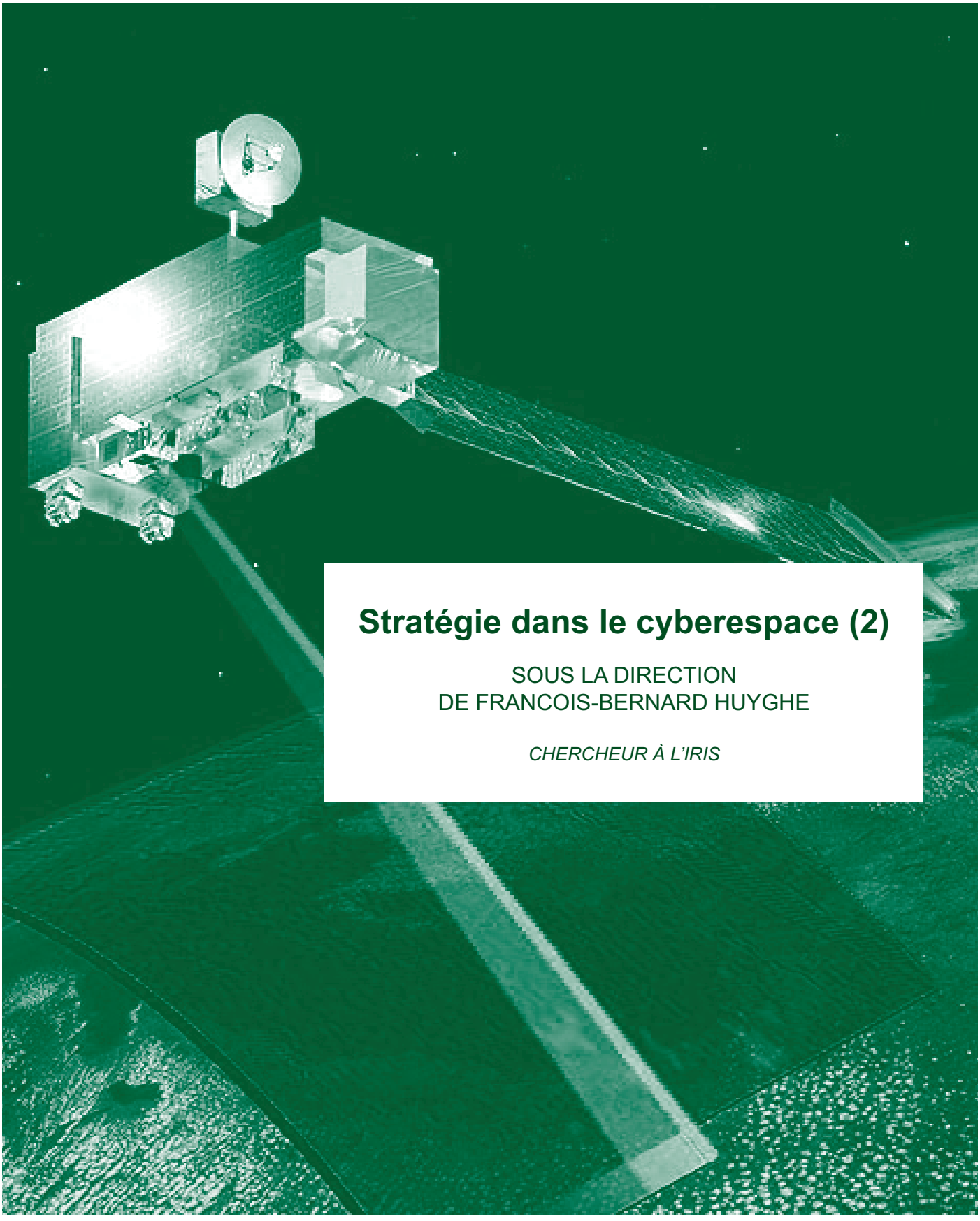
IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

OBSERVATOIRE GEOSTRATEGIQUE
DE L'INFORMATION

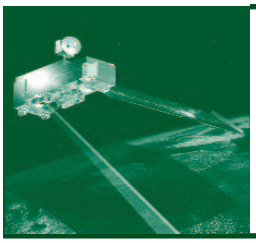
1er septembre 2012



Stratégie dans le cyberespace (2)

SOUS LA DIRECTION
DE FRANCOIS-BERNARD HUYGHE

CHERCHEUR À L'IRIS



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Cyberstratégie... 2

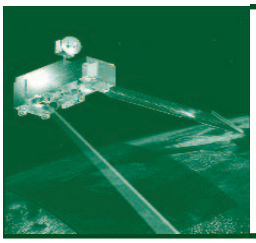
Au début de l'année 2012, l'Observatoire Géostratégique de l'Information avait publié un numéro intitulé « Stratégie dans le cyberespace ». Neuf mois plus tard, l'actualité nous suggère ce « Cyberstratégie 2 ». Certes, la cyberguerre annoncée depuis plus de dix ans n'a toujours pas eu lieu (personne n'en est mort et aucun pays n'a été conquis par écran interposé). Il n'y a pas eu d'attentat cyberterroriste majeur et les prophètes du « Cybergeddon » (cyber + Armageddon, l'Apocalypse) qui paralyserait les infrastructures vitales des pays développés attendent toujours.

En revanche, les affaires d'intrusion dans des systèmes informatiques ou d'espionnage électronique, certaines imputables à des États, se sont multipliées. L'éventualité que les Nations aient un jour à défendre leur souveraineté dans le « cinquième espace » (le cyberespace, après la terre, la mer, l'espace aérien et la stratosphère) ne paraît plus absurde... L'idée que nous défendions – le nécessaire passage d'une cyberdéfense purement technologique à une stratégie politique – progresse. Les recherches et les initiatives se sont multipliées.

Parallèlement à un dossier publié dans la Revue Internationale et Stratégique de l'IRIS ce mois-ci (Revue n°87), nous rendons compte de cette évolution dans le présent bulletin numérique. Les deux dossiers sont complémentaires, papier et virtuel. Trois pour ceux qui n'auraient pas téléchargé notre numéro de janvier 2012 toujours disponible. Ils peuvent se lire séparément.

Nous présentons ici un texte du sénateur Bockel dont le rapport sur la cyberdéfense française a fait grand bruit, notamment ses propos sur des armes informatiques offensives. Chris Demchak nous montre dans un tableau chronologique comment s'est construite historiquement (et empiriquement) la stratégie américaine en ce domaine. Rebecca Lopez nous initie ensuite aux arcanes de la stratégie russe y compris dans leur dimension diplomatique. Bertrand Boyer rappelle qu'une cyberstratégie ne concerne pas que les acteurs traditionnels des conflits. Bref, des pistes s'ouvrent sans cesse. Ce qui nous permet d'écrire, sans risque d'être démentis : à suivre... ■

François-Bernard Huyghe



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

La cyberdéfense : un enjeu mondial, une priorité nationale

par Jean-Marie Bockel,
Sénateur du Haut-Rhin, ancien ministre
Auteur d'un Rapport d'information sur la cyberdéfense, juillet 2012

Attaque informatique d'envergure de Bercy à la veille de la présidence française du G8 et du G20, espionnage informatique des entreprises à l'image d'Areva, perturbations de sites Internet comme celui du Sénat : les attaques contre les systèmes d'information se sont multipliées en France, comme partout ailleurs dans le monde, ces dernières années. Même la Présidence de la République aurait été victime récemment d'une ou de plusieurs attaque(s) informatique(s). On estime que nos grandes institutions et nos entreprises sont victimes chaque jour de plusieurs millions de tentatives d'intrusions dans les systèmes d'information.

De plus, les révélations du journaliste américain David Sanger sur l'implication probable des Etats-Unis dans la conception du virus Stuxnet, qui a détruit environ un millier de centrifugeuses d'enrichissement de l'uranium, retardant ainsi de quelques mois ou quelques années la réalisation du programme nucléaire militaire de l'Iran, ou encore la récente découverte du virus Flame, vingt fois plus puissant, laissent présager de nouvelles « armes informatiques », aux potentialités encore largement ignorées.

Il n'y a pas de « ligne Maginot » dans le cyberespace

Avec le développement de l'Internet, les systèmes d'information sont devenus les « centres nerveux » de nos sociétés, sans lesquels elles ne pourraient plus fonctionner. Dans ce contexte, la France est-elle suffisamment organisée et préparée pour faire face à une attaque contre les systèmes d'information ? Depuis le Livre blanc sur la défense et la sécurité nationale de 2008, la France a réalisé d'importantes avancées. Une agence nationale de la sécurité des systèmes d'information (l'ANSSI), a été créée en 2009 et la France s'est dotée en 2011 d'une stratégie nationale. La France dispose, avec cette stratégie et avec l'ANSSI, d'outils importants. Pour autant, notre dispositif connaît encore des lacunes. Avec des effectifs de 230 personnes et un budget de 75 millions d'euros, l'ANSSI reste encore loin des services similaires du Royaume-Uni ou de l'Allemagne, qui comptent entre 500 et 700 agents.

De plus, les ministères et les entreprises françaises restent insuffisamment sensibilisés à la menace. Renforcer la sécurité et la défense des systèmes d'information n'est pas seulement un enjeu technique. C'est aussi un enjeu économique, puisqu'il s'agit de protéger la chaîne de valeur, notre savoir-faire technologique, dans la véritable guerre économique que nous connaissons aujourd'hui, voire un enjeu stratégique, lorsque les intérêts de la nation sont en jeu. Or, avec l'espionnage informatique, la France, comme d'autres pays, est aujourd'hui menacée par un « pillage » systématique de son patrimoine diplomatique, économique, scientifique et culturel.

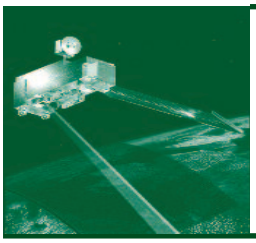
Enfin, à la différence de certains pays, la France ne dispose pas de capacités de protection et de systèmes permanents de détection des attaques informatiques à l'entrée des réseaux des opérateurs d'importance vitale (trans-

■■■ -ports, énergie, santé, etc.). Il s'agit là de notre principale lacune et d'un enjeu crucial pour notre sécurité. Quel serait le moyen le plus simple de provoquer une perturbation majeure de notre pays par le biais d'une attaque informatique ? Un moyen très simple serait de s'attaquer à la distribution d'énergie, aux transports ou à la santé. L'exemple du virus Stuxnet ou celui du ver Conficker qui a perturbé le fonctionnement de plusieurs hôpitaux en France et dans le monde, montrent que cela n'est pas une hypothèse d'école.

La cyberdéfense : une priorité nationale

La protection et la défense des systèmes d'information devrait faire l'objet d'une véritable priorité nationale, portée au plus haut niveau de l'Etat, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire. Il paraît ainsi indispensable de renforcer les effectifs et les moyens de l'ANSSI, des armées et des services spécialisés, afin de les porter progressivement à la hauteur de ceux dont disposent nos principaux partenaires européens. Beaucoup reste à faire pour sensibiliser les administrations, le monde de l'entreprise, notamment les PME, et les opérateurs d'importance vitale. Faut-il aller plus loin et passer par la loi pour fixer un certain nombre de règles ou de principes ? Après avoir beaucoup consulté, je crois qu'il est nécessaire de prévoir une obligation de déclaration en cas d'attaque informatique importante qui s'appliquerait aux entreprises et aux opérateurs d'importance vitale, afin que l'Etat puisse être réellement informé de telles attaques. Je pense aussi que l'Etat a un rôle important à jouer pour soutenir le tissu industriel, et notamment les PME, qui développent en France des produits ou des services de sécurité informatique, pour ne pas dépendre uniquement de produits américains ou asiatiques. Je plaide ainsi dans mon rapport pour une politique industrielle volontariste, à l'échelle nationale et européenne, pour faire émerger de véritables « champions » nationaux ou européens.■

*
* * *
*

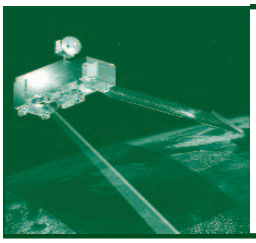


OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

S'adapter pour survivre dans le cyberespace : l'exemple des Etats-Unis

Chris Demchak, Professeur au Strategic Research Department de l'U.S. Naval War College présente dans la Revue internationale et stratégique n° 87 de l'IRIS un article sur l'organisation de la défense à l'ère du cyberconflit aux États Unis. Nous reproduisons ici, adapté au public français, un tableau chronologique complémentaire et révélateur. Il met en parallèle les grandes affaires de cybersécurité et les réactions complexes des trois groupes concernés aux USA : les organismes responsables des infrasctructures militaires et gouvernementales, les responsables des infrastructures critiques et les représentants des organes économiques privés. ■

Mars 1999	Virus Melissa
Mars 2000	Virus I love you
Juillet 2001	Virus Code Red
Oct. 2002	Création de la Joint Task Force-Computer Network Opérations (JTF-CNO)
Nov. 2002	Arrivée du cheval de troie "Beast" qui permet d'infecter les ordinateurs ayant Windows
Jan. 2003	Virus SQL Slammer worm
Fév. 2003	Publication du document National Strategy to Secure Cyberspace (NSSC) aux USA
Juin 2003	Création du DHS, Department of Homeland Security for critical infrastructure
Août 2003	Virus Blaster
Sept. 2003	Création du US-CERT, US Computer Emergency Readiness Team, DHS
Jan. 2004	Virus MyDoom.A
Sept. 2005	Création de la Joint Functional Component Command-Network Warfare (JCC-NW)
Jan. 2006	Virus Blackworm
Juin 2006	Publication du document National Military Strategy for Cyberspace Operations
Jan. 2007	Virus Botnet
Mai 2007	Cyberattaque russe du gouvernement, des médias et du sytème financier estonien
Juillet 2007	Arrivée du cheval de Troie Zeus qui s'attaque aux systèmes de sécurité bancaire
Juillet 2008	Arrivée du virus Koobface qui se concentre sur les réseaux sociaux
Oct. 2008	Arrivée du virus Conficker
Mai 2009	Publication du Cyberspace Policy Review (CPR)
Sept. 2009	Le virus chinois Ghostnet s'attaque aux structures informatiques tibétaines
Mai 2010	Création de l'US Cyber Command qui fusionne les institutions précédentes
Juin 2010	Arrivée du virus Stuxnet qui s'attaque au système nucléaire SCADA iranien
Oct. 2010	Publication du Comprehensive National Cybersecurity Initiative (CNCI)
Avril 2011	Publication du National Strategy for Trusted Identities in Cyberspace (NSTIC)
Juillet 2011	Publication du DOD Strategy for Operating in Cyberspace (DSOC)
Août 2011	Découverte de l'Opération Shady Rat (cyberattaque coordonnée venue d'Asie)
Nov. 2011	Publication du Blueprint for a Secure Cyber Future (BSCF)
Nov. 2011	Publication du DOD Cyberspace Policy Report (DCPR)
Déc. 2011	Publication du Strategic Plan for Federal Cybersecurity R&D (TCSP)
Jan. 2012	Publication du DOD Defense Strategic Guidance, highlights cyber threats (DSG)
Mars 2012	Publication du National Preparedness Report, DHS FEMA (NPR)
Avril 2012	Publication du DOD Joint Staff Joint Concept for Cyberspace



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Quelle stratégie russe dans le cyberespace ?

par Rebecca Lopez,
Assistante de recherche à l'IRIS

Face à des cyberattaques de plus en plus nombreuses, mais aussi de plus en plus sophistiquées, les Etats sont nombreux à développer des stratégies : unités militaires dédiées aux opérations cyber, agences et centres spécialisés. Si les Etats-Unis font figure de modèle, d'autres Etats se sont lancés dans la course. Dernière en date, la Russie qui a fait plusieurs annonces.

La Russie a un rang à tenir !

En septembre 2000, la Fédération de Russie a publié un document : la Doctrine de défense informationnelle. Il dresse un bilan des retards technologiques accumulés par le pays dans les années 1980-1990. Au cours de cette période de grande dépendance à l'égard des technologies occidentales, la sécurisation des données du pays – donc sa souveraineté – s'est fragilisée. Ce document est à l'origine de plusieurs projets : développement d'un système d'exploitation national – Natsionalnaïa programmnaïa platforma ou NPP.; création d'une Commission spéciale pour la modernisation et le développement technologique de l'économie russe ; construction d'un parc technologique à Slolvoko – la « Silicon Valley russe » où se déroulera le G8 de 2014 –, ou encore un projet d'infrastructure e-gouvernementale prévu pour 2014.

Cependant, le conflit avec la Géorgie en 2008 a révélé les lacunes de cette doctrine et la nécessité d'intensifier ses efforts de modernisation. Vladimir Poutine a officialisé le nouvel objectif : reprendre son statut de leader dans toutes les technologies militaires, c'est-à-dire dans les domaines aérien, spatial… mais également « dans le cyberespace ». Trois annonces majeures ont été formulées au premier trimestre de l'année 2012 :

• La création d'un cyber-command au sein des forces armées. Objectif : assurer la défense des systèmes d'information des organes militaires mais également, protéger les infrastructures nationales de l'information.

• La publication d'une Stratégie sur la sécurité de l'information, détaillant l'action des forces armées au sein du cyberespace.

• La création d'une agence de recherche militaire avancée, semblable à la Darpa américaine et dotée d'un budget équivalent (soit plus de 3 milliards de dollars).

Avec ces réformes, l'intention des Russes est de rattraper le retard vis-à-vis du géant américain, mais surtout de concurrencer dès maintenant les velléités chinoises et indiennes de devenir les numéros deux et trois du cyberespace. Un signal très fort est également envoyé à la communauté internationale.

La Russie, dans le collimateur de nombreux Etats ?

Ces annonces sont d'autant plus significatives qu'elles proviennent d'un Etat considéré depuis plusieurs années – du point de vue des Etats-Unis mais également de pays européens, d'entreprises et d'ONG – comme l'ennemi n°1 (ex-aequo avec la Chine) dans le cyberespace. Et pour cause, la Fédération de Russie est devenue, depuis les attaques de déni de service (DDoS) menées contre les autorités géor- ■■■

■■■-giennes en juillet 2008 parallèlement à des actions militaires « classiques », le seul pays officiellement impliqué dans une offensive militaire dotée d'une composante cyber. Il est difficile de croire – surtout depuis que la presse a révélé, sans être vraiment démentie, que le virus Stuxnet avait été fabriqué par les administrations Bush puis Obama – que les autres Etats n'ont jamais développé un volet cybernétique dans les conflits récents ; mais il serait tout aussi compliqué d'affirmer que la Russie fait l'objet d'un ostracisme infondé.

Pour qui s'intéresse aux nationalités des hackers et/ou cybercriminels les plus « doués », il faut bien avouer qu'une grande partie provient de Russie ou de la Communauté des Etats indépendants. Selon le rapport réalisé par le groupe russe IB sur l'activité des cybercriminels russes au cours de l'année 2011, les hackers de ce pays gagneraient à eux seuls 5,4 milliards de dollars dans un marché de la cybercriminalité estimé à 12,6 milliards de dollars ! Cela ferait déjà plusieurs années que les groupes mafieux pratiquant la criminalité traditionnelle se seraient alliés avec des hackers pour mettre en forme ce marché. Ils mèneraient des opérations de fraude en ligne, des attaques par déni de service, envoieraient des spam, proposeraient des services d'anonymisation ou encore vendraient des logiciels malveillants.

Si la Russie affirme combattre ce phénomène avec énergie et appréhender régulièrement des pirates via son unité de cybercriminalité (appelée département « K »), de nombreux experts pensent que le pays se sert au contraire de ce vivier pour développer une « cyberguerre open source» en échange d'une protection par le FSB sur le territoire national.

Pour maintenir une séparation vis-à-vis de ces hackers, le gouvernement russe n'assurerait pas directement leur financement, se servant d'entreprises pro-gouvernementales comme intermédiaires. Les attaques menées contre la Géorgie viendraient par exemple du gang criminel Russian Business Network (RBN), « dirigé par un certain « Flyman » – qui n'a pas encore 30 ans – neveu d'un puissant homme politique russe et donc à l'abri des forces de sécurité et des poursuites judiciaires ». La Russie aurait également offert plusieurs millions de dollars à Herman Simm, ancien chef de cabinet du ministre de la Défense d'Estonie, en échange d'informations sur la cyberdéfense européenne, otanienne et estonienne.

Avant les annonces officielles de l'année 2012, ces méthodes ont permis à la Russie de lancer une stratégie asymétrique de maîtrise du cyberespace et sont un outil de dissuasion considérable.

Virus Flame : une arme étatique ?

Découvert à la suite d'une alerte de cybersécurité, le virus Flame a défrayé la chronique à la fin du mois de mai 2012. Eugene Kaspersky – consultant russe indépendant sur la sécurité et fondateur de l'éditeur d'antivirus de renommée mondiale Karsperksy Lab – a été chargé de l'étudier. Il a conclu que Flame ne pouvait être que l'œuvre d'un ou de plusieurs Etats et que ses similitudes avec le virus Stuxnet le conduisaient à pointer du doigt, d'une manière à peine voilée, les Etats-Unis et Israël. Sans surprise, les experts en sécurité informatique américains ont crié au scandale, soulignant plusieurs éléments pouvant discréditer Karspersky Lab.

A posteriori, les contre-arguments américains ont eu deux effets contradictoires. Ils ont d'abord semblé vite démentis. Dès le début du mois de juin, le virus entrait dans une phase d'auto-destruction, ce qui indiquait que ses auteurs cherchaient à tout prix à effacer leurs traces. Quelques semaines plus tard, le Washington Post publiait des déclarations d'officiels américains affirmant que Flame avait été conçu par la National Security Agency, la CIA ainsi que l'armée israélienne, afin de ralentir l'effort ■■■

de nucléarisation de l'Iran. Cependant, ces arguments ont aussi soulevé l'hypothèse d'une collusion entre Karspersky Lab et la Russie d'une part, et la Russie et l'Union internationale des télécommunications (ITU) d'autre part. Cette relation est d'autant plus problématique qu'elle intervient quelques mois avant la Conférence mondiale sur les télécommunications internationales (WCIT), organisée par l'ITU du 3 au 14 décembre 2012 à Dubaï. La Russie y défendra une gestion étatique de l'Internet et l'affrontement avec les Etats-Unis semble inévitable.

Vers une confrontation Russie-USA ?

Après avoir décelé Flame, Eugene Karspersky s'est rangé sur les positions de l'Etat russe qui a qualifié le virus de « cyber-arme » et annoncé le pire si les Etats ne parvenaient pas à une plus grande collaboration internationale en matière de cybersécurité. Ce type de discours sert les intérêts économiques de la société – « marketing de la peur » –, mais aussi la position de la Russie : l'élaboration d'un traité international sur la sécurité informatique internationale (SII).

La Fédération russe est l'un des Etats les plus en pointe sur le sujet. Elle le traite autant au niveau bilatéral – y compris avec les Etats-Unis – que multilatéral (ITU, OSCE, OCS…). Si certaines résolutions d'initiative russe ont été adoptées à différents échelons, l'objectif russe est un traité international sous drapeau onusien qui réviserait et complèterait la convention de Budapest sur la cybercriminalité de 2001 – un traité que la Russie a refusé de signer en raison des atteintes à la souveraineté et la sécurité nationale que certains clauses induisent. Il s'agit donc de trouver un compromis entre le libre-accès des individus aux technologies de l'information et de la communication et le risque d'usage de ces dernières à des fins d'ingérence, d'atteinte à la souveraineté ou à la sécurité nationale, à l'intégrité territoriale etc.. Le sujet central du prochain événement organisé par l'ITU touche l'un des volets les plus sensibles de la SII : l'Internet. Les Etats y seront invités à adapter, pour la première fois depuis 1988, les International Telecommunications Regulations (ITR). Ces ITR conditionnent le partage du trafic télécom international et ont force de traités internationaux.

A quelques mois de cet événement, les tensions sont palpables. D'un côté, la Russie, la Chine, l'Inde mais également certains pays arabes comme l'Arabie Saoudite pour qui les ITR doivent être profondément révisés afin de parvenir à une gestion et une responsabilité commune en matière d'utilisation d'Internet. De l'autre, la position américaine pour qui une institution compétente est déjà en charge de l'Internet – l'ICANN, association sans but lucratif de droit américain –, du coup, seuls des changements minimes, relatifs au jeu de la concurrence et aux accords commerciaux, devraient avoir lieu.

La Revue internationale et stratégique n°87

■■■ Des deux côtés, des arguments de poids :

• La Russie et ses alliés essaieront de montrer que l'ITU est plus légitime que l'ICANN puisqu'elle est rattachée aux Nations Unies et même antérieure à l'organisation – il n'y aurait donc plus de « traitement de faveur ». Il se pourrait que la Russie instrumentalise les affaires Stuxnet et Flame pour montrer que les Etats-Unis ne sont pas des victimes, mais le grand responsable de la course aux cyber-armements. Ils joueront aussi sur la contradiction américaine entre la promotion d'un Internet libre, sans entrave étatique, et l'utilisation par ce même Etat des potentialités numériques au nom d'intérêts géopolitiques.

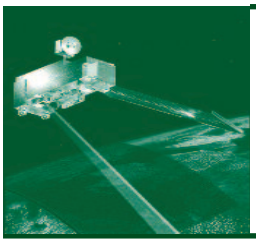
• Pour leur part, les Etats-Unis mettront l'accent sur les bénéfices économiques et démocratiques de la régulation libérale d'Internet. Par les biais de leurs firmes technologiques – qui contribueront à la sensibilisation des internautes –, ils agiteront la crainte que la Russie et ses alliés ne donnent un cadre légal à la censure du Web et n'exigent des internautes un paiement des frais de transmission.

Nul ne sait encore ni les résultats de ce sommet ni ce que le renforcement de l'ITU – donc une victoire du « front anti-ICANN » – signifierait pour les internautes. Rappelons que les décisions y seront prises à l'unanimité, ce qui réduit déjà grandement la possibilité d'un bouleversement total du fonctionnement actuel de l'Internet.

Certains blogueurs imaginent déjà la fin de l'anonymat sur Internet, une taxe au clic, ou la mise en place de dispositifs facilitant le contrôle et la régulation par les Etats du trafic Internet. Et il paraît peu probable que tous les Etats se rangent du côté de l'opposition aux Etats-Unis. L'axe principal de la stratégie américaine sera sans doute de « faire oublier » les affaires Stuxnet et Flame et la collusion américaine avec l'ICANN et d'insister sur les conséquences désastreuses d'un « changement de mains ». Quoi qu'il en soit, le degré de modification des ITR sera révélateur des gages que la Russie obtiendra ou pas. La partie ne fait que commencer... ■

*
* * *
*

[La Revue internationale et stratégique n°87]



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Le cyberespace, nouveau champ pour la géopolitique ?

par Bertrand Boyer,
Officier spécialiste de sécurité des systèmes d'information,
Auteur de « Cyberstratégie, l'art de la guerre numérique » aux éditions Nuvis

Dans les études géopolitiques classiques, les interactions entre le territoire et la politique occupent une place centrale. L'Etat fait toujours et encore figure de référence, bien que menacé dans son rôle de régulateur par l'émergence de nouveaux acteurs. Yves Lacoste définit alors la « nouvelle géopolitique » comme « l'étude des interactions entre le politique et le territoire, les rivalités ou les tensions qui trouvent leur origine ou leur développement sur le territoire ». Pourtant, à bien y regarder, un territoire demeure trop souvent exclu de cette analyse : le cyberespace.

Cette quasi absence du cyberespace dans la production géopolitique trouve probablement son origine dans la difficile appréhension de ce milieu qui ne se réduit pas à la description géographique et physique usuelle. Pourtant, les évolutions scientifiques et techniques ont contribué à modifier la relation de l'homme à la nature, elles ont également modifié sa perception de la géographie. Le cyberespace, résultat d'une révolution technique, a donc forcément contribué à façonner une autre vision du monde, tout en créant une forme d'espace propre. Ainsi, comme pour les espaces physiques, nous observons quotidiennement le jeu du droit et de la puissance, les rivalités autour de la définition des périmètres de souveraineté, les actes hostiles mais également des avancées positives qui répondent à une forme d'auto-organisation comparable à des politiques d'aménagement du territoire. Dès lors, aucune barrière théorique ne nous interdit de penser une géopolitique du cyberespace.

Le cyberespace comme un territoire éthologique

La notion de territoire se résume souvent à la définition d'espace politique. Ainsi, à la naissance même du terme se trouve l'idée de l'organisation d'un espace par une entité politique qui en fixerait les frontières ou les limites. Cette idée se retrouve chez Yves Lacoste pour qui le territoire a d'abord désigné au Moyen Age un certain nombre de fiefs et de localités sur lesquelles s'étend l'autorité d'un pouvoir ecclésiastique, puis les terres sur lesquelles s'exercent les lois et les pouvoirs d'un Etat. Dès lors, l'Etat, fixe, délimite, organise un espace qui par cette intervention se trouve propulsé au rang de territoire. C'est par ce biais que la géopolitique s'est longtemps développée, car la place de l'Etat comme acteur principal des interactions sur un territoire n'a été disputé que très récemment. Pourtant, en conservant cette vision centrée sur l'Etat, aucune analyse pertinente ne pourra aboutir dans le cyberespace car aucune autorité ne semble en fixer les limites, ni même les lois.

Pour que le cyberespace soit vécu comme un territoire, il convient de se tourner vers l'éthologie et la biologie plus que vers la géographie politique car ces disciplines nous proposent de structurer l'espace avec d'autres systèmes de références. Le règne animal nous offre ainsi une autre approche du territoire, une définition non plus liée à l'organisation politique, mais à la hiérarchie sociale. Le Robert en donne alors la définition suivante : zone qu'un animal ■■■

se réserve et dont il interdit l'accès à ses congénères. Le sujet, ici l'animal, définit donc lui même les limites de l'espace qu'il contrôle, la zone au sein de laquelle il occupe la plus haute place dans la hiérarchie des sujets. La similitude avec le cyberespace est alors plus simple à dégager. Le sujet peut être un internaute, un groupe fédéré temporairement autour d'un projet, un simple usager des réseaux ou encore une multinationale. Ce sujet, s'approprie alors une zone, la délimite et crée son propre système de référence. Introduire cette vision pour décrire le cyberespace comme un territoire présente alors l'avantage de minimiser le rôle des Etats dans la production de normes et replace l'individu au cœur de cet espace.

Le sujet est producteur de normes dans le cyberespace, notamment au travers d'institutions scientifiques où chacun peut librement contribuer à la réflexion, alors que les Etats peinent à investir ce champ. Cette vision introduit également avec force le lien originel entre territoire et violence, car le sujet définit son territoire en opposition avec le reste du groupe, il en « interdit l'accès ». Le cyberespace est alors organisé par la compétition entre les « sujets » et non par l'imposition de normes par une structure de gouvernance. Cette compétition génère une hiérarchie qui définit les frontières mouvantes d'un milieu que l'on a présenté à tort comme dé-territorialisé. Représentation territoriale à part, ni à côté, ni au dessus des espaces physiques, la notion de cyber territoire s'impose et entre de facto dans le champ de la géopolitique.

Les acteurs de la géopolitique du cyberespace

Devenu « territoire » le cyberespace doit, pour permettre à l'analyse géopolitique d'opérer, être le théâtre d'interactions entre sujets identifiés. Une première approche permet de distinguer trois catégories d'acteurs, ceux qui ont toujours eu un rôle dans les études géopolitiques, ceux qui sont apparus avec le cyberespace et enfin ceux dont le statut a changé du fait de l'apparition de ce nouveau territoire.

• Les acteurs classiques

Acteur historique principal de l'analyse des relations internationales, l'Etat a longtemps été l'unique objet de la géopolitique. Mettant en œuvre la violence légale, traçant les frontières, organisant les territoires et producteur de lois, il représente la forme aboutie d'organisation politique acceptant difficilement que sa position dominante soit remise en cause. Pourtant, l'émergence rapide du cyberespace, en réaction à la formidable révolution technologique, et son appropriation par des entité non-étatiques a paru un temps saper cette position centrale. Pour la première fois, les potentialités d'un objet technique échappaient à son contrôle. L'Etat a subi le choc initial et perdu l'initiative. Mais la vieille organisation politique, chahutée en cette fin de XX^{e} siècle n'est pas complètement désarmée. Ainsi, au terme d'une première phase de sa jeune histoire, le cyberespace semble aujourd'hui redevenir l'objet d'âpres convoitises et le théâtre des jeux de puissances classiques. La lutte contre la cybercriminalité ou le terrorisme offre l'occasion aux Etats de réinvestir le cyberespace et de tenter de mettre en place des outils de contrôle et de répression. Dans leurs sillages, les organisations internationales et supra nationales opèrent leur grand retour et multiplient les initiatives plus ou moins adroitement.

• Les acteurs mutants

Cette deuxième catégorie d'acteurs de la géopolitique du cyberespace rassemble des groupes dont l'existence n'est pas une conséquence de la « société de l'information » mais qui trouvent en elle un vecteur d'influence sans égal. Ce sont en définitive des acteurs classiques qui ont changé de nature par le fait de la révolution numérique et qui ont atteint une taille critique leur permettant d'interagir dans ce nouveau territoire. La plupart des grands groupes industriels, mais également les entreprises de taille plus modeste, ont, à l'image de cer-

■■■ -tains groupes criminels ou associatifs, rapidement investi le cyberespace. Au rang des acteurs mutants on peut également ranger les principaux groupes de presse dont les vitrines numériques constituent autant de vecteurs d'influence. Les métiers de « l'information » ont connu une véritable mutation faisant passer le journaliste du statut de témoin à celui de faiseur d'opinion, lui conférant une capacité de manipulation des masses que seul une solide éthique peut contrebalancer. Ainsi, les mutants numériques, s'ils n'étaient pas absents de la scène internationale par le passé, ne pouvaient cependant pas prétendre y jouer un rôle de premier ordre. Simple figurant du « grand jeu » des puissances, ils n'étaient pas acteurs de la géopolitique. Aujourd'hui, ils se constituent en acteurs autonomes s'invitant à la table des acteurs classiques, brouillent le jeu et complexifient le tableau.

• Les acteurs émergents

La dernière catégorie regroupe les acteurs du cyberespace nés de celui-ci. Si les « classiques » acceptent difficilement de voir l'influence croissante de la deuxième catégorie, ils ont encore plus de préventions lorsqu'il s'agit des « émergents ». J'entends englober dans ce groupe les entités qui pèsent aujourd'hui sur la scène internationale et qui n'existaient pas avant « l'ère numérique ». On retrouve ainsi les principales industries des nouvelles technologies et de la communication (au sens large, IT, Web, réseaux sociaux, télécommunications) mais également un acteur quasi inexistant dans la jeune histoire de la géopolitique : l'individu, l'usager du cyberespace. L'analyse classique évoque fréquemment « les populations » ou les groupes humains en les catégorisant suivant leurs nationalités, leurs croyances, mais jamais (très rarement) l'individu. Celui-ci n'existe que parce qu'il se raccroche à un acteur classique (Etat, Religion, groupe social), il est englobé dans une structure qui fait référence. Or la construction même du cyberespace place l'usager dans une position bien différente. La possibilité dont chacun dispose de « créer son territoire » et de le défendre fait de l'individu un acteur à part entière de la géopolitique.

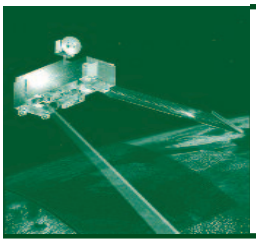
Pour la première fois, l'usager ne subit plus un territoire, il le construit, le façonne et s'y intègre pleinement hors de tout contrôle, hors de toute politique globale. Cette brève qualification des acteurs de la géopolitique du cyberespace offre donc à l'analyse une variation complexe de combinaisons où politique économie et territoire se mêlent.

Quelles interactions ?

Pour respecter la vision classique de la géopolitique, il ne suffit pas de placer des acteurs sur un territoire. L'effort principal est devant nous. Il convient maintenant d'étudier les interactions qui s'y opèrent. Si la cyberstratégie regroupe l'étude des principes et des modalités de l'affrontement dans, par et pour le cyberespace, on constate d'emblée la nature différente de la géopolitique. Il ne s'agit plus exclusivement de relations conflictuelles mais bel et bien de traiter de l'ensemble des interactions possibles et de leurs conséquences.

En quoi le milieu influence-t-il la politique et les actions des sujets qui y évoluent ? L'actualité nous offre quotidiennement le spectacle de l'utilisation de la sphère numérique par les acteurs classiques des relations Internationales. Comme une « surcouche » à leurs activités, cet aspect ne semble pas véritablement modifier les rapports de forces entre puissances. In fine, le cyberespace n'a pas inversé l'ordre établi et si l'on peut argumenter sur le terme de super-cyber-puissance, les Etats-Unis ne semblent pas prêt de céder leur place de leader.

Le cyberespace doit donc s'intégrer dans l'analyse géopolitique, il y a toute sa place et s'il est facile de mesurer l'impact de ce milieu dans les relations entre acteurs classiques, il est impératif de considérer aujourd'hui l'influence croissante des autres parties. ■



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Le cyberespace, un espace politique ?

par François-Bernard Huyghe, chercheur à l'IRIS

La cyberstratégie a trop longtemps été résumée à un problème technologique. Tout se passait comme si des attaques de plus en plus sophistiquées devaient forcément se produire un jour sans que l'on sache si elles relèveraient de la délinquance pure, de l'espionnage de données cruciales dans la compétition géoéconomique, de l'agression à motivation idéologique contre des régimes, de l'accompagnement (ou la préparation) d'offensives militaires classiques, ou enfin d'opérations de perturbation destinées à frapper les infrastructures vitales d'un pays, donc à répandre le chaos, pour faire passer un message terroriste ou exercer une contrainte politique. La solution aurait donc été de se doter de défenses impénétrables et d'alerter la population, et les entreprises doublement exposées, et comme proies à piller, et comme composantes de la sécurité nationale à désorganiser... Rien de tout cela n'est, à proprement parler, faux et il nous avons, bien entendu, besoin de meilleurs antivirus, d'une meilleure surveillance, de sytèmes de réaction plus rapides, de résilience, d'experts, d'insitutions pour coordonner le tout... Et l'État protecteur est bien dans son rôle en tentant d'assurer à ses citoyens qu'aucun danger majeur venu du cyberespace ne perturbe l'ordre public.

Mais ce que nous révèlent les derniers événements – et qu'analysent les articles de ce numéro –, c'est qu'il ne faut pas penser seulement en termes de logiciels ou d'infrastructure, de ravage ou de performance. Il faut aussi raisonner en termes politiques, sur ce que peuvent vouloir et entreprendre des rivaux en quête de puissance, donc sur ce que l'on peut faire pour agir sur leur volonté ou leur capacité.Chaque pays réagit en fonction de son histoire. Les USA se sentent exposés dans la mesure où ils dépendent d'infrastructures de haute technologie : d'où la nécessité à la fois de se défendre tous azimuts et de coordonner forces militaires, administrations, acteurs économiques dans une quête de sécurité totale. Mais en même temps Washington doit concilier sa promotion d'un Internet « ouvert » (politiquement, économiquement et culturellement) et ses alliances avec des acteurs économiques du Net qu'il s'agisse d'agir contre Wikileaks ou Megaupload.

Quelle place pour la France ?

Des puissances montantes comme la Russie (et sans aucun doute la Chine) ne considèrent pas seulement l'affrontement dans le cyberespace en termes capacitaires (des armes, des protections) mais aussi en fonction d'alliances, de manœuvres diplomatiques. Ils s'agit pour eux de conserver leur souveraineté sur un espace numérique et donc, de se protéger contre la dépendance technologiques ou les messages idéologiques venus de l'extérieur autant que contre des virus informatiques. Quant à la France, on voit bien, à travers sa façon encore timide d'aborder les questions des armes offensives, de la doctrine d'emploi (rendue ou non publique) ou de la perspective de « sanctuariser » notre espace numérique, combien pèse la problématique de l'indépendance nationale et de la dissuasion atomique. Qu'il s'agisse d'avancement technologique (le savoir), de règles techniques ou juridiques (la norme) ou de capacité de défense/destruction (la violence) une nouvelle dimension de la géopolitique s'ouvre devant les Nations qui sont tout sauf absentes ou dépassées dans le cyberespace. ■

Pour aller plus loin...

- AMBINDER M., The Revolution will be Twittered, *The Atlantic*, 15 Sept 2009
- ANSSI, Défense et SSI, stratégie de la France, 15 février 2011
- ARPAGIAN N., *La Cyberguerre – La guerre numérique a commencé*, 2009, Vuibert.
- ARQUILLA J. et RONFELDT D., *Networks and Netwar : the Future of Terror, Crime and Militancy*, Rand 2002.
- BOCKEL J.-M., Rapport d'information sur la cyberdéfense, Sénat, juillet 2012
- BOYER B., *Cyberstratégie L'art de la guerre numérique,* Nuvis 2012
- CAMPBELL D., *Surveillance électronique planétaire*, Allia, 2001.
- CARDON D., *La démocratie Internet : promesses et limites*, Seuil, 2010.
- CASTELLS M., *L'ère de l'information*, 3 tomes, Fayard, 1998.
- DARTNELL M., *Insurgency Online : Web Activism and Global Conflict*, Toronto Press, 2006
- DEMCHAK C., *Wars of Disruption and Resilience: Cybered Conflict*, Power and National Security UGA Press, 2011
- DOSSÉ St. et KEMPF O. (dir.), *Stratégies dans le cyberespace*, éd. L'esprit du livre, 2011.
- GRANT Rebecca, Victory in Cyberspace, Air Force Association, 2007
- HARREL Y., *Cyberstratégie russe*, Economica, 2012..
- HOFFMAN B., *The use of Internet by Islamic Extremists*, 2006, Permanent Select Committee on Intelligence.
- HUYGHE F.-B. *Écran/Ennemi Terrorismes et guerres de l'information*, Ed 00h00.com, 2002
- JIAN M., *China's Internet Dictatorship*, 2005, Project Syndicate.
- KEMPF O., *Introduction à la cyberstratégie*, Economica, 2012
- LIANG Q. & XIANGSUI W., *La Guerre hors limites*, 2003, Editions Payot & Rivages.
- LIBICKI M., *Cyberdeterrence and Cyberwar,* RAND, 2009
- MÉDIUM (revue), HUYGHE F.-B. (dir.), Réseaux : après l'utopie ?, *Médium n° 25*
- MOROZOV E., *The Net dellusion*, Public Affairs Books, 2011
- NYE J.S., *Cyberpower*, Harvard University, 2010
- Observatoire Géostratégique de l'Information Cyberstratégie, Iris, Jan. 2012
- PANORAMIQUES n°52, HUYGHE F.-B. (dir.), *L'information, c'est la guerre*, 2001
- Revue Internationale et Géostratégique, Dossier Cyberstratégie (F.B. Huyghe dir.) sept. 2012
- CSIS, Securing Cyberspace for the 44th President, *Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, 8 décembre 2008.
- VENTRE D. (dir), *Cyberguerre et guerre de l'information*, Lavoisier, 2010.

L'Observatoire Géostratégique de l'Information

Sous la direction de François-Bernard Huyghe, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Il analyse, par exemple les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

IRIS - Institut de Relations Internationales et Stratégiques
2 bis, rue Mercoeur
75011 Paris - France
iris@iris-france.org

www.iris-france.org
www.affaires-strategiques.info

Secrétariat de rédaction : Pierre-Yves Castagnac