Comment vraiment paralyser un pays à l'aide du cyber

Éric Filiol

Dirige le laboratoire (C+V)° de l'ESIEA, dédié à la vision offensive de la sécurité. Il dirige également la revue de recherche *Journal in Computer Virology and Hacking Techniques* (publiée par Springer). Il intervient dans la plupart des conférences internationales de *hacking* (*Black Hat*, *CCC*, *CanSecWest*).

Note de l'auteur : Une version longue de cet article est disponible (en anglais) : « *The operational reality of "cyberwar" and "cyber attacks" – How to really paralyze a country with the cyber* » (www.securiteoff.com/reality-of-cyberwar-how-to-paralyze-the-usa-really/).

Les illusions de la cyberguerre

Depuis une dizaine d'années, les armées du monde entier et leurs États, sous l'impulsion des États-Unis, se sont lancées dans une réflexion intense autour de l'évolution du concept de guerre et plus précisément sur la cyberguerre. Selon cette conception, les conflits seraient avant tout numériques, constitués essentiellement d'offensives menées *via* des codes malveillants, les cyberarmes, ou des attaques informatiques exploitant des vulnérabilités non corrigées (*exploit 0-days*). Ces « cyberarmes » sont présentées comme l'innovation la plus significative et la plus dangereuse de ce siècle : pour cela sont cités des codes comme *Stuxnet*, *Aurora*, *Duqu*, *Regin*, *Babar* ou *GrayFish* (voir encadré en fin d'article). Il ne se passe pas un jour sans qu'un officiel ou un expert ne vante les capacités destructrices sans précédents de ces armes et n'agite le spectre d'une apocalypse globale. Cela sert de prétexte et souvent de caution pour défendre l'idée qu'il faudrait désormais consacrer des milliards à cette nouvelle forme de guerre et, *in fine*, orienter les doctrines, l'industrie militaire, la nature même de nos sociétés et de notre vision philosophique pour ne pas dire morale de la guerre, en accord avec cette nouvelle vision.

En réalité, cette vision confine à une hystérie collective développée et soutenue par différents milieux et communautés (en particulier académiques) qui voient dans cette orientation des opportunités et des intérêts (*cf.* Thomas Rid). Elle est non seulement partisane, illusoire et fausse mais également dangereuse car elle oblitère des pans entiers d'insécurité face auxquels nos sociétés vont devenir de plus

(1) École supérieure d'informatique, électronique, automatique.

en plus désarmées et donc particulièrement fragiles. La vision actuelle de la cyberguerre est une hérésie entretenue dans des buts partisans par des esprits aveugles.

Énumérons les principaux dangers liés à cette vision :

• La dimension numérique [2] des conflits modernes n'est pas LA mais UNE dimension supplémentaire dans l'art de la guerre. L'objectif de cette dernière reste une action finale sur la sphère matérielle dans le but d'une captation de ressources ou de biens. Nous sommes dans la même situation qu'avec l'introduction de l'aviation au début du XX^{e} siècle, laquelle n'a jamais remis en cause les forces terrestres et maritimes.

• Les conflits actuels (Ukraine, Irak, Syrie, Mali…) ou la multiplication des attentats démontrent la prééminence du conventionnel sur le cyber, lequel n'intervient, quand cela est le cas, que de manière très réduite. Les cyberattaques vont en revanche prendre leur importance dans le cadre de ce que nous pouvons considérer comme le nouveau visage de la guerre : « les attaques de temps de paix », que vont se livrer certains États, essentiellement les pays du G-20, constituant de fait une situation de tension permanente dans les sociétés dites modernes.

• Si le risque lié au monde numérique existe réellement, il n'a pas l'universalité nécessaire pour des attaques de grande ampleur. Frapper avec succès un parc informatique ou des systèmes de *SCADA* [3] suppose que les éventuelles faiblesses exploitables affectent simultanément et au moment opportun de la manœuvre un nombre suffisant de machines. Or, la variabilité informatique (même au sein d'un parc supposé homogène) est suffisamment importante en général pour limiter fortement ce type d'approche. Alors que *Stuxnet* est souvent cité en exemple et que les codes analysés indiquent clairement l'intention et la nature opératoire, rien n'a jamais permis de prouver que l'attaque ait été réellement couronnée de succès.

• Contrairement aux attaques conventionnelles dont on peut toujours circonscrire les effets, une cyberattaque peut avoir des conséquences incalculables, même pour celui qui en est à l'origine. Le monde numérique est devenu si complexe et impacte tellement nos vies quotidiennes que personne à ce jour n'est capable d'établir une quelconque cartographie de tous ces systèmes et de leur interconnexion, qu'elle soit logique ou fonctionnelle. À titre d'exemple, lors des premiers mois de l'intervention américaine en Afghanistan, l'État-major a demandé une frappe contre les réseaux téléphoniques afghans (antennes relais) car ces derniers étaient très utilisés par les *talibans*. Cette opération a été annulée car il est très vite apparu que les *GI* auraient été privés eux-mêmes des communications téléphoniques vers leur famille et que cela affecterait trop le moral.

(2) Terme plus adapté que le terme « cyber » emprunté maladroitement aux travaux de Norber Wiener (voir en bibliographie).

(3) *Supervisory control and data acquisition* : système de contrôle et d'acquisition des données.

• Au plan philosophique, la dimension cyber, telle qu'elle est imaginée actuellement, a pour but de remettre en cause des aspects « moraux » de la guerre. Celui qui tue ou porte atteinte à autrui accepte par principe d'être lui-même tué ou de subir des dégâts symétriquement équivalents. Or, dans la conception actuelle de la dimension cyber, le but est de maximiser l'asymétrie entre attaquant et cibles, et de viser essentiellement des cibles civiles. L'exemple de la mort portée en Afghanistan ou en Irak *via* des drones pilotés de *bunkers* localisés en Arkansas par des militaires ventripotents (*cf.* Grégoire Chamayou) est choquant plus que ne l'est l'idée de guerre elle-même. Demain, avec la vision cyber actuelle, on nous propose une guerre menée par des *geeks* bien à l'abri, visant des victimes de tous types.

• Enfin, le concept de cyberguerre est dangereux car il est de nature à fragiliser grandement *Internet* et donc les sociétés occidentales qui reposent de plus en plus sur ce réseau. Pour que la cyberguerre soit viable et efficace, il est indispensable qu'un certain niveau d'insécurité soit maintenu en permanence par les États grâce au contrôle de la technologie. Cela passe par des failles *0-day*, des outils d'attaques, des protocoles non sécurisés, des mauvaises pratiques de développement, des équipements industriels, volontairement déficients (*cf.* notre article dans le *Journal in Information Warfare*). Or cela est incompatible avec la mission régalienne première des États qui est de protéger ses propres ressortissants, voire ceux des autres pays (dans le contexte de l'Europe par exemple). De plus, cela pervertit la fonction même de guerre prônée par les États : alors que la guerre classique est la réponse ultime, pour une démocratie, au maintien de la paix ou à son retour, la cyberguerre capitalise sur un état d'instabilité numérique permanent.

Si la vision actuelle de la dimension « cyber » est en fort décalage avec la réalité et nos valeurs, elle représente néanmoins une dimension incontournable. Mais, contrairement à l'orthodoxie actuelle, le cyber intervient faiblement dans la manœuvre elle-même, sinon au titre de frappes localisées, préventives, en soutien ou en préparation (comme dans le cas de l'opération *Orchard*, *cf. Der Spiegel*), mais joue un rôle majeur dans les phases de renseignement et de planification. Nous allons montrer comment la dimension cyber permet d'infliger des dégâts considérables sur des infrastructures de très grandes tailles avec des approches conventionnelles et surtout avec un nombre très réduit d'individus. Autrement dit, comment provoquer aujourd'hui autant de dégâts avec des petits groupes, qu'hier avec un corps d'armée ou une division.

Comment vraiment paralyser un pays à l'aide du cyber

La méthode générale s'appuie sur la combinaison de l'*open data* (ouverture généralisée des informations) et du *big data* (traitement par *data mining* sur des quantités colossales d'informations). Elle peut aussi impliquer des attaques ciblées pour la collecte d'informations complémentaires n'appartenant pas au domaine ouvert.

Un attaquant définit d'abord une cible, puis un effet à obtenir sur celle-ci avec une probabilité d'efficience. Ensuite, il choisit les moyens les plus adéquats à sa manœuvre. Contre un pays ou une infrastructure de grande taille, la manœuvre est généralement complexe, en plusieurs phases et faisant intervenir plusieurs composantes conventionnelles et éventuellement cyber. L'efficacité finale dépend de l'élément de plus faible probabilité de succès, lequel est encore souvent la partie cyber classique (*CNO* ou *CNA* [4]).

En effet, la véritable faiblesse des États modernes ne réside pas tant dans cette dépendance importante vis-à-vis du monde numérique que dans l'incommensurable accessibilité à toutes sortes de données, lesquelles vont permettre, lors de la phase de renseignement, d'identifier des faiblesses exploitables et les scénarios tactiques adéquats. Deux types d'informations et de renseignements sont alors disponibles :

- Les informations ouvertes (environ 70 %) qui ne nécessitent que d'être collectées, croisées, compilées et triées. Pour une manœuvre militaire, les éléments géographiques sont disponibles en masse et avec précision *via* Google Earth et consort. *Facebook* (cf. *Le Monde*) et les réseaux sociaux divers et variées, les *blogs*, *Twitter*, etc., fournissent des informations sur les personnes. Toutes les données sont intéressantes par nature. Seuls le contexte et la manœuvre décideront de leur importance finale.

- Les informations cachées (environ 25 %) [5] résident soit dans les métadonnées (informations cachées dans les données visibles, comme les coordonnées géographiques d'une photo) soit obtenues *via* un traitement mathématique (*data mining*) qui révèle des informations invisibles souvent sensibles à partir de données ouvertes.

La collecte sans limite, préventive, systématique des données et des métadonnées et leur traitement par des programmes comme *PRISM* sont essentiels.

En 2013, nous avons mené une étude opérationnelle de grande envergure (non publiée à ce jour) pour valider notre vision de la part réelle de la dimension cyber [6]. Notre cible était la moitié Ouest des États-Unis (dont la Californie, 6e économie du monde). L'effet à obtenir était l'oblitération du réseau électrique pendant 48 heures minimum [7]. Cette cible et cet effet sont capitaux pour comprendre un certain nombre de points essentiels :

(4) Sigles Otan signifiant *Computer Network Operations* et *Computer Network Attacks*.

(5) Les 5 % restants correspondent à des informations confidentielles ou secrètes obtenues par les techniques classiques d'espionnage (et en particulier, mais pas seulement, par des approches de type « cyber »).

(6) Voir également nos autres études préliminaires publiées dans *Défense nationale et Sécurité collective*, mars 2009, p. 74-86 et dans Julie Ryan (dir.) : *Leading Issues in Information Warfare & Security Research* (vol. 1), p. 36-53.

(7) Des attaques, relativement coordonnées, contre les infrastructures du réseau électrique américain ont déjà eu lieu depuis deux ans (*cf.* Rebecca Smith).

• Nos sociétés l'oublient peu à peu mais l'électricité, avant toute autre, est LA ressource primordiale. Coupez-la et tout ce qui est en aval, notamment tout ce qui dépend de la dimension « cyber », devient sans utilité. On ne peut pas mettre un pays ou une région entière sur groupes électrogènes.

• Une attaque doit comporter une frappe initiale et ensuite générer un effet domino (du fait de l'interdépendance des ressources et des composantes – humaines, techniques, services – caractérisant la cible ; voir notre contribution dans l'ouvrage dirigé par Daniel Ventre). Dans les grandes villes américaines, les pillages et les émeutes commencent en moyenne deux heures après le début d'une coupure généralisée, cela entravant grandement les possibilités d'intervention de l'État pour remettre les choses en ordre. Une telle panne provoquera des répercussions mondiales sur l'économie : chute libre du *Nasdaq* et des places boursières américaines puis internationales.

• De ce point de vue, la ressource « électricité » est capitale : qui la contrôle, contrôle tout. Or, la plupart des réseaux électriques dans le monde sont faibles, voire très faibles. Ils ont été construits souvent depuis plusieurs dizaines d'années, sur des distances importantes, avec des difficultés liées au terrain quelquefois colossales, en ayant pour souci principal la réduction des coûts. Tout cela entraîne des portions plus ou moins importantes de réseau proches de la vétusté, à la cartographie très simple voire simpliste (du point de vue de l'attaquant) et à une organisation privilégiant la fonctionnalité et le *business* sur la sécurité. Ce constat est le même pour un grand nombre d'autres infrastructures critiques dans le monde comme les routes, les ouvrages d'art, les zones portuaires…

La phase de renseignement de cette « opération » a consisté dans un premier temps à :

– cartographier précisément le réseau électrique américain (production, transformation, distribution, gestion, pylônes, sous-stations, etc.). Il est important en particulier de connaître les parties du réseau liées à la redondance et au soutien entre les trois principales zones électriques (Ouest, Est et Texas) ;

– rassembler des informations techniques sur certains points critiques comme des centrales nucléaires. Pour ces dernières, leur réseau électrique extérieur ou leurs générateurs de secours représentent des installations vitales non seulement pour leur fonctionnement mais aussi par voie de conséquence, pour leur sécurité (refroidissement des cœurs de réacteurs) ;

– collecter et analyser différents types d'informations annexes disponibles facilement en milieu ouvert :

❖ système routier à proximité ;

❖ plan des sites et informations sur les dispositifs de sécurité ;

❖ systèmes de secours ou d'intervention (pompiers, police, armée ou garde nationale) ;

❖ informations diverses (personnes impliquées, informations locales signalées dans la presse concernant des problèmes, des incidents, l'équipement…) ;

❖ analyse climatique et son impact sur les capacités d'intervention, de secours. Le moment de l'attaque est une dimension tout aussi importante que la manœuvre elle-même. Une attaque en hiver ou par grandes chaleurs – alors que la demande électrique est forte – maximisera l'effet final ;

❖ etc.

La phase de planification consiste ensuite à bâtir le scénario, identifier les forces à rassembler et les moyens à mettre en œuvre. Nous avons mis au point des techniques mathématiques de traitement de toutes ces informations implémentées dans une plateforme logicielle [8] afin d'identifier rapidement des zones de faiblesses exploitables facilement, de bâtir un scénario opérationnel (*patterns* d'attaque, chemins d'attaque) permettant la mise à profit d'un effet domino afin de maximiser l'effet final et sa probabilité de succès, et de minimiser le coût et le risque pour l'attaquant. Ce traitement permet, en particulier, de déterminer si des frappes de type « cyberattaques » sont nécessaires et avec quel degré d'implication. Les principaux résultats obtenus lors de notre étude sur les réseaux électriques américains sont les suivants :

• Dans un premier temps, quelques dizaines de points particuliers (pylônes, sous-stations…) présentant un intérêt ont été identifiés. Nous n'avons gardé que les points pour lesquels d'autres facteurs favorables (pour l'attaquant) étaient présents : zone difficile d'accès pour des camions ou des hélicoptères, possibilité de détection puis de réparation rapide, etc. Un graphe [9] réduit a été construit. Ce graphe est par nature très simple, peu dense et donc faible.

• Dans un second temps, un algorithme de recherche du nombre minimal de nœuds impactant l'ensemble du graphe a été lancé (algorithme dit du *vertex cover*, à ce sujet voir Ashay Dharwadker). Il est important de préciser que d'autres motifs combinatoires peuvent être considérés selon le type d'attaques, de cibles, d'effets à obtenir et les conditions opérationnelles souhaitées [10].

La phase d'attaque peut être menée par un groupe de taille relativement modeste (chaque membre du groupe ne connaissant pas les autres), avec des moyens réduits disponibles sur place [11]. Il est même possible d'exhiber deux groupes de cibles, produisant le même effet final, permettant de déployer en parallèle deux

(8) Actuellement en cours d'industrialisation par une société française, ARX Défense.

(9) Un graphe est une collection d'éléments mis en relation entre eux. Géométriquement, on représente ces éléments par des points (les sommets) reliés entre eux par des arcs (les arêtes) représentant les relations fonctionnelles entre les points (référence bibliographique à ajouter : Jacques Labelle : *Théorie des graphes* ; Éditions Modulo, 1981 ; 192 pages).

(10) Voir par exemple le cas des réseaux de caméras de surveillance : lire l'intervention d'Éric Filiol et Thibaut Scherrer à « La nuit du *Hack* » (congrès français de sécurité informatique), les 22-23 juin 2013 à Paris.

(11) C'est en particulier pour cet aspect que la prise en compte de la culture de la cible est fondamentale : aux États-Unis trouver des armes et des explosifs est très simple. Cela n'est pas le cas en Europe où il faudrait envisager les choses différemment.

équipes différentes à des fins de redondance opérationnelle et de maximisation de la probabilité de succès.

⁂

Si la dimension « cyber » est une dimension avec laquelle il sera inévitable de compter, elle n'est pas LA dimension incontournable qu'une certaine mode tente de promouvoir.

Là où la dimension cyber est fondamentale, c'est dans les phases de renseignement et de planification (travail classique d'état-major opérationnel) qui sont communes à tous les types d'attaques. De ce point de vue, le risque est moins dans les attaques purement « cyber », dont la portée sera forcément limitée, que dans la collecte, le traitement et l'analyse opérationnelle des données numériques qui circulent en une masse toujours plus grande. Le danger vient avant tout de la combinaison de l'*open-data* et des techniques du *big data*. Cette dernière permettra par des moyens conventionnels réduits et discrets de nuire gravement à nos infrastructures critiques.

Nous avons identifié dans le monde d'autres cas d'immenses zones de faiblesse permettant de maximiser l'effet domino en lançant une attaque contre un pays de sorte à porter atteinte à d'autre pays. L'attaque de certaines infrastructures critiques en Chine pourrait, par exemple, impacter gravement les économies occidentales.

Ainsi, notre analyse montre que la vision de ce qu'est réellement une infrastructure critique est biaisée et parcellaire, mais surtout que la cartographie des dépendances fonctionnelles est particulièrement déficiente.

Cyberarmes récentes

Stuxnet : ver informatique découvert en 2010 conçu par la *NSA* en collaboration avec l'Unité 8200 (Israël) pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium.

Aurora : importante cyberattaque chinoise, de type *Advanced Persistent Threat*, visant une trentaine d'entreprises principalement américaines.

Duqu : ver informatique découvert le 1er septembre 2011 et que l'on présume lié à *Stuxnet*.

Regin : logiciel malveillant sophistiqué utilisé comme plate-forme de cyberespionnage, attribue à la *NSA* et au *GCHQ* (le service de renseignements électronique britannique) pour espionner les institutions européennes.

Babar : virus informatique très sophistiqué de collecte attribué aux services de renseignement français.

GrayFish : cheval de Troie très performant dissimulé dans la partie électronique des disques durs (*firmware*) et conçu pour dérober des documents confidentiels en toute discrétion ou prendre le contrôle d'un ou plusieurs ordinateurs à distance (attribué à la NSA).

Vocabulaire

Advanced Persistent Threat : attaque informatique complexe mêlant différentes techniques dont les principales caractéristiques sont d'être furtives, ciblées et résidentes pendant un temps relativement long dans la cible.

Cheval de Troie : code malveillant orienté réseau dont le but est d'ouvrir une porte cachée vers le réseau *Internet* et permettre soit la fuite de données vers l'attaquant soit de permettre à l'attaquant d'agir à distance sur la cible.

Data mining : extraction de connaissances à partir de données, ayant pour objet l'obtention d'un savoir ou d'une connaissance à partir de grandes quantités de données, par des méthodes automatiques ou semi-automatiques ou des modèles mathématiques.

Geek : personne prise par une passion, à l'origine dans le domaine de la *high-tech*, puis par extension dans n'importe quel domaine sauf social.

Malware : terme générique anglo-saxon désignant tout type de codes malveillants (virus, vers informatiques, chevaux de Troie, bombes logiques…).

Patterns : mot désignant un motif (géométrique, de données…).

Virus : catégorie de codes malveillants ayant la capacité de se reproduire au sein de la cible et de l'attaquer.

Éléments de bibliographie

Smith Rebecca : « *Assault on California Power Station Raises Alarm on Potential for Terrorism* » in *The Wall Street Journal*, 5 fevrier 2014 (www.wsj.com/news/articles/SB10001424052702304851104579359141941621778).

Filiol Éric : « *The Control of technology by Nation States: Past, Present and Future - The Case of Cryptology and Information Security* » in *Journal in Information Warfare*, vol. 12, n° 3, octobre 2013.

Filiol Éric et Scherrer Thibaut : « *Securing Cities with CCTV? Not so Sure – A Urban Guerilla Perspective* » ; « La nuit du *Hack* », 22-23 juin 2013, Paris.

Chamayou Grégoire : *La théorie du drone* ; Éditions La Fabrique, 2013 ; 363 pages.

Rid Thomas : *Cyberwar will not take place* ; Oxford University Press, 2013 ; 218 pages.

Filiol Éric : « *Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct* » *in* Daniel Ventre : *Cyberwar and Information Warfare* ; ISTE, Wiley, 2011.

Filiol Éric : « *Operational aspects of Cyberwarfare or Cyber-Terrorist Attacks: What a Truly Devastating Attack Could Do* » *in* Ryan Julie (dir.) : *Leading Issues in Information Warfare & Security Research* (vol. 1) ; Academic Publishing International, 2011 ; p. 36-53.

Le Monde avec *Reuters* : « *Tsahal* annule une opération après une fuite sur Facebook » in *Le Monde.fr*, 3 mars 2010 (www.lemonde.fr/proche-orient/article/2010/03/03/tsahal-annule-une-operation-apres-une-fuite-sur-facebook_1313918_3218.html).

Follath Erich et Stark Holger : « *The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor* » in *Der Spiegel*, 2 novembre 2009 (www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html).

Filiol Éric et Raynal Frédéric : « Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur » in *Défense nationale et sécurité collective*, mars 2009, p. 74-86.

Dharwadker Ashay : « *The Vertex Cover Algorithm* », 2006 (www.dharwadker.org/vertex_cover/).

Labelle Jacques : *Théorie des graphes* ; Éditions Modulo, 1981 ; 192 pages

Wiener Norber : *Cybernetics or Control and Communication in the Animal and the Machine* (2nde édition) ; The MIT Press, 1961 ; 232 pages.