LA GUERRE ELECTRONIQUE N'AURA PAS LIEU

Focus de Knowckers

Auteur :

Pierre Caron

Ce document d'analyse, d'opinion, d'étude et/ou de recherche a été réalisé par un (ou des) membre(s) de l'Association de l'Ecole de Guerre Economique. Préalablement à leurs publications et/ou diffusions, elles ont été soumises au Conseil scientifique de l'Association. L'analyse, l'opinion et/ou la recherche reposent sur l'utilisation de sources éthiquement fiables mais l'exhaustivité et l'exactitude ne peuvent être garantie. Sauf mention contraire, les projections ou autres informations ne sont valables qu'à la date de la publication du document, et sont dès lors sujettes à évolution ou amendement dans le temps.
Le contenu de ces documents et/ou études n'a, en aucune manière, vocation à indiquer ou garantir des évolutions futures. Le contenu de cet article n'engage la responsabilité que de ses auteurs, il ne reflète pas nécessairement les opinions du (des) employeur(s), la politique ou l'opinion d'un organisme quelconque, y compris celui de gouvernements, d'administrations ou de ministères pouvant êtres concernés pas ces informations. Et, les erreurs éventuelles relèvent de l'entière responsabilité des seuls auteurs.
Les droits patrimoniaux de ce document et/ou étude appartiennent à l'Association, voire un organisme auquel les sources auraient pu être empruntées. Toute utilisation, diffusion, citation ou reproduction, en totalité ou en partie, de ce document et/ou étude ne peut se faire sans la permission expresse du(es) rédacteur(s) et du propriétaire des droits patrimoniaux.

Mots-clés

Guerre de l'électronique, stratégie, Internet, conflit, Etats.

Guerre de l'électronique ?

La presse s'intéresse particulièrement, ces derniers mois, à une menace émergente et polymorphe : à grand renfort de maximes de Sun Tzu, la guerre électronique y est décrite tantôt comme une alternative non violente aux opérations militaires, tantôt comme un prolongement de l'action terroriste traditionnelle, et tantôt comme un nouveau moyen de conduite de la guerre économique. Face à la confusion régnant autour de ces définitions, l'équipe de Knowckers.org tente un décryptage du phénomène.

La difficulté dans la compréhension de la guerre électronique réside principalement dans l'incertitude sur la nature de l'agression elle-même. Des questions aussi fondamentales que « qui m'agresse ? » ou « s'agit-il d'un acte de guerre ? » deviennent particulièrement difficiles car, contrairement aux conflits militaires classiques, y répondre relève d'un véritable défi technique qu'il n'est pas toujours possible de relever. Nous allons voir comment, sous l'étiquette « guerre électronique », sont trop souvent classés des actes de piratage dont le seul point commun est l'incertitude quant à leur origine et leur objectif.

TERRITORIALITE

Il devient évident, avec la généralisation d'Internet, que la notion de territoire, qui était prépondérante dans les guerres classiques, s'estompe complètement. Une attaque informatique ne nécessite aucune présence physique particulière, et peut donc être conduite indifféremment d'un pays ou d'un autre sans que ce dernier soit réellement impliqué dans l'attaque. Il suffit à cet effet de relayer l'attaque à travers des réseaux de proxies ou de machines compromises. C'est, par exemple, la question posée par la très médiatisée « opération Titan Rain » (pour rappel, il s'agit du nom donné à une opération de piratage massif en provenance de Chine ciblant des réseaux d'entreprises du Commonwealth, et qui a duré près d'un an) : comment lever l'incertitude sur l'implication du gouvernement chinois ? Comment établir la nationalité réelle des agresseurs, et comment prouver qu'ils prenaient bien leurs ordres d'une agence étatique ? Et cette opération est-elle réellement liée – comme cela a été évoqué par la presse – aux récentes tentatives de piratage dont ont été victimes des parlementaires anglais ? Par analogie, considérons les flux de spam sur la planète : en bout de chaîne, ils proviennent en grande majorité des Etats-Unis ; mais en amont, ils sont relayés par des réseaux de machines de particuliers infectées par des virus (ou « réseaux zombies »), qui

prennent leurs ordres depuis des serveurs en majorité hébergés à Taiwan ; serveurs eux-mêmes contrôlés par des individus de diverses nationalités (américaine, russe, ukrainienne, israélienne…) aux motivations particulièrement hétérogènes (contrefaçon pharmaceutique, escroqueries, phishing…). Il devient ainsi clair, au regard de ces incertitudes, qu'il n'est plus possible d'analyser ces phénomènes sous l'angle de la territorialité. Pire encore, en matière d'hacktivisme, on constate que les attaques échappent totalement au contrôle des états d'où elles émanent : les défacements massifs et répétés de sites web par des groupes de pirates aux revendications politiques – notamment dans le monde arabe et au Proche Orient, pendant l'affaire des caricatures de Mahomet, et en réaction aux politiques du Vatican et d'Israël – ne peuvent être ni jugulés, ni dirigées par les autorités locales qui se révèlent totalement dépassées par les évènements.

ACTE DE GUERRE

Le concept d'acte de guerre, relativement simple à appréhender dans le domaine militaire classique (espionnage, sabotage, frappe militaire…), devient en revanche extrêmement problématique lorsqu'il est transposé au domaine électronique. Prenons l'exemple de l'attaque récente des fournisseurs d'accès à Internet du Kirghizstan qui a coupé le pays du monde pendant plusieurs heures : s'agit-il, comme certains journaux l'affirment, d'une opération menée par les services secrets afin de stopper la propagande pro-démocratique, ou bien d'ingérence d'un état extérieur dans le but de soutenir le pouvoir en place ? Penchons-nous également sur l'attaque qu'ont subit pendant plusieurs heures les serveurs DNS racine en 2002 : cette tentative, qui aurait pu rendre hors service Internet dans son ensemble, et qui a été conduite depuis plusieurs milliers de machines piratées servant de caisse de résonnance réparties dans de nombreux pays, a-t-elle été commanditée et relève-t-elle d'un agenda politique, ou est-elle le fruit d'un individu ou d'un groupe isolé en quête de gloire ? Considérons enfin le piratage récent des serveurs de la société Swift par la CIA ; ici encore, la question se pose de savoir s'il s'agit, comme le prétend l'administration Bush, d'une question opportuniste de politique intérieure – lutter contre le terrorisme – ou d'un acte de guerre dirigé contre l'Europe permettant de capter un trésor inestimable d'informations financières confidentielles ; la question n'étant toujours pas tranchée par les européens. Et on le voit à travers ces exemples, ce n'est pourtant pas faute de se poser les bonnes questions : mais de fait, il est souvent impossible de trancher entre acte de guerre et opportunisme non commandité.

MOYENS OPERATIONNELS

Les opérations électroniques de grande ampleur requièrent la présence simultanée de compétences informatiques très pointues, d'une organisation parfaitement rôdée et d'outils évolués. Des analogies avec les forces armées classiques sautent aux yeux : d'une part, la spécialisation des individus en fonction des besoins des opérations ; d'autre part, la nécessité d'externaliser l'élaboration des armes et des technologies. En effet, à l'instar du marché de la défense, **il existe dans la sphère électronique un véritable réseau de sous-traitance technologique souterrain et de mercenariat**, permettant de couvrir les différents besoins liés à la conduite des opérations électroniques : la conception des virus et chevaux de Troie est prise en charge par des développeurs en freelance qui proposent leurs services moyennant rémunération, voire par des sociétés spécialisées – souvenons-nous de l'affaire Haephrati, ce couple de concepteurs de chevaux de Troie, qui avait fait trembler les plus grandes entreprises israéliennes ; la logistique est assurée par des spécialistes qui offrent à la location pour quelques dizaines de dollars des armées de machines piratées et pilotées par des virus, permettant de relayer et d'amplifier les attaques – l'an dernier, la police néerlandaise a démantelé un réseau d'un million et demi de ces machines ; les failles de sécurité, équivalent électronique des armes à feu, font l'objet d'un commerce particulièrement actif : des sociétés et agences gouvernementales rémunèrent en effet des chercheurs afin d'identifier des vulnérabilités inédites dans des composants logiciels ou réseaux, s'assurant ainsi l'exclusivité de la connaissance des moyens de leur exploitation. On trouve même à la vente des kits d'identité complets, incluant état civil, numéro de sécurité sociale et de cartes de crédit, permettant de s'assurer une couverture optimale. Autant de moyens techniques dont on ne peut pas dire qu'ils soient difficiles à réunir, puisque leurs détenteurs s'affichent en toute impunité sur des forums hébergés en Europe de l'Est, aux Etats-Unis ou parfois même en Iran. C'est ce qui alimente l'hypothèse très accrocheuse d'un « cyber-terrorisme » : on voyait mal, jusqu'ici, des terroristes se convertir aux nouvelles technologies et développer une expertise en informatique sans être financés et équipés par des états ; mais aujourd'hui, le

marché de la cybercriminalité se professionnalisant, il devient extrêmement simple de réunir ces moyens d'attaque à moindre coût pour monter une opération terroriste.

RENTABILITE

C'est peut-être le facteur le plus critique dont dépend à long terme la viabilité de la guerre électronique – le facteur qui rend aujourd'hui si peu probable un « cyber-jihad » global. La rentabilité d'une attaque électronique est extrêmement faible, non seulement en termes de pertes humaines, mais aussi en termes d'impact psychologique sur les populations : une telle attaque, à elle seule, est très peu susceptible de provoquer une terreur comparable à un attentat classique. D'ailleurs, le récent appel d'Al-Qaeda – se succédant à de nombreux autres – appelant les djihadistes à l'attaque des réseaux bancaires américains sonne faux par bien des aspects : si les attaques de déni de service peuvent occasionnellement fonctionner lorsqu'elles se concentrent sur des cibles uniques, en revanche la dispersion des sites ciblés et l'absence de coordination logistique centrale laisse prévoir un très faible « retour sur investissement » de cet appel. De plus, les banques sont parmi les rares organisations capables de repousser de telles attaques et de préserver leur activité économique. De nombreux conflits dans le monde offrent d'autres exemples frappants : en Palestine et en Israël, des pirates des deux camps s'attaquent aux systèmes d'information gouvernementaux de l'adversaire, défigurent leurs sites web et tentent de perturber leurs télécommunications ; c'est également le cas entre l'Inde et le Pakistan où aux incidents frontaliers s'ajoutent des opérations de piratage de réseaux gouvernementaux parfois très sensibles. Mais, malgré le fait qu'au moins deux des états mentionnés aient déjà intégré dans leurs doctrines militaires la guerre électronique, force est de constater que ces opérations n'ont jamais à elles été seules décisives, n'ont jamais réussi à donner l'avantage à l'un des deux côtés sans qu'il soit fait appel à la force militaire classique. Même dans la sphère économique, la spectaculaire attaque informatique contre la bourse de Moscou en début d'année a eu des répercussions mineures, puisque l'intrusion fut détectée et les systèmes réparés en à peine une heure. Ainsi, si la fameuse maxime « vaincre sans combattre » reste un objectif stratégique séduisant et loué par l'opinion publique, en revanche gagner une guerre à coups de virus informatiques relève du domaine de la science-fiction.

REACTION A L'AGRESSION

Dès lors que l'on ne sait ni qui nous agresse, ni dans quel but, il devient impossible d'adopter une attitude cohérente face à l'agresseur : les clients du couple Haephrati n'ont jamais été inquiétés ; l'opération Titan Rain a été classée sans suite, côté anglo-saxon ; l'affaire de l'interception des transactions financières Swift n'a entraîné qu'une vague protestation de l'Union Européenne. Ces réactions hasardeuses témoignent d'un manque de préparation chronique des autorités face à ce type d'attaques : **personne n'est en mesure d'obtenir une vision claire de ce qui fait l'essence même de la conduite de la guerre, à savoir la configuration du champ de bataille.** C'est d'ailleurs l'aveu du Department of Homeland Security américain, qui déclarait à l'issue de l'exercice Cyberstorm que le principal échec de cette simulation de crise informatique était précisément l'incapacité totale des organisations publiques et privées à coordonner leurs diagnostics pour obtenir une image claire des évènements à l'échelle nationale – les tentatives d'intrusion successives de l'exercice ayant été perçues comme des incidents isolés et non corrélés.

En résumé, la guerre électronique se caractérise donc par une absence de territorialité, une ambiguïté chronique sur la notion d'acte de guerre, une efficacité opérationnelle discutable lorsqu'elle n'est pas complétée par d'autres formes de guerre, et une impossibilité à être appréhendée à un niveau stratégique. Dans ces conditions, on ne peut considérer ce phénomène que comme une succession d'opérations ponctuelles, qui n'ont aucunement vocation à se substituer aux autres formes de guerre (militaire, économique, terrorisme…) mais bien plutôt de leur apporter un soutien. C'est peut-être la guerre de l'information, et par extension la guerre économique, qui seuls peuvent apporter un véritable sens à la notion de « guerre électronique ».

Sources

http://www.infosecnews.org/pipermail/isn/2006-November/013931.html

http://www.zone-h.org/content/view/14391/30/

http://www.zataz.com/news/12729/Decouverte-de-la-Centrale-d_enregistrement-et-d_analyse-pour-la-surete-de-l_information-Suisse.html

http://www.zone-h.org/content/view/14369/30/

http://feeds.feedburner.com/~r/DanchoDanchevOnSecurityAndNewMedia/~3/38801366/cost-benefit-analysis-of-cyber.html

http://news.com.com/2061-10789_3-6131302.html?part=rss&tag=6131302&subj=news

http://www.zataz.com/news/12749/Des-pirates-informatiques-modifient-la-presse-electronique-du-pays.html

http://www.scmagazine.com/uk/news/article/539631/russian-stock-exchange