11.
19. « La cyberdéfense au cœur des opérations », Ministère des Armées, 24 janvier 2018, disponible sur : www.defense.gouv.fr.
20. La Direction générale de la sécurité extérieure (DGSE) est bien entendu mobilisée tout comme la Direction du renseignement militaire (DRM), qu'il s'agisse de Renseignement d'origine cyber (ROC) ou de Renseignement d'intérêt cyber (RIC), à travers son Centre de recherche et d'analyse du cyberespace. Voir « Organisation », ministère des Armées, 24 novembre 2020, disponible sur : www.defense.gouv.fr.

« *Cyber Kill Chain* », qui suit un cycle s'apparentant, à peu de chose près, aux différentes étapes d'une action spéciale ou clandestine[21] :

1. **Reconnaissance** : évaluation initiale de la situation sur le terrain pour identifier les cibles, leurs vulnérabilités ainsi que la meilleure manière de les traiter (notamment en termes de rapport coût/efficacité des différentes options).

2. **Intrusion** : action hostile visant à pénétrer un système d'information ou de communication sans être détecté.

3. **Exploitation** : après une analyse approfondie des données recueillies, cette phase vise à tirer profit des vulnérabilités systémiques en installant des logiciels malveillants, ou *malwares* (virus, vers, chevaux de Troie, etc.), par le biais d'une faille de sécurité informatique détectée.

4. **Élévation des privilèges** : obtention de droits au sein du système afin d'y circuler plus librement et d'en prendre le contrôle. L'objectif de cette phase est le plus souvent de se substituer à la fonction d'administrateur du système.

5. **Commandement et Contrôle** : action permettant de se substituer à distance à l'administrateur d'une machine ou d'un système pour les soumettre et consolider la liaison avec l'attaque.

6. **Dissimulation** (ou obfuscation) : action visant à brouiller, atténuer voire effacer les traces de son passage pour induire en erreur les équipes adverses de LID, ou du moins retarder leur compréhension de l'attaque (utilisation de logiciels de type *rootkit*).

7. **Actions sur les objectifs** : cette phase peut prendre différentes formes en fonction de l'opération (neutralisation temporaire du système, sabotage, modification de données, etc.).

8. **Exfiltration** : faire sortir les données d'un système préalablement compromis (*leaks*), de manière plus ou moins discrète, puis les archiver dans un lieu sûr avant de les exploiter. Cette dernière phase est facultative et dépend de l'effet recherché.

D'après la typologie proposée par le chercheur allemand Thomas Rid dans son ouvrage *Cyber War Will Not Take Place*[22], les cyber-opérations clandestines relèvent soit de l'espionnage, soit du sabotage et de la subversion. Tandis que l'espionnage désigne la recherche de renseignement par des moyens clandestins, le sabotage consiste à détruire

21. Il s'agit d'une adaptation de l'auteur à partir du schéma de la *Cyber Kill Chain* de Lockheed Martin. Voir : *Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform,* Lockheed Martin Corporation, 2015, p. 6.
22. T. Rid, *Cyber War Will Not Take Place*, New York/London, Oxford University Press, 2013.

ou détériorer une installation, un matériel, ou un système afin de compromettre une action en préparation. La subversion implique quant à elle de saper les fondements de l'autorité en l'attaquant sur les valeurs pour la rendre illégitime. Or, ces modes opératoires peuvent très bien s'adapter au niveau du champ de bataille numérique.

Vecteurs et types d'attaque

L'intrusion et la question des vecteurs d'accès

L'intrusion est sans doute la phase la plus critique d'une cyber-opération. Si les moyens sont nombreux dans un monde civil où tous les utilisateurs sont connectés à Internet, il en va autrement dans le champ militaire, où les réseaux sont protégés par des passerelles, voire isolés physiquement (*air gap*) des autres réseaux. Les vecteurs d'attaque sont les moyens utilisés, ou plutôt détournés, pour mener une cyberattaque. Les failles de sécurité réseau – logicielle, humaine ou physique – sont exploitées pour porter l'attaque[23].

- **Vecteur physique**. Il s'agit d'un équipement externe (clé USB, souris, autres périphériques) qui, une fois connecté physiquement à la machine ciblée, injecte le code malveillant et la compromet, ainsi qu'éventuellement le réseau auquel elle est connectée. C'est par exemple le vecteur qui a été utilisé lors de l'opération *Olympic Games (cf. infra)*, pour pénétrer le système industriel contrôlant les centrifugeuses iraniennes du site de Natanz en 2010. Ce type de vecteur peut être employé pour des opérations très ciblées, nécessitant un montage minutieux et une prise de risque que seules les actions spéciales ou clandestines sont en mesure d'assurer.
- **Le vecteur réseau.** Ce type d'attaque exploite des failles dans la configuration réseau d'un système, en particulier celles des protocoles réseaux eux-mêmes (Ethernet, TCP/IP, UDP, FTP, SMTP, HTTP, etc.). Le réseau de communication est donc utilisé comme support de l'attaque proprement dite, mais aussi comme point d'entrée. Une attaque de type MITM (*Man In The Middle*), qui consiste à introduire un tiers dans la communication entre un émetteur et un récepteur à leur insu, utilise le vecteur réseau.
- **Le vecteur logiciel**. Ce vecteur utilise comme point d'entrée la vulnérabilité d'un logiciel déjà installé sur une machine. Il s'agit en général d'une attaque locale ciblant une machine spécifique.

23. R. Wakim, « Cybersécurité : cartographie des vecteurs d'attaque en milieu industriel », *Stormshield*, 12 août 2020, disponible sur : www.stormshield.com.

Néanmoins, si la machine est interconnectée, un mouvement latéral vers d'autres cibles est toujours possible. Une faille *zero-day* est par exemple est un vecteur d'attaque logicielle. Il s'agit de la vulnérabilité informatique d'un logiciel ou d'un système, qui n'est pas connue de son éditeur et qui n'est donc pas référencée, comme par exemple celle d'un système d'exploitation (Siemens, IBM, Windows, iOS, Android, etc.). Détecter cette faille donne un avantage comparatif évident à l'attaquant puisque le défenseur, en ignorant l'existence, ne peut s'y préparer.

- **Le vecteur humain**. Ce vecteur d'attaque, qui prend pour cible le maillon faible de la chaîne de sécurité qu'est l'être humain, implique de maîtriser les techniques de l'ingénierie sociale. Il s'agit d'outils de manipulation et de conditionnement, issus pour la plupart du monde du renseignement humain et des recherches récentes en sciences cognitivo-comportementales. Nécessitant un travail de ciblage préalable, puis d'environnement et d'approche souvent long, le vecteur humain permet de soutirer de l'information à une cible (technique dite d'« élicitation »), voire de la faire agir à son profit pour pénétrer l'objectif (manipulation). La méthode peut être douce lorsqu'elle s'applique à l'insu de la cible, ou avec son accord, ou plus forte lorsqu'elle est contrainte, par exemple par chantage.

  Le vecteur humain permet le plus souvent d'entrer en douceur dans une machine ou un système, sans éveiller de soupçon de la part de l'administrateur dudit système, car la connexion à ce dernier apparaît comme une connexion « légitime ». Ce type de vecteur, très répandu et efficace, est souvent sous-évalué par la défense adverse. À cet égard, la technique la plus employée est celle dite du *phishing* ou hameçonnage. Elle consiste à récupérer un maximum de données personnelles sur la cible humaine, le but ultime étant d'obtenir ses identifiants de connexion permettant d'usurper ultérieurement son identité. En règle générale, le *phishing* est mis en œuvre par le biais de mails frauduleux, simulant la plupart du temps une demande de connexion légitime nécessitant de s'identifier (nom d'utilisateur ou login) et de s'authentifier (mot de passe). Une fois ces éléments récupérés, l'attaquant peut accéder au compte de l'utilisateur et aux données auxquelles il a accès.

Ces différents types de vecteurs sont évidemment complémentaires. Ils doivent par ailleurs être aussi redondants que possible. Toutefois, plus le niveau de défense de la cible est élevé, plus il est nécessaire de les combiner de manière créative. Ces vecteurs portent les attaques proprement dites, c'est-à-dire les actions qui produisent les effets souhaités.

Typologie des attaques

Une fois l'accès sécurisé, l'assaillant peut se livrer à un large éventail d'actions malveillantes. Il convient de distinguer les différents types de cyberattaques. Ces derniers ne sont pas mutuellement exclusifs et les attaques complexes combinent la plupart du temps plusieurs de ces cyberarmes.

Les **attaques par déni de service** (*Denial of Service*, ou DoS), sont des attaques de « saturation ». Elles consistent à bloquer un serveur, un hébergeur ou une application Web (défiguration), en inondant son adresse IP de requêtes pendant plusieurs heures, voire plusieurs jours. Le système interrompt alors le service pour lequel il est programmé et se met en défaut. C'est un type d'attaques peu sophistiqué, qui n'est pas dissimulé et dont le but affiché est la déstabilisation de la cible par la neutralisation temporaire de son système connecté. Ce type d'attaque permet également à l'attaquant d'envoyer un message fort et simple à sa cible, en mettant en exergue sa vulnérabilité. Techniquement simple et par nature ouverte, l'attaque par déni de service est régulièrement employée par les hacktivistes. Ce type de cyberarmes figure notamment dans l'arsenal dédié aux opérations de lutte informationnelle dans le cyberespace (LIC) appuyées par la LIO. Une variante plus élaborée est l'attaque dite « distribuée » (*Distributed Denial of Service*, DDoS), menée à partir de plusieurs machines automatisées et mises en réseau (*botnet*) situées à des endroits différents, ce qui complexifie la remontée de l'attaque, sa caractérisation et son identification.

- **Les attaques par rebond**. Il s'agit là d'attaques masquées utilisant à leur insu des machines tierces dont les éléments d'identification sur les réseaux sont usurpés (*spoofing* de leur adresse IP par exemple), pour les faire agir à la place de l'attaquant ou les compromettre (DDoS, logiciels malveillants, etc.).
- **Les attaques par défiguration**. Ces attaques sont régulièrement employées par les hacktivistes pour faire passer un message politique ou manifester publiquement un désaccord. Elles consistent donc à attaquer le contenu (couche cognitive) et ses représentations (symbolique) et non plus le système uniquement.
- **Les attaques par implémentation de logiciels malveillants ou *malwares***. C'est une gamme de logiciels comportant la charge utile proprement dite de l'attaque, c'est-à-dire le code exécutable malveillant permettant d'atteindre l'effet majeur de l'opération. Il existe plusieurs catégories de *malwares*. On distingue en général le **virus** informatique qui s'infiltre dans un logiciel exécutable (y compris le système

d'exploitation lui-même) à partir desquels il se propage à d'autres programmes, des **vers** (*worm*) capables de se propager dans un système sans passer par des programmes hôtes. Enfin les **chevaux de Troie** (*Trojan*) sont des *malwares* se faisant passer pour un programme normal afin de persuader une cible de l'installer. Ils comportent souvent une fonction destructrice cachée, qui est activée au démarrage de l'application.

Virus, vers et chevaux de Troie peuvent ensuite recourir à tout un éventail d'utilitaires et de techniques pour assurer leurs méfaits. Ils peuvent par exemple introduire des **portes dérobées** (*backdoors*) permettant de contourner les procédures d'authentification normales, afin d'accéder à un programme à l'insu de l'utilisateur. Les ***rootkits*** désignent l'ensemble des logiciels malveillants qui permettent d'agir dans le système sans laisser de traces en modifiant le système d'exploitation de l'hôte, afin que le *malware* soit caché à l'utilisateur.

Enfin les *malwares* peuvent avoir des objectifs très variés. Dans le domaine de la cybercriminalité, les **rançongiciels** (*ransomware*) sont particulièrement répandus qui chiffrent tout ou partie des données d'une machine pour en interdire l'accès à l'utilisateur, conditionnant son « déblocage » au paiement d'une rançon. Souvent, l'écran affiche alors une fausse accusation de consultation de contenu illégal ou compromettant, pour faire peur aux cibles et les inciter à payer. Mais dans le domaine de la cyberdéfense, les *malwares* peuvent être employés à bien d'autres fonctions, comme le vol de données, le sabotage et la mise hors service de programmes, ou bien entendu leur prise de contrôle à distance.

Des opérations stratégiques au champ de bataille

Depuis quinze ans, les cyber-opérations tendent à prendre une part croissante dans les opérations militaires. Dans les années 2010, elles étaient encore exceptionnelles et généralement menées au niveau stratégique par des moyens exclusivement clandestins. Cependant, elles ont progressivement investi le champ de bataille, grâce à une organisation complexe des moyens militaires associés aux services de renseignement. Pour saisir cette évolution, il convient de revenir sur trois opérations qui ont jalonné cette décennie, afin d'en tirer des enseignements sur la place de la LIO et des cyberarmes dans la manœuvre de demain.

Trois cyber-opérations au XXIe siècle

Bien que disposant de moyens d'ampleur très différente, les États-Unis et Israël font partie des pays les plus avancés en matière de lutte informatique offensive. En effet, ils ont tous deux investi depuis longtemps dans les domaines de l'informatique militaire et du renseignement d'origine électromagnétique à l'échelle stratégique. Ils disposent par ailleurs d'un écosystème militaro-industriel dédié et très dynamique. C'est pourquoi leurs avantages comparatifs leur permettent de prétendre à la supériorité opérationnelle dans ce domaine contre leurs adversaires. Dans cette section seront donc étudiées trois opérations de niveau différent, dans lesquelles ces acteurs se sont illustrés, seuls ou en coalition.

Olympic Games : *une opération stratégique très ciblée*

Apparemment menée dans le cadre une coopération opérationnelle israélo-américaine, *Olympic Games* est une campagne d'opérations clandestines de cyber-sabotage qui a visé les installations nucléaires iraniennes du site de Natanz à la fin des années 2000[24]. Cette opération est plus connue sous le nom du célèbre *malware* utilisé par les attaquants : *Stuxnet*.

---

24. M. Kaminsky, « Operation 'Olympic Games'. Cyber-sabotage as a Tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Program », *Security & Defence Quartely*, vol. 29, n° 2, 2020 ; D. E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York, Crown, 2012.

À la fin des années 2000, l'avancée du programme nucléaire iranien inquiétait la communauté internationale, en raison du caractère potentiellement dual des installations et des mesures prises par Téhéran pour dissimuler certaines activités. La perspective du développement clandestin d'une arme nucléaire par les Iraniens faisait craindre un bouleversement de l'équilibre stratégique de la région et l'avènement d'une menace perçue comme existentielle par Israël.

L'usine d'enrichissement d'uranium de Natanz constituait alors l'un des principaux éléments du programme nucléaire iranien. Elle concentrait l'attention de la communauté internationale car l'enrichissement d'uranium pouvait autant indiquer un programme civil de production d'électricité que la production de matières fissiles de qualité militaire. L'usine de Natanz a donc vraisemblablement été identifiée comme une cible stratégique par l'échelon de planification américano-israélien. En effet, paralyser la capacité iranienne d'enrichissement d'uranium permettait de freiner le développement du programme nucléaire iranien, voire d'y donner un véritable coup d'arrêt. Dans le même temps, une telle opération réduisait le risque de voir Israël se lancer dans des opérations militaires contre les installations nucléaires de la République islamique.

L'objectif d'*Olympic Games* était d'attaquer le système informatique industriel contrôlant les centrifugeuses, dont la rotation à très haute vitesse permet la séparation des isotopes d'uranium. Pour ce faire, les assaillants ont exploité une faille de sécurité préalablement détectée dans le système de contrôle et d'acquisition de données (SCADA) de type Siemens Simatic WinCC. Le système n'étant de toute évidence pas connecté à Internet, une compromission humaine a été nécessaire pour introduire le *malware,* vraisemblablement par l'intermédiaire d'une clé USB. Présent dans le système, le virus « reniflait » d'abord le système d'exploitation, pour ne s'y attaquer que si celui-ci correspondait aux critères de cible, ce qui rendait sa détection extrêmement difficile. Une fois sa cible repérée, *Stuxnet* a reprogrammé le SCADA afin de saboter l'installation industrielle, en modifiant la vitesse de rotation des centrifugeuses jusqu'à ce que celles-ci soient hors d'usage. Parallèlement, il s'est attaqué aux systèmes numériques d'alerte, d'affichage et d'arrêt contrôlant les centrifugeuses, les rendant aveugles aux perturbations en cours.

Dans un ouvrage extrêmement documenté, David E. Sanger révèle la manière dont ce ver informatique, décrit comme « une cyberarme de destruction massive », aurait été élaboré puis utilisé par l'agence américaine de sécurité nationale (NSA) en collaboration avec l'armée israélienne (dont l'unité 8200 de Tsahal). En altérant la vitesse de rotation des centrifugeuses, *Stuxnet* a non seulement ralenti l'enrichissement

d'uranium, mais également occasionné la destruction de 10 % du parc. Cette opération de haute volée aurait en effet permis de détruire 1 000 centrifugeuses de type IR-1 et de retarder d'un an le programme nucléaire militaire iranien[25]. Bien que certains aient vu dans l'aptitude iranienne à se remettre rapidement de cette attaque la preuve de l'efficacité limitée du sabotage, il est clair que l'objectif d'*Olympic Games* dépassait le seul niveau technique. À travers cette coopération d'envergure dans le domaine cyber, Washington a pu réfréner Tel Aviv, qui voulait bombarder les installations nucléaires iraniennes.

Une telle opération, stratégique bien que clandestine, a ainsi permis de demeurer sous le seuil de l'agression caractérisée et d'éviter le recours à la force. En parallèle, l'attaque a permis de maintenir le régime iranien sous pression et de juguler son aptitude à poursuivre un programme nucléaire[26]. Dans cette perspective, l'objectif était vraisemblablement autant d'établir un rapport de force par une démonstration de puissance dans le cyberespace, que d'affecter l'activité opérationnelle des usines iraniennes. Comme le soulignait l'ancien directeur de la Central Intelligence Agency (CIA), Michael Hayden, *Stuxnet* « est la première attaque majeure de cette nature qui parvient à entraîner des destructions physiques affectant une infrastructure importante ». Et d'ajouter à l'époque : « Je ne veux pas dire que nous allons assister aux mêmes conséquences, mais, d'une certaine manière, nous sommes un petit peu en août 1945. »

Orchard : *la LIO au service de la neutralisation des défenses aériennes*

L'opération de l'armée de l'Air israélienne contre le site nucléaire syrien d'Al-Kibar de septembre 2007, connue sous le nom d'opération *Orchard*, a été officiellement reconnue par les autorités israéliennes en 2018[27]. Si la cinématique aérienne de l'opération a fait l'objet de nombreuses analyses, peu d'informations ont circulé sur la neutralisation préalable des défenses aériennes syriennes (SEAD[28]) par les unités de guerre électronique et de LIO israéliennes.

25. D. E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, op. cit.*
26. F. Kaplan, *Dark Territory: The Secret History of Cyber War*, New York, Simon & Schuster, 2016.
27. P. Smolar, « Israël revendique la destruction d'un réacteur nucléaire en Syrie en 2007 », *Le Monde,* 21 mars 2018.
28. SEAD : *Suppression of Enemy Air Defences*.

Le 6 septembre, juste après minuit, quatre chasseurs *F-15* israéliens survolaient un réacteur nucléaire en construction dans la région de Deir Ez-Zor à l'est de la Syrie et le démolissaient grâce à des bombes et des missiles à guidage laser. Quelques mois avant l'attaque, l'armée syrienne s'était pourtant dotée de nouvelles batteries de défense aérienne russes, sur lesquelles les entraînements avaient été satisfaisants. Les militaires en service cette nuit-là ont d'ailleurs déclaré n'avoir vu aucun avion sur leurs écrans radar.

De fait, peu avant le raid aérien, les émetteurs radars de la région avaient été repérés et intoxiqués grâce à un flux de fausses données permettant de masquer les traces des chasseurs[29]. L'unité 8200, le bureau israélien de guerre cybernétique, avait en effet piraté le système radar de défense aérienne syrien, grâce à un programme informatique appelé *Suter*, développé par un bureau clandestin de l'armée de l'Air américaine.

Plusieurs hypothèses ont été proposées pour expliquer la manière dont ce code malveillant a été injecté. La première suggère qu'il a été transmis par une source humaine, par exemple par le biais d'une clé USB comme pour l'opération *Olympic Games*. Une deuxième indique que le *malware* a été injecté par des forces spéciales qui se sont branchées sur le système d'information. Enfin, si l'on en croit la troisième hypothèse, le code a été transmis par signal aéroporté (radar, radio, ou autre), retranscrit ensuite dans le système d'information du système de défense aérienne intégrée (SDAI)[30]. Quelle que soit la modalité de l'intrusion, c'est ce code malveillant qui a permis de neutraliser SDAI lors de l'attaque – non pas en désactivant le radar, mais en perturbant la liaison de données le reliant aux écrans des opérateurs. Dans le même temps, il a piraté le signal vidéo des écrans, afin que l'équipe de l'unité 8200 puisse voir ce que les opérateurs radar voyaient, tandis que les écrans des opérateurs étaient vides.

Pour comprendre cette attaque surprise, il faut remonter près d'un an en arrière. En effet, fin 2006, les services spéciaux israéliens ont introduit un « cheval de Troie » dans l'ordinateur portable d'un représentant du gouvernement syrien, alors qu'il séjournait dans un hôtel du quartier de Kensington à Londre[31]. Le disque dur de ce fonctionnaire imprudent contenait des plans des installations d'Al-Kibar ainsi que des informations compromettantes sur la coopération de Pyongyang avec Damas dans le transfert de technologies nucléaires. Les preuves étaient suffisantes pour

29. C. Bwele, « Le raid cyber d'Israël en Syrie », *Électrosphère,* 21 décembre 2007, disponible sur : https://electrosphere.blogspot.com.
28. F. Kaplan, *Dark Territory*, *op. cit.*
31. V. E. Follath et H. Stark, « How Israel Destroyed Syria's Al Kibar Nuclear Reactor », *Der Spiegel,* 2 novembre 2009.

décider Tel Aviv à mener une opération de destruction, permettant de surcroît d'envoyer un message fort à Damas, et par ricochet à Téhéran et Pyongyang.

Glowing Symphony : *une cyber-opération interalliée au niveau d'un théâtre entier*

Décidée au niveau du Strategic Command (STRATCOM) de l'armée américaine, l'opération *Glowing Symphony* a été mise en œuvre par le Cyber Command (CYBERCOM) au profit de la Joint Task Force Ares (JTF-ARES) avec l'aide de la National Security Agency (NSA) pour contrer l'action numérique menée par l'État islamique (EI) depuis ses bases en Syrie et en Irak[32]. Comme pour *Orchard*, la JTF-ARES appuyait directement les opérations cinétiques, en fournissant du renseignement et des options opérationnelles aux commandants sur le terrain. Contrairement au cas précédent, il s'agissait de lutter contre un adversaire irrégulier, dans le cadre d'une campagne de longue durée. Au sein de cette force, le CYBERCOM avait quant à lui pour mission de contester à l'EI sa liberté de manœuvre dans l'espace informationnel.

Déclenchée le 10 novembre 2016, cette opération visait en particulier à perturber le système de propagande de l'EI sur Internet et les réseaux sociaux, au moyen de cyberattaques contre les systèmes informatiques de ses centres médiatiques[33]. Dans un premier temps, les assaillants ont cherché à environner les cibles, afin d'accéder aux systèmes utilisés par les djihadistes. *Glowing Symphony* a donc débuté par la compromission du système d'information et du réseau des djihadistes grâce à une campagne d'hameçonnage (*phishing*), qui a permis de cartographier leur environnement informatique. À partir de cette cartographie, des *patterns* ont été identifiés (manière de nommer leurs comptes sur les réseaux, horaires de fréquentation des sites, plateformes privilégiées, etc.). L'étude minutieuse des traces numériques laissées par les combattants de l'EI sur les réseaux et de leurs comportements numériques a ainsi permis de déceler leurs vulnérabilités. Les fautes de sécurité qu'ils commettaient en ligne ont ensuite permis aux services américains d'accéder aux structures d'intérêt. De fausses informations ont alors été introduites dans cet écosystème pour en compromettre les activités. Ces dysfonctionnements ont perturbé les activités en ligne des combattants, en particulier la

32. Le premier commandant de la JTF-ARES est le général Paul M. Nakasone, en 2016. Il est nommé, en 2018, directeur de la NSA et commandant de l'US CYBERCOM. Voir J.-B. Florant, « Fort Meade sort ses muscles », *Ultima Ratio*, 31 janvier 2020, disponible sur : http://ultimaratio-blog.org.
33. À l'époque, l'EI disposait de deux centres médiatiques : al-Furqan visant un public arabophone et al-Hayat à destination d'une audience plutôt occidentale ne maîtrisant pas la langue arabe.

propagande, le recrutement, la communication et les levées de fonds. Finalement, la totalité des serveurs adverses a été détruite.

Cette opération a semé la confusion parmi les djihadistes, amoindri leur efficacité opérationnelle et perturbé leurs activités en ligne. Elle a associé des moyens de lutte informatique offensive et de cyber-influence pour déstabiliser au maximum l'EI. L'intégration et la synchronisation des capacités cyber ont ainsi été utilisées pour produire des effets informationnels utiles sur le plan opérationnel, afin de réaliser des objectifs militaires.

Le travail préparatoire a été mené par la NSA, qui dispose à la fois des moyens et des savoir-faire techniques de pénétration, ainsi que de la connaissance des cibles et de leur environnement. Son rôle a donc prépondérant, bien que l'articulation avec le CYBERCOM ait été délicate. En effet, la déconfliction opérationnelle[34] et l'évaluation des mesures d'efficacité de l'opération ont représenté des défis de coopération d'ampleur[35].

L'un des principaux points d'achoppement entre les responsables militaires de l'opération et leurs homologues des services de renseignement a porté sur la confidentialité des structures d'attaque, des techniques et des moyens clandestins mis en œuvre. En effet, si l'action militaire peut être discrète, elle n'a pas vocation à demeurer secrète, et peut même être révélée pour les besoins de la mission. Contrairement à une action secrète et encore plus clandestine, elle doit toujours être assumable car elle engage la responsabilité des États qui la conduisent. C'est là toute la difficulté posée par la conduite d'opérations cyber mixtes, menées avec l'appui d'un service de renseignement pour concevoir et mettre en œuvre une infrastructure clandestine d'attaque (fournisseur), sous la houlette du commandement militaire de l'opération elle-même (client bénéficiaire). Alors que le premier cherche avant tout à préserver le secret, le second privilégie l'efficacité.

Le manque de coopération durant l'opération *Glowing Symphony* aurait ainsi créé des frictions entre les agences de renseignement américaines (la CIA, la NSA, voire le Federal Bureau of Investigation – FBI) et le CYBERCOM. La dimension interalliée a également ajouté une complexité supplémentaire, les informations étant partagées au sein de la coalition anti-Daech qui comptait alors une soixantaine de pays. Lors de

34. La déconfliction opérationnelle consiste en un dialogue entre parties alliées sur le champ de bataille afin notamment d'éviter les tirs fratricides.
35. M. Martelle, « US CYBERRCOM After Action Assessments of Operation Glowing Symphony », *National Security Archive*, 21 janvier 2020, disponible sur : https://nsarchive.gwu.edu.

cette opération, des renseignements transmis à des membres de la coalition ou à des alliés peu rigoureux sont aussi vraisemblablement tombés aux mains d'ennemis des États-Unis. C'est pourquoi les services de renseignement, qui craignent avant tout la compromission, préfèrent généralement mener des opérations qu'ils maîtrisent de bout en bout, afin d'en assurer une sécurité maximale.

Quelles leçons en tirer pour la manœuvre ?

Les enjeux de l'hyperconnectivité

Quel que soit le type d'opération, l'appui de la LIO nécessite un temps de préparation important, tant la neutralisation d'un système de commandement et de contrôle ou de combat ne s'improvise pas. En amont, il est indispensable de recueillir les caractéristiques techniques de ces systèmes, et des informations sur la manière dont ils sont utilisés (techniques, tactiques et procédures), afin d'en connaître les failles techniques ou d'emploi. Pour certaines opérations, les services de renseignement acquièrent même des copies des systèmes, comme l'a fait la NSA pour préparer l'opération *Olympic Games*, en achetant d'anciennes centrifugeuses – les mêmes que celles utilisées par les Iraniens[36].

Si le seul recours à des armes logiques peut sembler un facteur de réduction du risque, il n'est suffisant que lorsque la cible est peu protégée et que ses systèmes sont reliés à Internet. Moins les systèmes sont interconnectés, plus les capacités cybernétiques doivent être complétées par d'autres moyens. Aussi, l'étape de l'intrusion du système peut-elle nécessiter une action humaine préalable (compromission), qui augmente d'autant la difficulté – et donc le risque d'échec – de l'opération. Concrètement, il s'agit soit d'introduire un agent au sein de la structure cible, soit d'en recruter un déjà inséré, pour injecter un *malware* au sein d'un système fermé auquel il a accès[37]. Dans les deux cas, cela implique une opération clandestine souvent longue, difficile, coûteuse et risquée, qui ne peut être conduite que par un service spécial[38]. Cette séquence est en soi

35. D. E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, *op. cit.*, p. 197-198.

37. En matière de renseignement clandestin, l'accès à la structure-cible, c'est-à-dire l'entité physique ou virtuelle dans laquelle se trouve le renseignement, est une étape essentielle du processus de recherche.

38. Un service *spécial* est un service gouvernemental en charge de mener des actions clandestines. Voir F. Beau, « Culture du renseignement et théories de la connaissance », *Revue Internationale d'Intelligence économique*, vol. 2, janvier 2010, p. 167.

une « opération dans l'opération », qui peut prendre des semaines, des mois, voire des années.

En outre, étant donné la généralisation des systèmes d'information et de commandement d'une part, et de la télétransmission de données numérisées sur le champ de bataille d'autre part, les armées sont désormais vulnérables à la pénétration. De surcroît, la vulnérabilité peut être indirecte, comme l'a montré l'attaque contre un système de défense aérienne intégrée menée à partir d'une cyberattaque sur le réseau téléphonique auquel il était connecté au Kosovo en 1999[39]. La supériorité informationnelle requiert par conséquent une défense active de ces systèmes (Hypervision[40], entraînement des équipes, technologies, etc.).

Par ailleurs, le développement des véhicules autonomes, des drones et des robots, y compris militaires, repose en grande partie sur ces technologies de communication. Un objet connecté étant un dispositif qui communique en permanence, sa transmission de données constitue, par définition, une voie d'accès électromagnétique à son système d'information. Ces objets, qui serviront essentiellement de capteurs tactiques dans la manœuvre infovalorisée de demain, s'apprêtent donc à étendre la surface d'attaque des systèmes et des réseaux auxquels ils appartiennent, et donneront lieu à de nouvelles vulnérabilités aux actions offensives. De fait, cette généralisation des liaisons de données nomades et aéroportées accélère la convergence entre le monde cyber et celui de la guerre électronique.

La convergence cyber-électronique

La guerre électronique et la guerre dans le cyberespace sont intimement liées parce qu'elles mènent toutes les deux des opérations sur ou à partir d'un signal. Elles sont donc particulièrement complémentaires sur le théâtre de la manœuvre.

La guerre électronique permet d'ouvrir des brèches dans le spectre électromagnétique du champ de bataille, quand la LIO s'y engouffre pour pénétrer les systèmes adverses et les neutraliser. Par exemple, lorsque la

38. B. S. Lambeth, *The Transformation of American Air Power*, Ithaca/New York, Cornell University Press, 2020, p. 199-200.

40. Hypervision : « L'hypervision est la capacité de disposer d'une vision actualisée et globale du système d'information pour faciliter la détection et la réponse à des incidents. L'hypervision est différente de la supervision en ce qu'elle procède à l'agrégation, au croisement et à la corrélation de nombreuses données techniques et métiers. En matière de cyberdéfense militaire, l'hypervision vise à donner aux opérationnels une vision large de l'état de fonctionnement de leurs systèmes ». CEIS, « L'hypervision au service de la Cyberdéfense », *Observatoire du monde cybernétique*, 3 janvier 2019, disponible sur : https://omc.ceis.eu.

donnée est transmise par un signal électromagnétique (comme la 5G ou le wi-fi), la guerre électronique s'attaque au contenant (l'onde) et les capacités cyber au contenu (la donnée). C'est de cette complémentarité et surtout des synergies entre les différents domaines de lutte que dépend *in fine* l'efficacité des opérations cybernétiques de demain. Penser en termes de « prérogatives périmétriques » est, en ce domaine, un combat d'arrière-garde. Seule une stratégie exploitant la capacité à produire des effets convergents sera profitable[41].

À cet égard, l'opération israélienne *Orchard* montre que l'avenir des opérations de LIO sur les théâtres d'opérations devrait passer par leur rapprochement avec les capacités de guerre électronique des trois armées. En effet, la guerre électronique permet, localement et sous certaines conditions, un accès plus facile aux systèmes d'information de systèmes d'armes adverses peu connectés avec l'extérieur voire protégés par des « *air gaps* ». Tous les systèmes adverses n'étant pas numérisés, agir avec des moyens de guerre électronique permet une marge de sécurité, dans des cas où les cyber-capacités sont insuffisantes, temporaires, ou qu'elles ont été découvertes.

Enfin, la combinaison de la guerre électronique et des opérations cyberoffensives permet d'accroître les capacités de déception et même d'intoxication d'une force sur le champ de bataille. La pénétration des systèmes adverses ouvre la voie à l'altération des données de l'ennemi, en particulier celles relatives à la localisation et au volume des forces amies déployées sur le terrain. Induire l'ennemi en erreur pour lui faire prendre des décisions favorables est alors beaucoup plus aisé, comme l'a illustré l'opération *Orchard*.

Ainsi, certaines opérations permettent de leurrer un adversaire sur les données contenues dans ses propres systèmes[42]. Ce mode d'action n'est pas très éloigné de celui utilisé par les frères Blanc. Prenons le cas par exemple des données de l'AIS (*Automatic Identification System*) qui permet de connaître l'identité, le positionnement et le statut d'un navire ainsi que d'autres caractéristiques techniques comme sa vitesse et la route qu'il suit. Il est possible aujourd'hui de corrompre ces données, tout comme il est

41. *Effect-Based Operations* ou EBO : opérations centrées sur les effets. Concept militaire américain développé lors de la planification de la campagne aérienne de la guerre du Golfe (1990-1991) par David A. Deptula, alors lieutenant-colonel de l'US Air Force.
42. *Spoofing* : techniques d'usurpation d'identifiants utilisées dans le domaine Telecom/Cyber. Sens élargi : technique de manipulation.

possible de tromper le système de géolocalisation et de navigation par un système de satellites (GNSS) de type GPS[43].

Le rôle central du renseignement

L'exploitation du renseignement lors de l'opération *Glowing Symphony* a été rendue difficile par le flux de données qui a submergé la TF-ARES, et auquel elle ne s'attendait pas[44]. C'est pourquoi une architecture de stockage des données doit être pensée dès la phase de préparation des opérations de pénétration et adaptée au fur et à mesure des reconnaissances effectuées dans les systèmes-cibles. « Ne pas hésiter à voir grand », même lorsque l'adversaire est un groupe non étatique n'utilisant *a priori* que des systèmes d'information « grand public », est à ce titre une des leçons à tirer de cette opération. Le rôle central du renseignement dans les opérations cyberoffensives a d'ailleurs fait dire en septembre 2016 au général Len Anderson, alors commandant adjoint de la Joint Task Force Ares, que « près de 90 % de ce que nous faisons [en matière de cyber] s'apparente au renseignement[45] ».

Bien entendu, la manœuvre n'est pas juste consommatrice de renseignement. Elle en produit aussi en grande quantité, y compris lorsque les autres capteurs sont inopérants sur le théâtre. Par exemple, si l'environnement est trop contesté pour une manœuvre de capteurs physiques, les moyens cyberoffensifs peuvent renseigner le commandement, et même produire des effets sur le terrain (sabotage, intoxication, déstabilisation, déception, etc.). Dans les opérations de ciblage, les cyberarmes jouent également un rôle clé pour la neutralisation d'individus ou d'objectifs spécifiques grâce au traitement de métadonnées personnelles par exemple, dans le but d'identifier des profils ou des « *patterns* ».

Enfin, les opérations de LIO peuvent fournir du renseignement « actionnable » d'opportunité aux autres domaines de lutte, voire à des services extérieurs au ministère des Armées. Ce peut être par exemple le cas de renseignements récupérés de manière fortuite au sujet de transactions financières en cryptomonnaies alimentant le terrorisme. En France, dans les armées, la transmission de ce type de renseignement aux services compétents, comme la DGSI ou Tracfin, sera du ressort de la DRM.

43. GNSS désigne également un système associant plusieurs systèmes à couverture mondiale comme les systèmes GPS (américain), Glonass (russe) et Galileo (européen).
44. C. Cimpanu, « L'armée américaine n'était pas prête à gérer la quantité de données récupérée chez Daesh », *ZDNET*, 23 janvier 2020, disponible sur : www.zdnet.fr.
45. M. Pomerleau, « How Cyber Command Can Limit the Reach of ISIS », *FifthDomain*, 17 septembre 2019, disponible sur : www.fifthdomain.com.

L'écrasement des niveaux opérationnels

Les opérations de LIO montrent la difficulté à distinguer les niveaux stratégique, opératif et tactique dans le cyberespace. En effet, ces trois échelons y sont imbriqués, parfois de façon inextricable.

D'abord, rappelons que le cyberespace, contrairement aux autres milieux de lutte, est un milieu entièrement artificiel, ne pouvant exister sans machines, serveurs, réseaux interconnectés, câbles, ondes et énergie. Il est caractérisé par un écheveau de frontières juridiques – en fonction du droit s'appliquant à une plateforme, du lieu où se trouve la donnée, etc. Cette complexité donne lieu à des échanges de données peu contrôlés, au cours desquels des acteurs de tous niveaux interagissent. L'attaque du système d'arme peut rapidement dépasser le niveau du champ de bataille ou du théâtre des opérations, pour affecter le niveau stratégique d'un conflit. Réussir à compromettre un tel système laisse non seulement planer le doute sur la compromission probable de l'ensemble d'une flotte de combat, d'un parc d'aéronefs ou de blindés, mais affecte aussi directement les intérêts de l'État visé.

Bien qu'une action cyberoffensive puisse se limiter au seul niveau tactique lorsque ses effets ne dépassent pas le champ de bataille, il est difficile de garantir que des codes malveillants conçus pour des systèmes fermés ne sont pas diffusés sur Internet. Ainsi, l'opération *Olympic Games* a été révélée en juin 2010 par la société biélorusse d'antivirus VirusBlokAda, lorsque ses experts ont découvert l'existence de *Stuxnet* sur Internet, alors même qu'il visait initialement un système fermé. La maîtrise des effets demeure donc une question centrale, afin que les actions conduites dans le cyberespace reflètent bien l'intention politique. C'est un enjeu d'autant plus critique qu'il existe des risques de contamination collatérale des systèmes civils.

Les cyberarmes, un levier stratégique

Les cyberarmes ont pour caractéristique d'être invisibles – ou à tout le moins difficilement détectables. En revanche, elles sont aisément réplicables une fois que leur code source est identifié. Elles revêtent un caractère insidieux que l'on retrouve par exemple dans le combat de sape mené par le génie pour attaquer une fortification par les dessous. Il s'agit d'une arme de la surprise et de la ruse, qui donne un avantage tactique

certain sur l'adversaire puisqu'elle « permet d'obtenir la supériorité en un point décisif[46] ».

Le risque d'une cyberattaque suscite chez l'ennemi une incertitude quant à l'intégrité de ses systèmes d'information et de commandement, qui sont le système nerveux des états-majors modernes. La menace cyber oblige donc à investir du temps et des moyens dans leur protection et leur défense[47]. La peur d'être attaqué à l'intérieur peut alors inhiber la décision et, partant, paralyser l'action.

Les cyberarmes sont donc particulièrement redoutées, car elles peuvent frapper n'importe où, n'importe quand, et sans préavis. En ce sens, la LIO est en mesure de décourager une action hostile et peut appuyer une stratégie élargie de la dissuasion[48]. Au contraire des armes nucléaires cependant, la crédibilité de la menace cyber ne peut être aisément démontrée à l'adversaire par des gesticulations stratégiques, et la vulnérabilité de ce dernier n'est ni acceptée, ni démontrable avant une attaque. Par ailleurs, pour être activées au moment opportun, les cyberarmes doivent sommeiller dans des systèmes adverses qu'elles auront préalablement pénétrés. Aussi, l'usage de cyberarmes repose-t-il sur des actions préemptives, déjà hostiles en elles-mêmes.

La LIO, un engagement persistent ?

Il est rare et extrêmement complexe de faire tomber un système d'information adverse au moyen d'une attaque logique. Une telle opération nécessite un investissement humain et financier important, ainsi que des compétences techniques élevées. En revanche, il est plus aisé de mener des attaques moins ambitieuses sur des cibles de moindre importance et plus faciles d'accès. En multipliant ce type d'attaques sur des cibles secondaires situées sur les arrières de l'ennemi, comme les systèmes informatiques de la chaîne logistique de maintenance des matériels ou d'approvisionnement en vivres et en munitions, le fonctionnement d'une force déployée peut être très perturbé et le moral des troupes sérieusement ébranlé. À défaut d'atteindre la chaîne de soutien, l'attaque peut également se porter sur l'équipement personnel des soldats, en général très peu protégé : ordinateurs personnels, tablettes, *smartphones*, montres connectées, etc.

46. R. Hémez, « L'avenir de la surprise tactique à l'heure de la numérisation », *Focus stratégique,* n° 69, Ifri, juillet 2016, p. 13.
47. Par exemple, le ministère français des Armées consacre 1,6 milliard d'euros de son budget à la cyberdéfense de 2019 à 2025 selon la loi de programmation militaire.
48. B. Barbier, E. Guillaud et J.-L. Gergorin, « Cybercoercition : un nouveau défi stratégique », *Le Monde,* 28 janvier 2020.

Cette stratégie d'usure menée grâce à un harcèlement systématique de l'ennemi, à la manière du moucheron face au lion dans la célèbre fable de La Fontaine[49], est d'autant plus efficace qu'elle joue sur l'effet de surprise. Elle correspond aussi à ce que le général Paul Nakasone, commandant de l'US Cyber Command, appelait en 2019 le « *persistent engagement* » pour qualifier la guerre larvée et permanente à laquelle se livrent les États dans le cyberespace. Entretenir ainsi l'insécurité dans les usages numériques quotidiens d'une force lui donne le sentiment d'être assiégée par un ennemi qui semble partout et apte à frapper en tout temps. Il est alors possible de prendre l'ascendant psychologique sur une force en faisant la démonstration régulière de son exposition et en combinant cette manœuvre à des actions d'influence ciblées. Il n'est pas systématiquement nécessaire d'attaquer un adversaire sur des ressources stratégiques très bien protégées – et donc hors de portée – si de plus petites attaques permettent *in fine* de contribuer à saper le moral de ses troupes.

En cela, la LIO est un domaine de lutte dont les modes d'action s'apparentent à ceux des opérations spéciales, dédiées à l'attaque des arrières de l'adversaire. Ces opérations devraient d'ailleurs bénéficier d'un appui particulier dans ce domaine tant elles en partagent le caractère innovant, souple et agile, et tant elles sont proches des actions clandestines.

49. J. de La Fontaine, « Le lion et le moucheron », *Fables*, Livre II, Fable 9, Paris, Folio Gallimard, 2015.

Forger les cyberarmes de demain

La numérisation sans précédent du champ de bataille et l'intégration progressive des cyberarmes dans la manœuvre des armées modernes laissent entrevoir les formes que pourrait prendre la LIO dans les opérations militaires de demain. En effet, alors que de nouvelles possibilités techniques et tactiques apparaissent pour prendre l'avantage sur l'adversaire, des aménagements d'ordre organisationnel et doctrinal pourraient aussi permettre de tirer davantage profit du potentiel des cyberarmes dans la manœuvre future.

Des contextes d'engagement diversifiés

Tantôt capacité d'appui, tantôt capacité de neutralisation, la lutte informatique offensive offre, en fonction des contextes opérationnels, de nouvelles possibilités pour prendre l'ascendant sur l'adversaire. Il convient de passer en revue certaines d'entre elles, sans pour autant prétendre à l'exhaustivité.

Actions cyberoffensives contre un adversaire irrégulier

La LIO continuera très probablement à être employée sur les moyens de transmission d'acteurs non étatiques peu durcis ne disposant pas de véritables systèmes d'information et de commandement. C'est le cas par exemple de la lutte contre des groupes armés terroristes camouflés derrière des activités et des populations civiles. Ce paramètre occasionne des pressions sociétale et internationale plus importantes, et restreint l'usage d'armes aux effets disproportionnés. Dans ce contexte, les marges de manœuvre étant assez étroites sur le plan opérationnel, les opérations cyberoffensives apparaissent comme un recours aux avantages tactiques indéniables. En effet, les actions de LIO favorisent l'accès au renseignement, elles sont furtives, discrètes, difficilement attribuables, créent des pressions psychologique et technologique, et sont exploitables dans le champ informationnel à des fins d'influence. Les cyberarmes constituent alors une ligne d'opération supplémentaire renforçant l'efficacité des actions cinétiques. Elles peuvent s'avérer très utiles pour

cibler des lignes d'opérations adverses difficiles d'accès dans le champ matériel (propagande, messageries, levée de fonds, etc.)

Dans ce type de conflit de basse intensité, qui exige un investissement élevé dans le renseignement tactique et son exploitation opérationnelle dans des temps très courts, les cyberarmes peuvent être un facteur important de supériorité opérationnelle. De fait, les opérations de LIO sont particulièrement opportunes au regard du renseignement lorsque l'ennemi fuit le contact. La lutte informatique offensive peut donc être utilisée de manière complémentaire aux autres capteurs, afin par exemple de réduire les risques encourus par les acteurs du renseignement humain, ou parce qu'il est parfois impossible de faire manœuvrer des plateformes aériennes de type ATL-2, C-160 *Gabriel*, E-2/3, ou des drones.

Emploi des cyberarmes en zone grise

Derrière son apparente transparence, le cyberespace peut se révéler extrêmement opaque, et les acteurs qui y agissent se présenter sous de fausses identités (ainsi de l'attaque informatique contre TV5 Monde, en avril 2015, initialement attribuée à un « Cyber Califat » de Daech avant que l'enquête ne pointe du doigt un groupe de *hackers* lié aux services russes). Inversement, la lutte informatique offensive peut être employée à des fins de renseignement, voire de neutralisation, sur des acteurs non étatiques soutenus par des puissances régionales. Un tel emploi est toutefois susceptible de donner lieu à un conflit plus complexe, tant les acteurs impliqués sont nombreux[50]. Les conflits ethno-territoriaux, qui sont animés par des visées séparatistes et utilisent le terrorisme comme un mode d'action violent de harcèlement politique, en sont un exemple. Or, s'ils sont instrumentalisés par des États proches s'appuyant sur des organisations criminelles pour créer l'insécurité, ces conflits peuvent se prêter à l'utilisation de cyberarmes.

L'un des principaux avantages de la LIO est qu'elle permet de disposer de davantage de renseignements tactiques, tout en exerçant une pression sur les parties prenantes au conflit. En cela, les armées modernes bénéficient d'un avantage comparatif évident, du fait la maîtrise des technologies cyber. L'intrusion dans les systèmes de communication et de commandement adverses à des fins de renseignement, l'altération des données en vue d'opérations de déception voire d'intoxication sont en effet rendues possibles par les cyber-capacités. Les objets connectés des chefs de milices, tels que leurs *smartphones*, leurs tablettes et leurs montres

50. M. Goya, « De la stratégie face à la complexité des choses », *La voie de l'épée*, 20 septembre 2019, disponible sur : https://lavoiedelepee.blogspot.com.

peuvent ainsi être piégés. L'accès à leurs données personnelles ainsi qu'à celles de leur environnement proche permet alors de renseigner en temps réel les forces amies. Sur la base de certains de ces éléments, des opérations ultérieures de *naming and shaming* peuvent être orchestrées.

Néanmoins, des États faibles ou des groupes criminels sont aussi susceptibles de recourir à des cyber-mercenaires, c'est-à-dire des prestataires privés offrant une gamme de services dans le domaine cyber allant du renseignement au sabotage des systèmes en passant par des attaques subversives. En 2018, pour faire face à ces défis, Emmanuel Macron a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Dans cette déclaration, il a plaidé en faveur de l'élaboration de principes communs de sécurisation du cyberespace et décrit le cyber-mercenariat comme une « nouvelle menace ».

La LIO dans un conflit de haute intensité

La neutralisation massive par des cyberarmes de matériels de guerre et des systèmes d'information et de commandement ennemis est certainement le scénario le moins probable à échéance de dix ans, en raison de la difficulté à pénétrer des réseaux militaires durcis et préparés à la menace par des moyens de LID[51]. C'est pour cette raison que les cyberarmes devraient demeurer des armes d'opportunité.

En revanche, il sera sans doute plus aisé de cibler les chaînes logistiques et de soutien sur les lignes arrière de l'ennemi, souvent plus vulnérables aux attaques de LIO. Ces opérations s'apparenteraient à des opérations spéciales cyber, voire à des opérations clandestines de lutte informatique active (LIA). L'avènement de la 5G et la généralisation de l'Internet des objets dans le soutien permettront à ceux qui en maîtrisent les protocoles d'en percer les systèmes et d'attaquer des points de plus en plus inattendus de la chaîne de valeur.

Les armées les plus avancées en ce qui concerne les attaques contre les réseaux réussiront sans doute à pénétrer certains *clouds*[52] tactiques, qui s'apprêtent à être développés par les armées modernes. En effet, le volume de données numériques provenant du champ de bataille ne cesse de

51. Notons toutefois que certains systèmes d'armes anciens, comme le chasseur *F-15*, sont vulnérables et que leur pénétration ne nécessite pas d'investissements démesurés. J. Marks et T. Riley, « The Cybersecurity 202: Hackers Just Found Serious Vulnerabilities in a U.S. Military Fighter Jet », *The Washington Post*, 19 août 2019.

52. Il s'agit d'infrastructures et de services distants pouvant être externalisés. Le *cloud computing* permet ainsi de stocker d'importantes quantités de données (*big data*) dans des entrepôts (*data centers*) et de les traiter avec des outils animés par des intelligences artificielles (*machine learning* par exemple).

croître. Dans le même temps, il est désormais nécessaire de stocker ces données dans des entrepôts sécurisés et distants, où l'intelligence artificielle est utilisée pour les traiter. Or, on peut présager que, demain, ces services seront sous-traités dans des espaces souverains. Ces *clouds*, bien que durcis, seront des cibles à très forte valeur ajoutée, dans la mesure où ils concentreront l'information utile. Mis en œuvre par des prestataires extérieurs, ils feront l'objet d'une attention très forte de la part des attaquants. La cyberattaque dont a été victime la société Lockheed Martin en 2007 témoigne des enjeux découlant du processus d'industrialisation. En effet, le programme du chasseur de 5e génération *F-35 Lightning II* a vraisemblablement été piraté par des *hackers* chinois, alors qu'il n'en était au stade que de la conception[53]. Cet exemple démontre combien la stratégie d'attaque d'un système d'arme intervient au long cours. Dans une stratégie d'attaque profonde, le système de combat ou de commandement est ainsi appréhendé dans l'ensemble de son écosystème, et dès sa genèse.

Enfin, la robotisation et l'avènement des systèmes d'armes létaux autonomes (SALA) mus par des intelligences artificielles promettent de transformer la guerre dans la décennie à venir. Ils bouleverseront les rapports de force sur le terrain par des effets de saturation du champ de bataille et de vélocité dans la manœuvre. Néanmoins, la faiblesse de ces systèmes résidera en grande partie dans leurs vulnérabilités aux cyberattaques. Leur cuirasse informatique fera l'objet d'assauts répétés, eux-mêmes menés par des systèmes autonomes exploitant des failles logicielles ou réseaux. Aussi les attaquants se doteront-ils certainement d'outils d'intrusion *ad hoc*. Les forces devront cependant s'assurer de la supériorité informationnelle avant de déployer des cyberarmes. Or, il n'y a pas de supériorité informationnelle sans maîtrise préalable du champ électromagnétique, c'est-à-dire sans guerre électronique.

Il est en outre envisageable que des essaims de drones intelligents (*swarming*), terrestres, aériens ou navales, soient la cible de cyberarmes s'attaquant à leur système de C2. En effet, tandis que le brouillage offensif permet la neutralisation d'un système d'armes, les cyberarmes permettent d'en prendre le contrôle en vue, par exemple, de les retourner contre leurs détenteurs. L'association de ces deux composantes ouvre alors la voie à de nouvelles perspectives tactiques.

Dans quelques années, les systèmes lourds de défense électroniques, comme les radars, les systèmes de brouillage électromagnétique, les systèmes de suivi de la force amie (*Blue Force Tracking*) et d'identification

53. F.-S. Gad, « New Snowden Documents Reveal Chinese Behind F-35 Hack », *The Diplomat*, 27 juin 2015.

ami-ennemi (*Identification Friend or Foe*), seront probablement eux aussi la cible d'attaques automatisées, visant à en prendre le contrôle afin de leurrer l'adversaire sur le champ de bataille.

Enfin, le domaine spatial demeurera un théâtre de compétition entre les grandes puissances. Il s'agira, de plus en plus, d'acquérir la supériorité militaire dans les domaines des télécommunications et du renseignement géospatial (GEOINT). Ce dernier s'imposera bientôt comme un domaine d'affrontement, comme l'a montré en 2018 l'attaque par le satellite russe Luch-Olymp du satellite franco-italien Athena-Fidus, spécialisé dans les communications militaires sécurisées[54]. Dans ce contexte, on peut raisonnablement s'attendre à ce que les communications satellitaires, ainsi que les satellites eux-mêmes, soient la cible de cyberattaques. Là encore, la lutte informatique offensive aidera à répondre à ce type de menaces.

Comment intégrer les cyberarmes aux opérations militaires ?

S'il ne fait aucun doute que les cyberarmes tiendront une place centrale dans la conflictualité future, la façon de les intégrer au sein de la manœuvre militaire pose question. Relevant jusqu'à présent du niveau stratégique – voire de la décision politique – la lutte informatique offensive cherche encore sa place au sein des états-majors opérationnels. Plusieurs pistes doivent être envisagées.

Diffuser une culture de LIO dans les forces

La LIO est une sphère très spécialisée, qui nécessite des connaissances techniques pointues. L'art de manœuvrer dans le cyberespace et la compréhension des chaînes de commandement sont encore loin d'être maîtrisés dans les forces. Par ailleurs, les acteurs évoluant dans cet écosystème particulier, tels que les services de renseignement, les entreprises de cybersécurité, et les départements de recherche et développement des industries de défense, sont méconnus. C'est par conséquent un domaine de lutte inédit, encore mal compris dans les états-majors opérationnels, où il est souvent envisagé comme hermétique.

Aussi conviendrait-il de sensibiliser les futurs officiers d'états-majors destinés à servir en opération à la lutte informatique offensive. C'est en prenant conscience des effets qu'ils peuvent en attendre dans le cadre d'une manœuvre multi-domaines qu'ils pourront véritablement en tirer

54. « La France accuse la Russie de tentative d'espionnage par satellite », *Le Monde*, 7 septembre 2018.

profit. Il faut également apprendre aux jeunes officiers à transmettre davantage d'éléments techniques et de contexte recueillis dans le cadre de leurs fonctions, parce que les opérations dans le cyberespace, à l'instar de celles conduites dans d'autres domaines de lutte, sont en grande partie dépendantes des manœuvres réalisées dans les autres milieux. En effet, le cyberespace n'échappe pas à l'interdépendance des milieux.

De surcroît, une formation commune aux opérations militaires dans le cyberespace serait éminemment profitable aux officiers et aux sous-officiers cyber. Les domaines de lutte du cyberespace sont si interdépendants qu'un socle de connaissances partagées permettrait de mieux les articuler. Tandis que les acteurs de la LID disposent d'une connaissance approfondie des cyberarmes et des modes opératoires ennemis, ceux de la LIO aident à appréhender les vulnérabilités adverses et les moyens de les exploiter. La LIC favorise quant à elle une compréhension fine de l'environnement informationnel et des mécanismes socio-numériques qui le structurent.

Créer des cellules mixtes Cyber-GE-IO dans les états-majors interarmées de théâtre

Cyber, guerre électronique et opérations d'information (IO) sont de plus en plus imbriqués dans le cadre d'une stratégie militaire d'influence. La création de cellules mixtes dans les états-majors de théâtre – soit au niveau du commandement tactico-opératif – présenterait trois intérêts majeurs. D'abord, elles permettraient à la LIO de se coordonner avec les autres domaines de lutte. Elles favoriseraient également la détection des opportunités opérationnelles, afin d'en donner une première évaluation en vue de leur exploitation. Elles contrôleraient enfin la mise en œuvre des moyens déployés sur le terrain.

Ces cellules pourront avoir à leur tête un officier de liaison, assisté de quatre officiers chargés chacun d'un domaine de lutte : l'un pour la lutte informatique défensive, un autre pour la lutte informatique offensive, un troisième pour la cyber-influence[55] et un dernier pour la guerre électronique offensive et défensive. Intégrées au sein des états-majors de forces, ces cellules devraient disposer d'un lien direct avec l'échelon de commandement de la force, en raison de la sensibilité de la LIO et de

54. Domaine de lutte qui définit le rôle des forces armées, leurs moyens et leur manière d'appréhender la guerre de l'information à l'ère numérique. Une doctrine de lutte informationnelle dans le cyberespace est en cours d'élaboration au sein de l'état-major des Armées et devrait prochainement paraître.

l'implication d'acteurs tiers. Le niveau de l'officier général commandant adjoint des opérations semble à cet égard adéquat.

À titre d'exemple, les forces armées américaines prennent le chemin d'une intégration des capacités de cyber, de guerre électronique, de renseignement et d'opérations d'information (*Information Operations* ou IO) au sein d'entités opérationnelles dédiées[56]. Il en est ainsi de l'US Navy qui prévoit de déployer des cellules de guerre de l'information au sein de ses centres des opérations maritimes et dans ses états-majors embarqués à partir de 2022[57]. L'US Air Force, le corps des Marines et l'US Army se réorganisent également dans ce sens même si la composition de ces entités diffère[58].

Rapprocher la LIO de la guerre électronique et du renseignement d'intérêt cyber

Les capacités de guerre électronique des armées de Terre, de l'Air et de l'Espace et de la Marine permettront d'ouvrir des brèches dans le spectre électromagnétique des forces ennemies sur les théâtres d'opérations. Par le biais d'intrusions localisées, elles permettront d'introduire des cyberarmes dans les réseaux et les systèmes d'information ennemis.

Pour être couronnée de succès, la LIO nécessite un soutien extrêmement marqué de la fonction de renseignement d'intérêt cyber (RIC). Cet appui en renseignement doit précéder l'opération en amont, l'accompagner dans son exécution et lui succéder pour qu'elle soit exploitée ultérieurement.

L'intégration de ces trois compétences au sein de mêmes plateaux opérationnels, situées au CPCO pour le niveau stratégique et dans les états-majors de théâtre pour le niveau opératif, devrait favoriser une concentration des effets et une accélération des processus décisionnels.

Enfin, pour renforcer les capacités cyberoffensives depuis la terre, la mer, l'air ou l'espace, il est primordial d'investir dans les moyens tactiques d'intrusion des systèmes et réseaux informatiques à partir du champ électromagnétique[59]. Cet investissement doit s'accompagner d'un

56. M. Pomerleau, « How the Defense Department Is Reorganizing for Information Warfare », *C4isrnet.com*, 26 juillet 2020, disponible sur : www.c4isrnet.com.
57. *Ibid.*
58. *Ibid.*
59. Dans le cas de systèmes informatiques tactiques coupés du réseau Internet, il est possible de les pénétrer notamment à partir des ondes électromagnétiques. La guerre électronique devient alors un vecteur adapté aux cyberattaques.

développement des techniques, tactiques et procédures nécessaires à l'intrusion, et d'un entraînement régulier avec les unités de LIO.

Développer une doctrine de défense active

Si la France entend disposer d'une capacité de contre-attaque efficace et ajustée, elle doit travailler à une meilleure articulation entre luttes informatiques défensive et offensive. En effet les acteurs de la LID, par le biais du CALID, de l'ANSSI et des services de renseignement, sont extrêmement au fait des cyberarmes et des modes d'action utilisés par l'adversaire[60]. Concevoir une doctrine de contre-attaque cyber, faisant mieux interagir la LID et la LIO, permettrait alors de mieux circonscrire ce domaine de lutte.

Dans le domaine offensif, si les opérations cyber à fins de renseignement et les attaques de neutralisation ont déjà fait l'objet de nombreuses analyses, les opérations visant à contrer les tentatives d'influence semblent d'emblée moins évidentes. Pourtant, les opérations de déstabilisation sont en plein développement et leur coût politique et social va croissant[61]. Les opérations dites de « mise au pilori » (*naming and shaming)* ou d'atteinte à la réputation, rendues possibles grâce à des pénétrations permettant la fuite de données (*leaks*), sont aujourd'hui un instrument de coercition efficace. En témoigne la révélation par les autorités britanniques de la responsabilité du GRU, le service de renseignement militaire russe, dans la cyberattaque contre la Convention nationale démocrate lors des élections présidentielles américaines en 2016[62].

Dans certaines conditions, ce mode d'action permet en effet de déstabiliser des organisations, voire des États – à condition que le rapport de force dans le cyberespace et dans le champ politique soit favorable. En révélant publiquement les actions malveillantes d'un adversaire qui agit sous le seuil de l'agression, le *naming and shaming* contribue à le mettre au ban de communauté internationale. C'est le cas, par exemple, lorsqu'une cyberattaque est « attribuée », c'est-à-dire officiellement « imputée à un attaquant identifié en y apportant des éléments de preuve[63] ».

60. L'ANSSI détient une connaissance approfondie et renouvelée des cyberattaques touchant les Organismes d'Intérêt Vitaux (OIV) pour l'État.
61. M. J. Mazarr *et al.*, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*, Santa Monica, California, RAND Corporation, 2019.
62. A. Guiton, « L'attribution des cyberattaques, un bras de fer diplomatique », *Libération*, 5 octobre 2018.
63. Ministère des Armées, « Lettre mensuelle n° 63 », *Observatoire du monde cybernétique*, juin 2017, p. 7.

Toutefois, cette stratégie représente deux risques. Elle équivaut d'une part à révéler à l'adversaire que l'on a pénétré ses systèmes et risque donc de compromettre les modes d'action utilisés contre lui. D'autre part, l'accusé est susceptible de nier son implication, comme le font très souvent les adversaires irréguliers peu sensibles à l'opprobre de la communauté internationale, ou les États misant sur une stratégie de cyber-espionnage profond, tels que la Chine ou la Russie[64].

Dans cette perspective, l'interdépendance des trois couches physique, logique et cognitive du cyberespace requiert une approche globale de la menace et une réponse à la fois défensive, contre-offensive et informationnelle coordonnée et cohérente.

Maintenir le contrôle opérationnel au niveau stratégique

Bien que l'emploi de cyberarmes puisse être tactique, c'est-à-dire réalisé au profit de la manœuvre, les opérations de LIO sont toujours décidées, coordonnées et contrôlées au niveau stratégique[65].

En effet, la lutte informatique offensive doit être préparée sur le temps long et requiert un degré élevé de dissimulation. Elle mobilise des acteurs nombreux et divers, et peut provoquer des effets collatéraux sur le cours des opérations difficilement maîtrisables. Ces facteurs font peser un risque politico-diplomatique important sur ceux qui initient la LIO et plaident en faveur de son rattachement au niveau stratégique.

C'est l'une des leçons qui peut être retenue de l'opération *Glowing Symphony*. De fait, l'organisation de la chaîne cyber américaine facilite d'autant plus la coordination stratégique que la NSA et le CYBERCOM, bien qu'institutionnellement distincts, sont commandés par le même décideur. Les modèles russes et chinois, également très centralisés en ce qui concerne la décision d'engager les cyberarmes, sont aussi intéressants à cet égard, puisque leur mise en œuvre peut en revanche être décentralisée. En conséquence, la décision d'emploi et le contrôle de la LIO relèvent du niveau stratégique, tandis que son exécution et les effets attendus peuvent être délégués aux niveaux opératif ou tactique. En cela, le positionnement des commandements de cyberdéfense de ces trois pays peut être comparé à celui des opérations spéciales.

64. A. Segal, « Shaming Chinese Hackers Won't Work Because Cyber-espionage Is Here to Stay », *The Guardian*, 30 mai 2013.

65. CIVIS, « À propos d'une classification des armements », *Politique étrangère,* vol. 27, n° 3, 1962. Une arme peut jouer un rôle stratégique ou tactique, en fonction de son emploi et des effets attendus sur le champ de bataille (tactique) ou portant sur les mouvements, les arrières de l'ennemi ou la conduite des opérations (stratégique).

Ces dernières relèvent par principe du niveau stratégique. Sensibles et discrètes, elles sont menées la plupart du temps en coordination interarmées, voire interministérielle, et font souvent intervenir de multiples domaines de lutte. Les opérations spéciales se distinguent également par une prise de risque élevée et l'utilisation d'armes et de modes d'action émergents. Le même type de cadre d'exécution que celui dans lequel elles interviennent semble alors tout à fait adéquat pour intégrer au mieux la LIO dans la manœuvre sur le terrain. Autrement dit, sur les théâtres d'opérations, le contrôle tactique des opérations de LIO pourrait être confié aux opérations spéciales. En cas de nécessité, il serait possible de recourir à des experts projetés sur le terrain provenant d'unités conventionnelles spécialisées[66].

En revanche, l'intégration de capacités de LIO au niveau tactique ne pourrait se faire que ponctuellement, tant diffèrent les tempos des manœuvres cinétique et cybernétique. L'effort de synchronisation serait tel qu'il est difficile d'imaginer la délégation systématique des actions de LIO au niveau d'un théâtre.

66. Pour la France, il pourrait s'agir, par exemple, d'unités telles que la 785e Compagnie de guerre électronique, du 54e Régiment de Transmissions (armée de Terre) ou l'Escadron électronique aéroporté 00.054 « Dunkerque » (armée de l'Air et de l'Espace).

Conclusion

L'intégration de la lutte informatique offensive et des cyberarmes dans la manœuvre militaire est un défi à la fois technologique, organisationnel et doctrinal. En effet, le cyberespace ouvre un nouveau champ de bataille avec ses propres logiques de fonctionnement, parfois en décalage avec une vision plus conventionnelle de la guerre. Rapide, furtive, entretenant volontiers le flou sur l'origine des attaques pour mieux se fondre dans les « zones grises », la LIO est une arme de supériorité opérationnelle au potentiel disruptif majeur.

Dans le même temps, la manœuvre de demain sera résolument multi-domaines, c'est-à-dire qu'elle combinera un ensemble d'effets provenant de capacités aussi bien létales que non létales, cinétiques ou non cinétiques, et ce dans les champs matériels ou immatériels. Dans le cadre d'un ciblage dit à large spectre, la LIO sera donc un fournisseur d'effets. Elle permettra, par ses actions concourantes, d'atteindre l'état final recherché – au même titre que d'autres domaines de lutte tels que la guerre électronique.

En ce qui concerne les actions spécialisées, la LIO concourra à des opérations plus indépendantes, ne s'inscrivant pas nécessairement dans le cadre spatio-temporel des opérations classiques, tant la pénétration d'un système adverse s'organise sur le temps long. Seule une action planifiée dans la durée et au niveau stratégique permet de mener des attaques d'envergure.

Cependant, pour être mise en œuvre de manière optimale, la lutte informatique offensive requiert la construction d'un écosystème à la fois complexe et agile, qui devra être caractérisé par une coopération civilo-militaire robuste, des boucles de recherche-production-utilisation rapides et rétroactives, ainsi qu'une intégration de bout en bout des services de renseignement dans le processus opérationnel. C'est à cette seule condition que les cyberarmes pourront être pleinement intégrées dans les opérations militaires de demain. Dans cette perspective, bien qu'elle ne soit pas vouée à changer la nature de la guerre, la lutte informatique offensive pourra, en revanche, influer sur son modèle d'organisation.

Institut français
des relations
internationales