Observatoire du Monde Cybernétique

Avril 2012

Même s'il s'inscrit dans la continuité de l'Observatoire de la Guerre Informatique – OGI, créé en 2005 par la DAS, l'Observatoire du Monde Cybernétique – OMC – marque un changement d'orientation important. Au-delà des menaces et des doctrines de lutte informatique, l'objectif est d'appréhender le cyberespace comme un enjeu de puissance globale.

Le portail OMC, une plateforme intuitive

Le portail OMC propose une nouvelle plateforme de navigation agrégeant les produits de la veille réalisée par CEIS. De la page d'accueil, vous aurez accès aux brèves d'actualité, aux analyses OGI et OMC publiées jusque-là ainsi qu'aux « analyses pays » par simple clic sur le pays correspondant.

Le présent mensuel est notamment disponible sur le portail. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

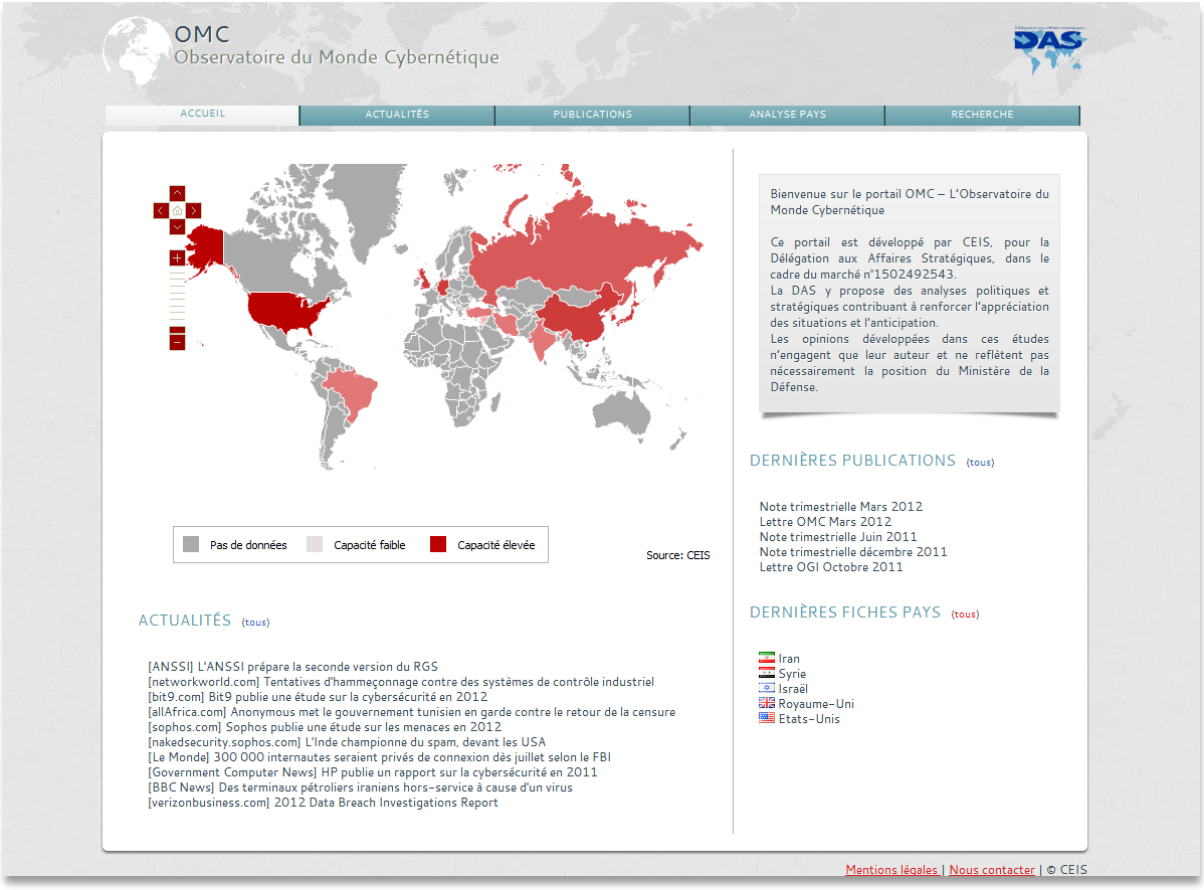

Figure 1 - Page d'accueil du portail OMC - https://omc.ceis.eu/

Pour vous y connecter, n'hésitez pas à demander vos identifiants à CEIS.

Contact : Barbara Louis-Sidney - blouis@ceis.eu et omc@ceis.eu

Figure 2 - Actualités du portail OMC

Une approche « pays » privilégiée

Le portail OMC élargit le périmètre de veille et d'analyse et s'intéresse à l'ensemble des enjeux liés au cyberespace, qu'ils soient politiques, diplomatiques, militaires, économiques ou technologiques. A côté d'une approche thématique transverse, OMC privilégie une approche « pays » permettant d'évaluer de façon plus fine les capacités « cyber » d'une vingtaine de pays clés, ainsi que les rapports de force dans le cyberespace.

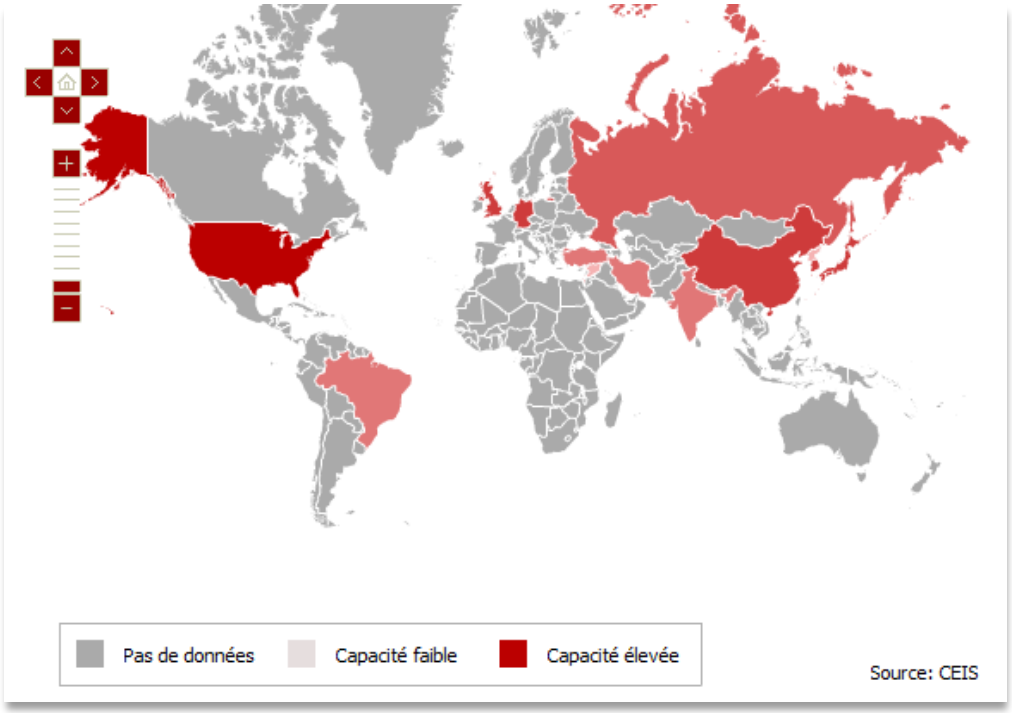

Figure 3 - Carte mondiale sur le portail OMC

Méthodologie

L'analyse des capacités cybernétiques de chaque pays s'articule autour de cinq critères, dont la pertinence a déjà été éprouvée dans les nombreux rapports annuels de l'OGI.

Rubrique	Quelques exemples de thématiques
Infrastructures	Connectivité internationale, points d'échange, FAI, taux de pénétration Internet…
Capacités scientifiques et techniques	Centres de recherche, normalisation…
Base industrielle et technologique	Composants électroniques, hardware informatique, industrie logicielle…
Sécurité des systèmes d'information	Gestion des événements sécurité (lutte informatique défensive), outils et technologies de sécurité, bonnes pratiques…
Sécurité et gouvernance des réseaux	Cadre juridique, forces de police, écosystème cybercriminel et hacktiviste…
Capacités de cyberdéfense	Stratégie, prises de position politiques, règles d'engagement, unités militaires dédiées, budgets, exercices et entrainements…

Les fiches pays sont accessibles en permanence sur le portail. Chaque critère d'analyse est associé à un marqueur visuel, indicateur de capacité cybernétique.

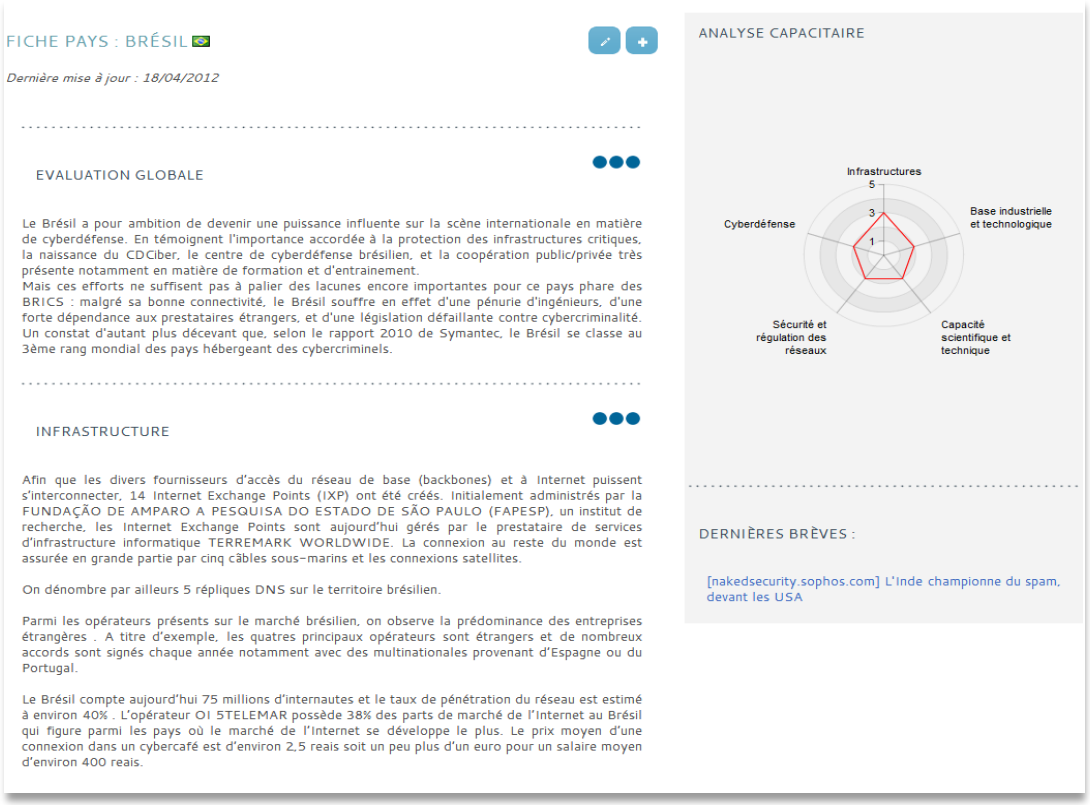

Figure 4 - Fiche pays du portail OMC

Pour vous y connecter, n'hésitez pas à demander vos identifiants à CEIS.

Contact : Barbara Louis-Sidney - blouis@ceis.eu et omc@ceis.eu

L'ANSSI prépare la seconde version du RGS

L'ANSSI publiera une deuxième version du RGS (Référentiel Général de Sécurité) afin de l'adapter à ses nouvelles missions. L'Agence compte notamment assouplir la directive quant à l'usage unique des clés privées d'authentification spécifié dans la première version du RGS.

Free veut gérer les .fr à la place de l'AFNIC

Free a annoncé son partenariat avec la start-up Starting Dot et lance Frnic, afin de remplacer l'AFNIC pour la gestion de noms de domaine français. Cette annonce fait suite à l'appel à candidatures de l'ICANN sur les nouveaux TLD (*Top Level Domain*).

Selon le président estonien, le principal enjeu de la cyberguerre n'est pas militaire

Le président estonien, Toomas Hendrik Ilves, a affirmé, au cours d'un discours aux Etats-Unis, que le principal enjeu de la cybersécurité n'était pas militaire, mais économique. Paraphrasant Bill Clinton, il a déclaré *« It's the economy, stupid »*, soulignant que la cybercriminalité constituait une menace importante pour une économie fondée sur la propriété intellectuelle.

Un rapport du *Commerce Department's* chiffre à 40 millions le nombre d'emplois reposant sur cette économie.

Le Royaume-Uni serait mal préparé en cas de cyberattaque

L'ancien directeur du GCHQ a déclaré que le Royaume-Uni était moins protégé contre les cyberattaques que ses alliés américains, français ou allemands.

Il attribue ces faibles capacités à un manque de coordination entre les différentes agences, et pense que de meilleurs résultats seraient possibles avec davantage de centralisation. Il salue la prise de conscience des décideurs politiques qui ont augmenté les budgets alloués à la cybersécurité.

Le retard de la Suisse en matière de lutte anti-cybercriminalité constaté

Le cinquième congrès informatique de la police suisse a mis en avant le manque d'effectifs dans la lutte contre la cybercriminalité, le besoin d'harmonisation des démarches et le besoin de partenariats publics/privés. Helmut Picko, chef du centre de compétences *Cybercrime* de l'office de police judiciaire de Rhénanie du Nord/Westphalie, constate une professionnalisation toujours plus accrue des cybercriminels, qui n'est cependant pas accompagnée d'une protection adéquate des grandes infrastructures sensibles.

L'Union européenne doit investir d'avantage en technologies de cybersécurité

Neelie Kroes, commissaire européenne en charge de la société numérique, a annoncé lors de la conférence *Infosecurity Europe* à Londres que l'Union européenne devrait investir d'avantage dans les technologies permettant de sécuriser le cyberespace européen et encourager l'innovation en matière de cybersécurité.

La NSA investit dans le « *Big Data* »

Une partie des 250 millions de dollars investis par le Pentagone dans la cybersécurité visera à donner à la NSA une capacité de cassage de code utilisant des technologies privées de *Big Data*. Ces technologies seront aussi utilisées pour découvrir des tendances hostiles (ou APTs) parmi de gigantesques banques de données, ou encore tisser des liens entre les données de différents services d'intelligence.

Le Pentagone se dote de procédures de développement de cyberarmes

Selon un rapport remis au Congrès, le Pentagone souhaite augmenter ses capacités de développement de cyberarmes. Deux processus de développement sont envisagés. Le premier est rapide, permettant de mettre au point une cyberarme en quelques jours grâce à une réutilisation de code.

Le second est plus long, de l'ordre de quelques mois, et concernerait le développement de cyberarmes sur-mesure, adaptées à un objectif précis.

CISPA, un projet de loi sur la cybersécurité controversé

Un projet de loi américain, CISPA *(« Cyber Intelligence Sharing and Protection Act »)* a pour objectif d'assurer la cybersécurité du territoire américain en facilitant l'échange d'informations entre agences fédérales et entreprises privées. D'après l'EFF (*Electronic Frontier Foundation*), le CISPA ne serait pas suffisamment précis dans sa définition des « cybermenaces » et pourrait permettre aux entreprises d'espionner ses utilisateurs et de partager les informations obtenues avec les agences fédérales.

L'US Air Force veut développer un système de communication plus sécurisé

L'US Air Force a rassemblé des scientifiques venant de sept universités américaines pour développer un moyen de communication plus sécurisé. Disposant d'un budget de 8.5 millions de dollars pour 5 ans, le projet va se concentrer sur les propriétés des photons intriqués - domaine de la physique quantique.

Exercices de cyberguerre entre la Chine et les Etats-Unis

Deux exercices de cyberguerre auraient eu lieu entre la Chine et les États-Unis, un troisième étant d'ores et déjà prévu courant mai. Ces entrainements sont destinés à limiter le risque d'escalade si l'un des deux pays s'estime victime d'une cyberattaque. Ces « rencontres » sont organisées dans un cadre assez informel par deux *think tanks*, le *Center for Strategic and International Studies* (CSIS) et le *China Institute of Contemporary International Relations*, autorisant une certaine liberté aux participants. Le premier exercice consistait pour chaque équipe à décrire sa réaction en cas d'attaque sophistiquée de type Stuxnet. Pour le second exercice, les équipes devaient décrire leur réaction en cas d'attaque venant de l'équipe adverse.

Focus sur la stratégie chinoise dans le cyberespace

La Chine refuse de dépendre d'autres pays pour les technologies dites « critiques », et considère le système actuel injustement favorable aux États-Unis, puisqu'elle estime être la plus grande victime de cybercrimes. D'après l'auteur de l'article, la Chine poursuivrait une stratégie cohérente, en utilisant des *hackers* « patriotes », en contrôlant étroitement les informations sur Internet et en proposant aux Nations unies un Code de Sécurité de l'Information. Ce que l'auteur de l'article qualifie de *« plus grand transfert de richesse de l'histoire »* vers la Chine (par le vol de données) devrait être considéré avec la plus haute attention par les autorités.

L'Iran chercherait à « purifier » Internet

Selon un document traduit du persan à l'anglais, le ministère iranien des communications cherche l'aide d'entreprises nationales pour « purifier » Internet. Pour certains, cet appel à proposition infirmerait la rumeur selon laquelle l'Iran envisagerait de se couper du réseau Internet, car le gouvernement ne chercherait pas à censurer le réseau s'il souhaitait s'en déconnecter. Cependant, des experts préviennent qu'il est possible qu'un réseau national performant coexiste avec un Internet lent et filtré.

Des terminaux pétroliers iraniens hors-service à cause d'un virus

Un virus informatique aurait contraint l'Iran à mettre certaines installations hors-service dans le terminal pétrolier de Kharg, par lequel passe environ 90% des exportations du pays. Il s'agirait d'une mesure de précaution, car le cœur du système n'aurait pas été atteint. L'agence de presse Mehr, citant un officiel sous couvert d'anonymat, précise que l'attaque n'a pas causé de dommage. Le ministère du pétrole a reconnu avoir été victime d'un piratage, mais nie toute fuite de données.

L'Inde commande du matériel de guerre électronique

Le gouvernement indien a commandé à la société canadienne Ultra Electronics du matériel de guerre électronique pour un montant de 3,4 millions de dollards. Le contrat porte notamment sur du matériel de cryptage et de surveillance des télécommunications. La livraison au *Defence Avionics Research Establishment* (DARE) de Bangalore est prévue pour fin 2013.

Vers une course aux cyber-armements ?

Plusieurs experts américains en cybersécurité ont affirmé lors d'une conférence à l'Université de Georgetown qu'une « course aux armements » avait actuellement lieu sur Internet. Ils ont appelé à une meilleure collaboration entre les différentes agences américaines et avec les entreprises du secteur et les pays alliés. Steven Schleien, l'un des directeurs du programme « cyber » au Pentagone, a déclaré que les États-Unis avaient pris contact avec les autorités japonaises, sud-coréennes, néo-zélandaises, britanniques et australiennes, afin d'établir une politique de cyberdéfense commune.

Guerre et paix dans le cyberespace

Joseph S. Nye, ancien assistant du secrétaire à la Défense des États-Unis et professeur à Harvard, défend dans son dernier ouvrage, « The Future of Power », que le cyberespace renforce les menaces asymétriques. La force militaire et financière des grandes puissances ne serait plus suffisante pour maintenir leur hégémonie, et les acteurs non-étatiques sont appelés à jouer un rôle de plus en plus important dans les relations internationales. Au *« cyber-Pearl Harbor »* évoqué par Leon Panetta, il préfère un *« cyber-11 septembre »*, selon lui beaucoup plus probable. Après avoir réfléchi sur les définitions possibles de la cyberguerre, il dégage quatre catégories de menaces : la cyberguerre et l'espionnage industriel seraient plutôt l'apanage des États, alors que le cybercrime et le cyber-terrorisme sont plutôt pratiqués par des acteurs non-étatiques.

Le risque d'un effet boomerang dans l'usage des cyberarmes

Plusieurs experts en sécurité alertent sur les dangers de l'usage de cyberarmes telles que Stuxnet. Le risque que cette arme soit retournée contre ses créateurs est débattu : le nombre d'acteurs capables de réutiliser le code de Stuxnet par exemple est très restreint, mais le danger existe. Le véritable risque est que la publication d'un virus aussi abouti démontre qu'il est possible d'atteindre un tel objectif. Stuxnet servirait alors de « guide » pour d'autres projets similaires partout dans le monde.

Les réseaux sociaux peuvent représenter des risques pour les opérations militaires

La société Imperva a publié un rapport dans lequel des chercheurs mettent en garde contre les risques liés aux informations publiées sur les réseaux sociaux pour les États. Des soldats, ou des familles de soldats, peuvent publier involontairement des informations de localisation ou de mouvement de troupes, comme ce fut par exemple le cas en 2011 lorsque Tsahal a annulé une opération après qu'un soldat en ait parlé sur Facebook. Les réseaux sociaux peuvent également servir à comprendre la hiérarchie et le fonctionnement de certaines agences, ainsi qu'à élaborer des « phishing » plus efficaces.

[ENISA] Guide sur la gouvernance de service *Cloud*

L'ENISA a publié un guide pratique sur la mise en place et la gouvernance de services de *Cloud Computing*.

Son objectif est d'améliorer la qualité des services *Cloud* que se procurent les secteurs privés et public, en leur permettant de poser les bonnes questions aux prestataires qu'ils seront amenés à rencontrer.

[GCN] Guide pour la création d'un système de gestion de clés cryptographiques

Le National Institute of Standards and Technology (NIST) américain a publié un guide pour la création d'un système de gestion de clés cryptographiques - problème critique de la sécurisation des données.

Son objectif est de standardiser la méthode avec laquelle les entités publiques gèrent leur infrastructure de clés cryptographiques, pour une meilleure homogénéité de la sécurité globale.

[cso.com.au] Websense 2012 Threat Report

Selon le rapport 2012 de Websense Security Labs, les attaques les plus répandues sont les leurres au sein de réseaux sociaux (extrêmement efficaces), les *malwares* évolutifs et difficiles à repérer, ainsi que les exfiltrations sophistiquées de données confidentielles.

L'immense majorité des attaques utilisent les sites visités, les mails consultés, ainsi que l'ingénierie sociale comme vecteurs principaux.

Selon le rapport, les défenses traditionnelles des SI doivent être complètement revues afin de lutter contre ce type de menaces.

[bit9.com] Bit9 publie une étude sur la cybersécurité en 2012

Le groupe Bit9 a enquêté auprès de 1800 professionnels en Europe et aux États-Unis. Les résultats de cette étude sont très instructifs : seulement 26% des personnes interrogées se sentent en sécurité sur leur ordinateur. Bit9 précise qu'aux yeux des interrogés, les principales menaces sont : les hacktivistes de type Anonymous, les cybercriminels classiques et les États.

La société Imperva a réagi aux résultats de cette étude sur son blog. Elle s'étonne de l'importance accordée aux hacktivistes au détriment de menaces non moins dangereuses, comme les injections SQL, qui ne sont redoutées que par 4% des personnes interrogées. Imperva rappelle que cette technique est pourtant utilisée dans la majorité des fuites de données.

[Government Computer News] HP publie un rapport sur la cybersécurité en 2011

HP revient, dans un livre blanc, sur les principaux risques en matière de cybersécurité en 2011. Le rapport souligne la persistance de failles anciennes, dont certaines ne sont toujours pas corrigées. La diminution du nombre de failles découvertes - de 11000 en 2006 à environ 6600 en 2011 - ne serait donc pas due à une amélioration du niveau de sécurité des SI.

Le rapport revient également sur les tendances en matière de vulnérabilités et d'attaques en 2011.

[sophos.com] Sophos publie une étude sur les menaces en 2012

Dans ce rapport d'une trentaine de pages, les chercheurs de Sophos passent en revue les menaces de 2011 et annoncent les menaces à venir : hacktivisme, menaces sur les Mac, *Cloud*, terminaux mobiles, DLP, etc.

La stratégie de cyberdéfense russe – Dissuader, prévenir, résoudre… et contre-attaquer ?

Le 10 février 2012, le Ministère de la défense russe publiait en ligne un document intitulé *« Points de vue conceptuels sur les activités des Forces armées de la Fédération de Russie dans l'espace d'information »*. Retour sur ce document présenté comme la nouvelle stratégie de cyberdéfense de la Russie.

Une réponse à la stratégie américaine publiée en 2011

La stratégie russe est axée sur trois concepts phares : **dissuader**, **prévenir** et **résoudre** les conflits armés dans le domaine numérique. Si elle n'aborde pas l'éventuelle conduite d'opérations militaires offensives dans le cyberespace par les forces armées russes, elle envisage clairement la mise en œuvre de la **légitime défense** ; c'est-à-dire la possibilité de répondre aux cyberattaques en utilisant des moyens militaires tant informatiques que conventionnels.

Il s'agit là d'une véritable réponse à la stratégie américaine prévoyant elle aussi la riposte. Le 16 mai 2011, la Maison Blanche dévoilait en effet ses règles de conduite militaires en matière de cyberattaques. Le document précisait que les Etats-Unis *« répondront aux actes hostiles dans le cyberespace de la même manière qu'à toute autre menace pour le pays. […] [Ils se réservent] le droit d'utiliser tous les moyens nécessaires – diplomatiques, relatifs à l'information, militaires et économique – en fonction des besoins et dans le respect du droit international, pour défendre [leur] pays, [leurs] alliés, [leurs] partenaires et [leurs] intérêts ».*

Notons également que, si la Russie prévoit clairement la riposte aux cyberattaques, elle s'applique à préciser que cette riposte se fera **en accord avec les normes et principes de droit international**. Seraient donc pris en compte les problèmes d'attribution, d'identification et de seuil d'intensité posés par la notion d'agression. A l'image du principe d' *« équivalence »* développé par les Etats-Unis, permettant de jauger la proportionnalité de toute réponse à une cyberattaque.

Le document confirme également la tendance à la **régionalisation du cyberespace**. Malgré sa volonté de donner à l'ONU un rôle essentiel dans la régulation du cyberespace, la Russie, qui n'a pas signé la Convention de Budapest de lutte contre la cybercriminalité, précise vouloir approfondir sa coopération avec les pays de l'Organisation du Traité de sécurité collective (OTSC), de la Communauté des Etats indépendants (CEI) et de l'Organisation de coopération de Shanghai (OCS).

Positionnement militaire ou civil ?

Cette stratégie ne fait pas mention, en apparence tout du moins, du cyberespace comme le 5ème espace de bataille. La vision russe est centrée sur la **guerre de l'information**, ce qui englobe à la fois la guerre électronique, le renseignement, les opérations psychologiques, l'influence et les opérations dans le cyberespace.

Le fait que cette stratégie soit publiée par le Ministère de la Défense russe (et non par le Service fédéral de sécurité de la Fédération de Russie (FSB), jusque-là principal interlocuteur en matière de conflits

informatiques), marque cependant un revirement important, soulignant l'implication désormais directe de la Défense et des armées russes dans les cyberconflits.

Un document encore largement conceptuel ?

Malgré son caractère ambitieux, le document reste assez flou : il consiste en l'énumération de concepts généraux[1], sans préciser les moyens de mise en œuvre d'une telle stratégie. A titre d'exemple, les forces armées russes fonderont leurs activités dans le cyberespace sur six principes : la légitimité (agir en accord avec le droit international), la priorité (veille, recueil d'informations, analyse et développement), la coordination (participation des états-majors à tous les niveaux), l'interaction (participation d'organes fédéraux du pouvoir exécutif), la coopération (à l'échelle internationale) et l'innovation (technologique).

Mais quel sera le budget consacré ? Quels moyens humains seront mis en œuvre ? Quelles infrastructures seront dédiées à son application ? Les évènements ayant suivi la publication du document apportent des éléments de réponse et témoignent de l'engagement de la Russie sur la question de la cybersécurité :

- La Russie a annoncé sa volonté de créer un cyber commandement, suivant ainsi *« l'exemple des Etats-Unis et de l'OTAN » ;*
- Dmitri Medvedev a déclaré que l'une des priorités pour l'année 2012 était la création d'un nouveau « système de contrôle des forces armées », « *unifié dans un seul espace informatique basé sur des technologies de l'information et de la communication innovantes »* ;
- Enfin, le Ministère des Affaires étrangères de Russie a récemment créé un poste de spécialiste en sécurité de l'information, un poste qui aura un rôle diplomatique important. Selon les dernières informations, Andreï KROUTSKIKH avait été nommé à ce poste. Il a auparavant été directeur adjoint du département de risques opérationnels du ministère des Affaires étrangères.

En l'état, le document reste un acte fort de communication et de dissuasion. Et il est probable qu'il ne soit que la version publique d'une stratégie probablement classifiée, plus complète et opérationnelle.

Critères	Sous-critères	Contenu
Doctrine globale	**Publications**	• Stratégie présentée par le Ministère de la Défense de la Fédération de Russie : *« Points de vue conceptuels sur les activités des Forces armées de la Fédération de Russie dans l'espace d'information »* (élaborée en 2011, publiée en 2012) ; • Cette stratégie s'appuie sur la *« Doctrine sur la sécurité informatique de la Fédération de Russie »* (approuvée le 9 septembre 2000 par le Président Vladimir Poutine ; • Et sur la *Doctrine militaire de la Fédération de Russie*, approuvée par le décret présidentiel de 5 Février, 2010.
	Prises de position politiques	• La Russie place toujours la **dimension psychologique** des conflits informatiques au cœur de sa stratégie de cyberdéfense. La sécurité informatique n'est pas définie uniquement comme la sécurité du contenant mais également comme la sécurité des contenus, avec tout ce que cela peut entraîner en termes de censure sur Internet ; • La Stratégie de 2012 a pour objectif de **prévenir la course aux cyber-armements et résoudre les conflits** armés dans l'espace de l'information (ou cyberespace) (Doctrine militaire, 2010, page 17) ; • Cette stratégie prévoit d'expliquer publiquement, en cas de conflit dans l'espace de l'information, les causes et les origines de ce conflit à la communauté internationale.
	Positionnement militaire ou civil ?	• Jusque-là, on ne retrouvait pas chez les stratèges russes le caractère très martial du concept américain de *cyberwar*. Et il n'est pas fait mention, en apparence tout au moins, du cyberespace, 5ème espace de bataille ; • La vision russe était centrée sur la **guerre de l'information**, ce qui englobe, comme dans la vision chinoise, à la fois la guerre électronique, le renseignement, les opérations psychologiques, l'influence et les opérations dans le cyberespace ; • La stratégie de 2012 met en lumière **six axes** en vertu desquels les forces armées russes pourront assurer la sécurité et la défense du cyberespace russe : légitimité, priorité, complexité, interaction, collaboration et innovation (voir *infra* pour plus de précisions) ; • Le fait que cette stratégie soit publiée par le Ministère de la Défense russe (et non par le FSB, jusque-là principal interlocuteur en matière de conflits informatiques) marque un revirement important et souligne l'implication désormais directe de la Défense et des armées russes dans les cyber-conflits.
Axe défensif	**Dissuasion**	• La publication de cette stratégie constitue en elle-même un acte fort de dissuasion. Elle prévoit en effet la mise en œuvre de mesures de prévention des conflits, ainsi que l'usage de la légitime défense en cas de conflit.
	Renseignement – anticipation – prévention – détection	• Le renseignement et l'anticipation tiennent une place importante dans la stratégie russe. Une des priorités est d'améliorer leur lutte contre la *« propagande informatique et psychologique »* d'adversaires potentiels (Doctrine, 2000) ; • En vertu du **principe de priorité**, la Russie envisage le recueil d'informations pertinentes sur les menaces, le traitement et l'analyse de ces données ; • Les autorités russes prendront en effet toutes les mesures possibles pour assurer la **détection précoce** d'éventuels conflits militaires dans le cyberespace. Ils identifieront également les organisateurs de ces conflits, les instigateurs et les complices ; ainsi que les facteurs de survenue de ces conflits ; • *« La politique militaire de la Fédération de Russie vise à prévenir une course aux armements, la dissuasion et la prévention des conflits militaires … »* (Doctrine militaire, 2010, page 17).

Critères	Sous-critères	Contenu
Axe défensif	**Protection / SSI des infrastructures critiques**	• En vertu du **principe de priorité**, la Russie envisage le développement de mesures de protection de ses SI. Notamment des SI des Forces armées elles-mêmes ; • Elle envisage d'améliorer la circulation de l'information entre les différentes entités.
	Lutte contre la cybercriminalité ordinaire	• La Russie intègre la lutte contre la cybercriminalité classique dans sa stratégie. Par exemple, dans le cadre du programme fédéral *« Internet sécurisé »* lancé en 2012, le Ministère de l'Intérieur russe souhaite distribuer des brochures afin d'informer les citoyens russes sur les cybermenaces ; • Le département K (luttant contre la criminalité informatique) du Service fédéral de sécurité (FSB) a constaté une forte augmentation de plaintes dans le domaine de la cybercriminalité.
	Résilience – amélioration des réseaux – investigation et *forensic*	• La Russie fait de la lutte contre la vulnérabilité de ses SI une priorité. En ce sens, elle souhaite améliorer les *« méthodes de l'investigation stratégique et opérationnelle »* (Doctrine, 2000) ; • La Russie envisage le développement d'un système visant à résoudre et contenir les conflits armés dans l'espace de l'information (Stratégie, 2011) ; • La Russie souhaite prendre des mesures pour **neutraliser les facteurs donnant lieu à tout conflit** en vue de l'interaction directe entre les parties en conflit allant dans le sens d'une coopération constructive ; • La stratégie prévoit également la mise en œuvre de mesures d'urgence.
	Cyberdéfense active	• La Russie reconnait le droit à l'exercice de la légitime défense en matière de lutte informatique (voir le principe de légitimité, critère *« cadre juridique » infra*) ; • *« La Fédération de Russie considère qu'il est légitime d'utiliser les forces armées et autres troupes pour repousser l'agression contre elle et (ou) ses alliés et maintenir la paix d'après la décision du Conseil de sécurité, d'autres institutions de sécurité collective, ainsi que de protéger ses citoyens, en dehors de la Fédération de Russie conformément aux principes et normes généralement reconnues du droit international et des traités internationaux de la Fédération de Russie » (Doctrine militaire de la Fédération de Russie, approuvée par le décret présidentiel, 5 Février 2010, p 20) ;* • C'est ce principe militaire à portée générale qui est transposé au cyberespace dans la Stratégie de 2012 ; • Ainsi, en cas de conflit dans l'espace d'information et de transition vers une phase de crise, la Russie se réserve le droit d'exercer le droit de légitime défense, individuelle ou collective avec tous les moyens choisis, moyens ne contredisants pas aux normes et principes universellement reconnus du droit international ; • La proportionnalité de la riposte sera étudiée : La Russie souhaite *« déterminer la capacité requise de la réponse sur la base de procédures démocratiques nationales, en tenant compte des intérêts légitimes de la sécurité d'autres Etats, ainsi que la nécessité pour la sécurité et la stabilité internationales » ;* • La Russie s'appuiera sur des moyens et « forces de sécurité informatique » qu'elle déploiera sur les territoires d'Etats « amis », conformément aux accords internationaux en vigueur.

Critères	Sous-critères	Contenu
Axe offensif	Règles d'engagement	• NC* • Le document n'aborde pas explicitement la conduite d'opérations militaires offensives dans le cyberespace ; • Mais la Russie semble s'orienter vers une utilisation de l'arme informatique dans le respect des règles internationales dans le cadre de la légitime défense.
	Autre (seuils d'intensité admis)	• NC* • Le conflit informatique est en général perçu par les autorités russes comme principalement clandestin dans le cadre d'affrontements de basse intensité ou en appui d'opérations conventionnelles ; • Le document publié en 2012 ne donne pas d'informations sur le sujet. Mais puisque la Russie semble s'orienter vers une utilisation de l'arme informatique dans le respect des règles internationales dans le cadre de la légitime défense, elle devra justifier d'un seuil d'intensité minimal afin de se prévaloir de la légitime défense.
Aspects techniques		• Le **principe d'innovation** met en avant la conception et l'utilisation des technologies de pointe, d'outils et de méthodes avancés, élaborés dans des **centres d'innovation de la Fédération de Russie.**
Cadre juridique		• En vertu du **principe de légitimité** développé dans la Stratégie de 2011, les forces armées doivent agir conformément aux normes et principes de la législation russe actuelle ainsi qu'aux normes et principes du droit international. • Ainsi, d'après l'artide 20 de la Doctrine militaire russe, le recours aux forces armées en temps de paix se fait par la décision du Président de la Fédération de Russie. • En ce qui concerne le droit international, il est indispensable, selon les autorités russes, de respecter : - la souveraineté d'un Etat ; - la non-ingérence dans les affaires intérieures d'un autre Etat ; - les droits à la légitime défense individuelle et collective.

Critères	Contenu
Coopération internationale	• Le pays n'a pas signé la Convention de Budapest sur la cybercriminalité, considérant que celle-ci ne respecte pas les principes de souveraineté des Etats et de non-ingérence dans les affaires intérieures d'un autre Etat ; • La coopération avec les forces étrangères est limitée ; • Mais le **principe de la coopération** développé dans la stratégie (2012) souligne que les forces armées russes coopéreront avec forces des pays alliés et des organisations internationales ; • La Russie coopérera prioritairement avec les pays du Traité de sécurité collective (OTSC)[1], la Communauté des Etats indépendants (CEI)[2] et l'Organisation de coopération de Shanghai (OCS)[3] ; • Elle élargira le cercle de partenaires sur la base d'intérêts communs conformément aux dispositions de la Charte des Nations Unies et d'autres normes du droit international ; • Le développement de cette coopération au niveau mondial pourrait se faire notamment à travers la mise en place d'un régime juridique international : un traité dans le cadre de l'ONU visant à assurer la sécurité au plan international et étendant l'application de normes généralement reconnues et aux principes du droit international dans le cyberespace. → Voir à cet égard le code de bonne conduite proposé par l'OCS à l'ONU.
Budget	• NC*
Organisation	• Le **principe de complexité** évoqué dans la Stratégie russe implique la participation des états-majors et du commandement dans l'organisation des activités dans le cyberespace en temps de paix et en temps de guerre ; • Le **principe de l'interaction** exige du Ministère de la Défense russe qu'il coordonne ses activités dans le cyberespace avec d'autres organes fédéraux du pouvoir exécutif.
Formation et entrainement – ressources humaines	• La Russie souhaite mettre à disposition de ces opérations du personnel hautement qualifié dans le domaine de la cybersécurité ; • La Russie envisage de déployer des « *forces de sécurité informatique* » (Stratégie 2012) sur son propre territoire, mais aussi sur les territoires de pays « amis ». S'agit-il d'un début de coopération en matière d'opérations militaires offensives ? Ce point n'est pas abordé dans la stratégie russe.

* NC : « non communiqué » : pas d'informations disponibles.

[1] Organisation à vocation politico-militaire regroupant la Russie, la Biélorussie, l'Arménie, le Kazakhstan, le Kirghizistan, l'Ouzbékistan et le Tadjikistan.

[2] Entité intergouvernementale composée de 11 des 15 anciennes républiques soviétiques : Biélorussie ; Russie ; Kazakhstan ; Arménie ; Ouzbékistan ; Tadjikistan ; Kirghizistan ; Moldavie ; Azerbaïdjan ; Ukraine (État participant) ; Turkménistan (État associé) ; Mongolie (État observateur).

[3] Organisation intergouvernementale régionale asiatique regroupant la Russie, la Chine, le Kazakhstan, le Kirghizistan, le Tadjikistan et l'Ouzbékistan

TakeDownCon 2012	Houston (USA)	8 – 10 mai 2012
Annual AusCert Information Security Conference	Victorie (Australie)	13 – 18 mai 2012
IEEE Symposium on Security and Privacy 2012	San Francisco (USA)	20 – 23 mai 2012
Conférence ISO 31000 sur le management des risques	Paris	21 – 22 mai 2012
CEIC 2012	Summerlin (USA)	21 – 24 mai 2012
Challenge Hacknowledge RSSIL	Maubeuge	2 – 3 juin 2012
Conférence Octopus : coopération contre le cybercrime	Strasbourg	6 – 8 juin 2012
North America CACS	Orlando (USA)	7 - 10 Mai 2012
Integralis Security World	Boulogne	7 juin 2012
Hack In Paris	Paris	18 – 22 juin 2012
CyberDefence 2012 SMI Group	Londres	18 -19 juin 2012
The 1st International Conference on Cyber Crisis Cooperation - Cyber Exercises	Paris	27 juin 2012

CEIS

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

Les opinions exprimées dans cette lettre n'engagent que la responsabilité de leurs auteurs.

Retrouvez cette lettre et l'ensemble des articles cités sur notre extranet
https://owldesk.ceis.eu/
(Accès soumis à authentification)

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07