Lettre n°62 - Mai 2017 - disponible sur omc.ceis.eu

Brève du mois

« The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits »[1] - Brad Smith, directeur des affaires juridiques de Microsoft.

Table des matières

[1] https://techcrunch.com/2017/05/14/microsofts-response-to-widespread-cyber-attacks-may-make-you-wannacry/

L'ABSTRACTION DE CONCEPTS CYBER : UNE REPONSE A LA PENURIE DE COMPETENCES ?

Dans le domaine de la cybersécurité et de la cyberdéfense, tous les Etats et organisations sont confrontés à la même difficulté : les compétences, notamment techniques, disponibles sur le marché ne permettent pas de répondre à la demande. Un grand écart qui résulte du développement continu de la cybercriminalité et de la compétition capacitaire des Etats.

La première réponse à ce défi est bien entendu celle de l'automatisation, qui se voit aujourd'hui renforcée par le développement de l'apprentissage machine (*machine-learning*). Mais entre la ressource humaine et l'automatisation quasi-complète, non réaliste, il existe un concept intermédiaire qui peut être considéré comme une étape : l'abstraction des concepts cyber au profit de solutions permettant de diminuer le palier de formation nécessaire à la lutte informatique. Ceci sera rendu possible par l'association d'une sémantique définissant les concepts propres au cyberespace (entités, évènements, actions, etc.), d'interfaces intuitives de visualisation et d'interaction avec le cyberespace, et enfin de capacités analytiques et opérationnelles adaptées au cyberespace.

Quels sont les effets de la mise au point de systèmes permettant une nouvelle couche d'abstraction cyber ?

L'exemple des langages de programmation

Dans le domaine informatique, l'abstraction des concepts de programmation occupe une place centrale. Un langage de programmation est déjà une abstraction, puisqu'il fait correspondre à un langage binaire un langage intelligible pour l'être humain. Dans ce secteur, une grande étape a été franchie avec les langages de programmation haut-niveau, qui ont permis la croissance fulgurante du secteur. On est ainsi passé du programmeur, qui avait pour mission de traduire un algorithme en un langage directement applicable par la machine, au développeur, qui manipule des concepts haut-niveaux et n'a besoin que d'une compréhension très superficielle de nombreux concepts sous-jacents. Sans l'automatisation d'un certain nombre de tâches (telle que la gestion de la mémoire), et l'utilisation d'éléments de langage naturel (si… alors…, etc.), la programmation logicielle représenterait un coût tel que ce que l'on appelle la transition numérique n'aurait pas pu avoir lieu.

De façon analogue, l'abstraction a continué sous différentes formes, y compris visuelles. Ainsi, de nombreux langages de programmation visuelle[2] ont émergé pour des besoins spécifiques : éducation (à la programmation), multimédia, simulation, programmation d'automates, etc. Il ne s'agit plus de rédiger du code en langage pseudo-naturel, mais de construire un programme à partir de blocs visuels qui remplissent une fonction propre.

[2] https://en.wikipedia.org/wiki/Visual_programming_language

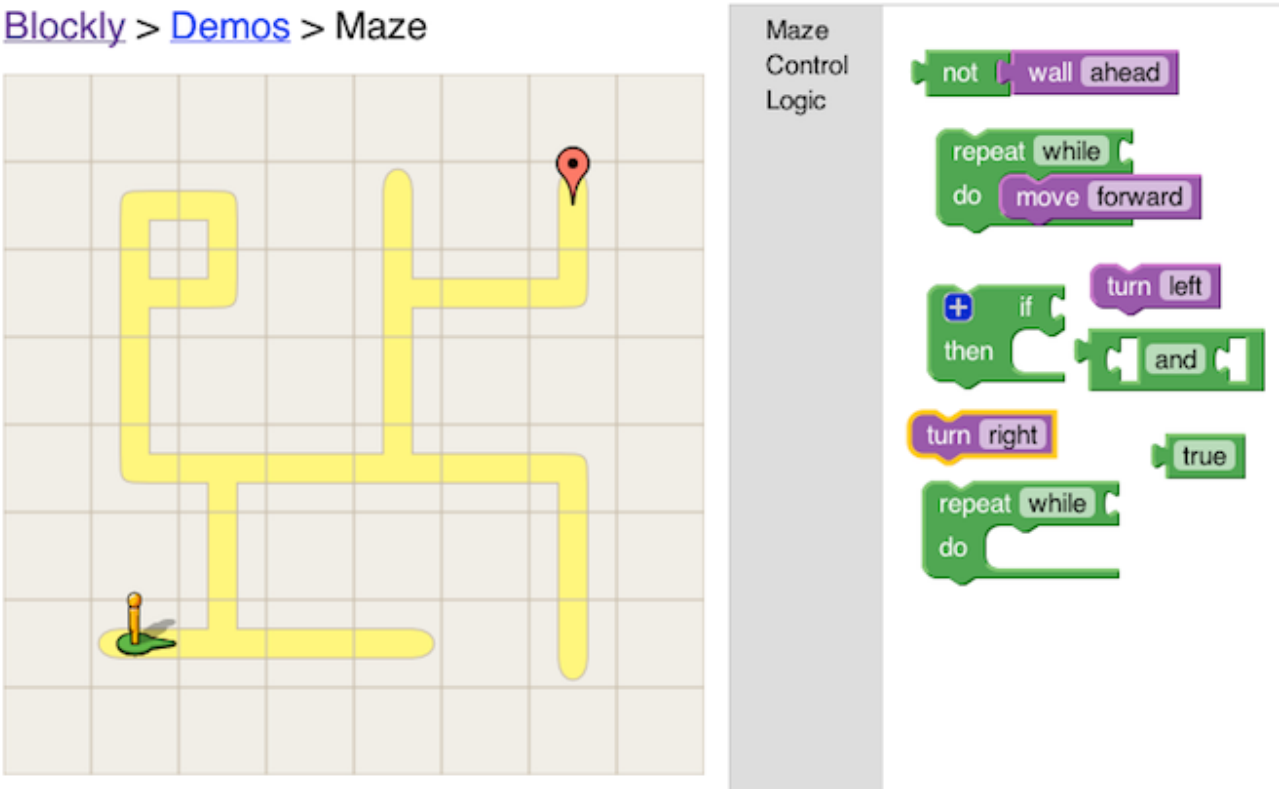

Figure 1 : Exemple de programmation d'une méthode de résolution de labyrinthe avec le langage de programmation visuelle Blocky

L'abstraction au service des moyens de lutte informatique

L'abstraction des concepts cyber permet deux choses :

- Apporter la perception de situation (*situational awareness*), à différents niveaux (technique, stratégique) ;
- Permettre d'opérer sur un réseau et ses systèmes, de façon défensive ou offensive.

Ce concept est développé par la DARPA depuis 2013, dans le cadre d'un premier projet appelé Plan-X qui arrivera à son terme à la fin de l'année 2017[3]. Celui-ci vise à offrir un modèle de données exploitable de façon visuelle, d'une façon analogue à la façon de penser les relations entre les objets physiques. Le développement de ce concept doit accompagner les objectifs de recrutement de professionnels de la cybersécurité du Pentagone.

A cette fin, un des objectifs de Plan-X est de réduire sérieusement les prérequis en termes de formation : ainsi, la perception de situation du cyberespace doit être facilitée par une représentation visuelle intuitive – et intelligible au plus grand nombre – qui doit donc transcender les *dashboards* et autres interfaces d'administration traditionnels. Pour mener à bien leurs opérations, il est question d'éviter aux cyber-soldats de devoir rédiger ou de modifier directement des lignes de codes. On élimine ainsi le besoin pour eux d'en maîtriser toutes les ficelles. Pour y parvenir, Frank Pound, *Project Manager* de Plan-X, indique que son

[3] https://www.fbo.gov/utils/view?id=49be462164f948384d455587f00abf19

équipe s'est fortement inspirée des outils de formation issues de la Silicon Valley, et notamment d'un langage de programmation visuelle appelé Scratch[4]. A l'instar de ce type de programme, le cyber-soldat prépare ses opérations à l'aide de blocs visuels d'instructions préprogrammées issus d'une librairie partagée. La nature graphique d'une telle programmation se rapprocherait ainsi de la planification militaire, à travers la visualisation du plan de bataille.

Figure 2 : Planification de mission. Source : Powerpoint de présentation de Plan X de la DARPA

Les questions de représentation opérationnelle intuitive des réseaux ont beaucoup été mises en avant lors des diverses présentations du projet. Cependant, avant de pouvoir définir des représentations visuelles des entités, des évènements et des opérations cyber, il doit exister des termes spécifiques pour les définir. D'autant plus que Plan X doit se nourrir, comme les systèmes SIEM[5], de l'information d'intérêt cyber disponible en provenance notamment des différents éléments réseaux : il est donc préférable que ceux-ci parlent autant que possible le même « langage ».

Dans cet optique, l'agence a suivi les travaux du MITRE sur les standards de définition et d'échange d'information de Cyber Threat Intelligence. Ces standards, CybOX, STIX et TAXII, ont depuis été transférés à l'OASIS CTI TC (OASIS Cyber Threat Intelligence Technical Commitee).

[4] https://www.defense.gov/News/Article/Article/758219/darpas-plan-x-gives-military-operators-a-place-to-wage-cyber-warfare/
[5] Security information management system

STIX (Structured Threat Information Expression) est un langage et un format permettant d'exprimer de façon structurée de l'information de type Cyber Threat Intelligence, ceci afin de permettre son partage, son échange et son analyse de façon uniforme. STIX intègre maintenant CybOX (Cyber Observable eXpression), qui est un langage standardisé de caractérisation d'évènements ou de propriétés d'objets du cyberespace. Enfin, TAXII (Trusted Automated eXchange of Indicator Information) est un protocole de transport sécurisé des données STIX.

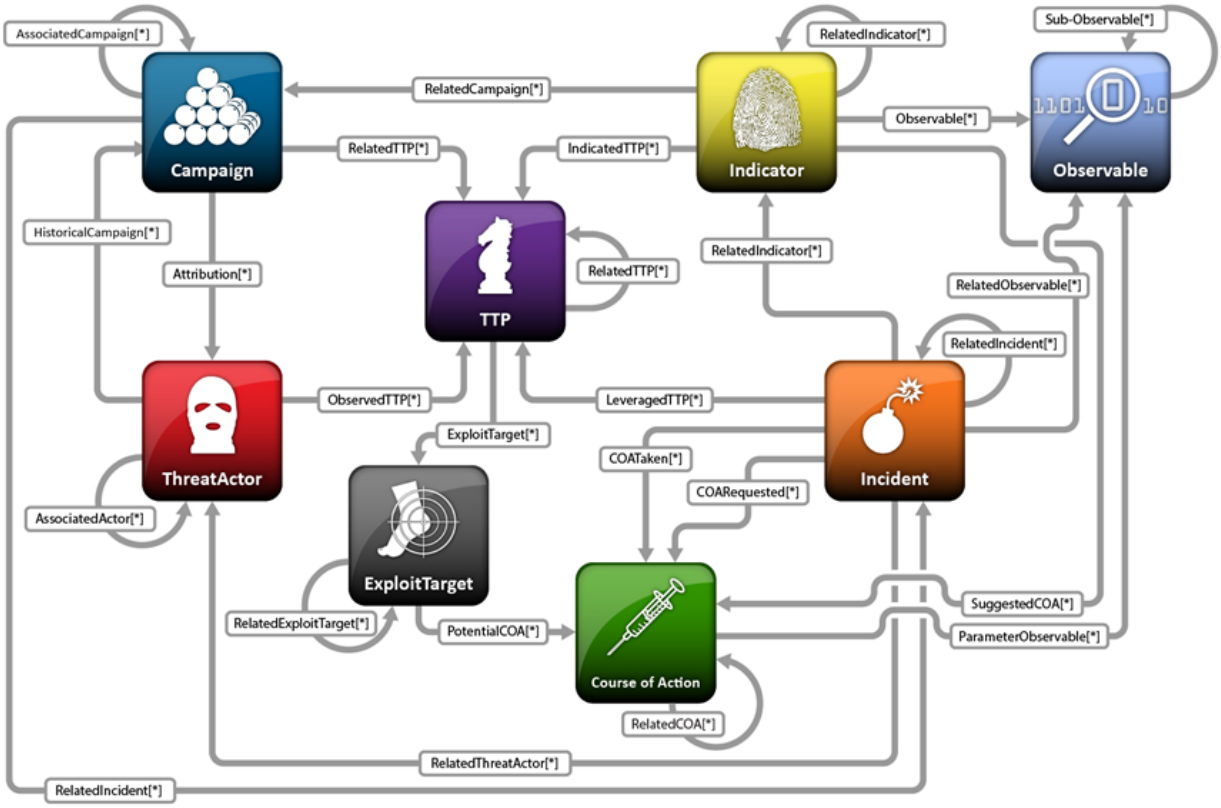

Figure 3 : Diagramme d'architecture du modèle STIX, qui possède 8 modèles principaux.

Cette définition sémantique des évènements et des entités (matériel, logiciel et humain) du cyberespace, offerte par ce langage commun, constitue les fondations nécessaires de tout système permettant une accessibilité renforcée du métier de cyber-défenseur et de cyber-soldat.

La place de l'intelligence artificielle

L'intelligence artificielle est au cœur de ce changement de paradigme annoncé. Plan X est avant tout un framework qui nécessite de s'appuyer sur de fortes capacités analytiques. L'un des cinq domaines techniques du programme, appelé Cyber Battlespace Analytics dans l'appel d'offre de la DARPA, correspond donc au développement de techniques d'analyse automatique visant à faciliter la compréhension humaine de l'espace de bataille.

Le support de l'intelligence artificielle devient incontournable pour permettre notamment, en tenant compte du contexte de mission :

- Le découpage topographique des réseaux considérés ;
- La détection des menaces ;
- L'attribution des attaques ;
- L'interprétation des commandes.

Des réseaux de neurones aux moteurs d'inférence en passant par la compréhension du langage naturel, le succès des systèmes de pilotage tels que Plan X dépendra des progrès de ces sous-domaines de l'intelligence artificielle et de leur application aux problématiques du cyberespace.

Plan X étant entré dans sa dernière année, la DARPA travaille actuellement avec les forces armées au transfert du projet vers un programme commun à la disposition de l'ensemble des unités cyber. Concrètement, il s'agit d'un système constitué d'un environnement d'exécution léger sur poste client, qui est supporté par une solution serveur. Celle-ci se nourrit notamment des données de Threat Intelligence remontées par les solutions de cybersécurité du DoD. Pour cette raison, on peut s'attendre à une accélération de l'adoption des standards STIX et TAXI par l'armée américaine, ainsi que par les agences civiles. La technologie développée est intégralement GOTS (Government Off-The-Shelf) et basée sur des outils open-source. Elle a donc vocation à être adaptée aux agences civiles, mais également à avoir des applications commerciales : tous les projets de la DARPA doivent en effet produire des technologies à double usage.

L'adoption de STIX, déjà bien avancée[6], sera bénéfique au fonctionnement de l'application dans sa dimension défensive. Cependant, l'adoption ou non de ce standard n'a pas d'implications pour la dimension offensive des programmes qui seront dérivés de Plan X. Rappelons que la DARPA n'est jamais en charge de développer des capacités purement offensives, celles-ci étant le fruit de projets ultérieurs faisant suite au transfert des technologies vers le DoD et les entreprises privées.

Il y a fort à parier que le DoD appuiera l'adoption des programmes issus de Plan X, et que ceux-ci accéléreront le développement des technologies de *Machine Learning* appliquées au cyberespace, technologies encore balbutiantes aujourd'hui. Ces programmes permettront de tirer parti des autres

[6] https://wiki.oasis-open.org/cti/Products

investissements en matière cyber et d'en amplifier leurs effets et leur utilité auprès d'un plus grand nombre d'opérateurs.

La mise au point de programmes de visualisation et d'opération dans le cyberespace opérera un changement de paradigme similaire à ce qu'a représenté le développement des langages de programmation haut-niveau. En effet, ces systèmes nécessiteront des capacités de calculs extrêmes pour porter l'intelligence artificielle sous-jacente. En donnant un avantage certain aux grandes organisations, et notamment aux Etats, cela remettra en question l'asymétrie des rapports de force permise par le cyberespace aujourd'hui.

LES DONNEES, NOUVEL ENJEU GEOPOLITIQUE ?

Souvent qualifiées de « nouvel or noir », les données constituent désormais un véritable enjeu de pouvoir entre les Etats qui veulent s'assurer le contrôle sur celles qui circulent sur leur territoire, et entre les entreprises privées qui fournissent les réseaux qu'elles empruntent. Véritable richesse immatérielle, nouveau capital virtuel, l'intérêt qu'elles suscitent reflète bien les transformations que connaît la géopolitique à l'ère numérique : remise en cause des frontières physiques nationales, affirmation d'acteurs privés et non étatiques, « numérisation/digitalisation » des conflits (revendications de souveraineté sur le cyberespace, attaques informatiques) Outre l'information elle-même, c'est en effet la façon dont les données sont générées (et par qui), dont elles circulent, et la façon dont elles sont stockées, qui font des données une ressource précieuse. Maîtriser la donnée suppose de maîtriser ses moyens et ses conditions de production, ses canaux de transmission, et son mode et son lieu de stockage. La donnée, ainsi créatrice de valeur et de pouvoir « fait le lien entre espaces physiques et numériques. »[7] Elle est au cœur de l'interpénétration de deux univers qu'a priori tout oppose, la géopolitique qui s'intéresse aux rapports de force entre Etats en tant qu'entités délimités par des frontières nationales, et le monde virtuel du cloud computing qui présente par définition un caractère transnational et s'affranchit des frontières physiques. En s'imposant comme un élément central des relations internationales, elle reconfigure les rapports de forces sur la scène internationale et donne lieu à de nouvelles représentations de souveraineté.

Les données, au centre de nouveaux enjeux de souveraineté.

Les données au cœur du cyberespace

Les données, omniprésentes dans un monde bouleversé par la transformation numérique, participent à la redéfinition des territoires et à l'émergence d'espaces d'échanges et d'interactions d'un type nouveau. Les données sont en effet au cœur du cyberespace, ce nouveau territoire virtuel et sans frontières, cet « espace d'information généré par l'interconnexion globale des systèmes d'information et de communication, dans lequel les données sont créées, stockées et partagées »[8] et qui constitue désormais le cadre des échanges et communications internationales. Un espace qui comprend non seulement l'infrastructure physique sur lequel repose cet environnement, c'est à dire les différentes composantes de l'internet (câbles, serveurs, routeurs, les satellites, appareils connectés, datacenters), mais aussi l'espace virtuel et immatériel dans lequel circulent l'information et les données.[9] Un espace dont les frontières sont difficile à établir, puisque si celles de l'ancrage physique du cyberespace – son réseau d'infrastructures– sont relativement bien délimitées, celles de la couche virtuelle et informationnelle dans lequel circulent les données sont en revanche plus difficile à définir. L'exemple le plus significatif est sans doute celui des systèmes autonomes, ces ensembles de réseaux IP liés par une politique de routage commune et indépendante sans ancrage territorial aucun, et dont les frontières sont juridiques et contractuelles plus que géographiques. Mouvantes et dynamiques, les frontières du cyberespace restent donc toujours à établir. Comme les frontières

[7] Internet. Géopolitique de la donnée. Maîtriser la donnée : enjeux et défis géopolitiques. Moteurs de recherche et web profond, Thierry Berthier
[8] Cyberespace, un enjeu géopolitique, Frederick Douzet
[9] Idem

physiques d'un territoire, elles seront le fruit des rapports de forces entre acteurs qui y cherchent leur place et sont déjà aujourd'hui à l'origine de nouvelles tensions et disputes interétatiques. Comme tout nouveau territoire, le cyberespace est en effet un territoire à conquérir, à contrôler, à surveiller, à se réapproprier, sur lequel il faut faire respecter sa souveraineté, ses lois et ses frontières, c'est à dire les limites de l'espace sur lequel s'exerce la souveraineté nationale.[10]

Les données, à l'origine de représentations rivales de la souveraineté.

Or dans ce nouveau contexte, la notion de souveraineté fait l'objet de représentations divergentes qui opposent les acteurs qui y opèrent. Certains comme les Etats-Unis ou l'Europe considèrent le cyberespace comme un espace autonome, « un objet exclusif incomparable qui nécessiterait ses propres règles de gouvernance ».[11] D'autres comme la Russie ou la Chine privilégient au contraire une conception du cyberespace comme un « espace informationnel », une simple prolongation numérique des États sur lequel doit s'appliquer les lois nationales de la même façon que sur le reste du territoire. Pour les premiers le cyberespace transcende les frontières étatiques et doit faire l'objet d'une régulation dédiée au niveau international ou supranational. Pour les seconds le cyberespace doit au contraire être rattaché à un territoire national et soumis aux lois de l'Etat auquel il est rattaché, la souveraineté de chaque État se manifestant donc par la territorialisation et la nationalisation d'un segment du cyberespace. Ainsi la Russie revendique sa mainmise sur le Runet sur la base d'une communauté de langue, de pratiques et de valeurs.[12] Pourtant, même dans un monde excessivement numérisé, les partisans d'une conception d'un cyberespace autonome détaché des frontières nationales ne peuvent faire l'économie d'un ancrage territorial qui semble à ce jour être le seul moyen d'y affirmer sa souveraineté et d'exercer une influence dans la gouvernance du cyberespace.

De nouveaux acteurs font concurrence aux Etats

C'est par le biais de géants industriels du numérique pour lesquels les données constituent à la fois la matière première et le moteur économique que la puissance américaine étend son influence et son contrôle au-delà de ses frontières nationales. Car la maîtrise de la donnée confère à des acteurs privés un rôle et un poids jusque-là inégalé permettant aux géants du numérique de défier les Etats dans ce qu'ils ont de plus précieux, leur souveraineté. Ce n'est pas tant le chiffre d'affaires de Google, dont la valeur correspond au PIB de pays comme la Suède ou la Norvège, qui fait de la société américaine un géant géopolitique. C'est surtout le fait que ses datacenters détiennent des données collectées auprès d'utilisateurs dans le monde entier, que même installés hors des Etats-Unis ils échappent aux législations et autorités de leurs pays d'accueil tout en restant ouverts aux agences fédérales et au système judiciaire américains, et que grâce à des techniques d'optimisation fiscale, ces sociétés réussissent à ne reverser qu'une partie de leurs revenus aux Etats dans lesquels sont installés leurs datacenters. Ces sociétés viennent ainsi directement concurrencer les Etats hôtes dans l'exercice de certaines prérogatives régaliennes : le contrôle sur les informations des administrés, la gestion de leurs identités numériques, leur capacité à mettre en œuvre leurs politiques de lutte contre le crime et le terrorisme, ou encore le prélèvement des impôts.

[10] Idem
[11] Limonier Kevin, « La Russie dans le cyberespace : représentations et enjeux »
[12] Idem

L'émergence de nouveaux acteurs en mesure de rivaliser d'égal à égal avec les Etats, dans un espace numérique où les frontières et le contrôle de territoires virtuels sont en pleine définition, pose aussi la question de la gouvernance de l'Internet.

La maitrise des données et le défi de la gouvernance

La gouvernance d'Internet, c'est à dire l'ensemble des dispositifs permettant aux acteurs du cyberespace d'agir de façon coordonnée et de prendre des décisions consensuelles sur la gestion de ce territoire mi-virtuel mi-physique, revêt à la fois des aspects formels (lois, régulations, protocoles), mais aussi des règles, normes et standards plus informels. En l'absence de consensus sur une gouvernance globale ou supranationale, la régulation du cyberespace est aujourd'hui le fruit d'une combinaison de juridictions et souverainetés nationales et n'est soumis au droit international que dans le cadre de mesures de confiance et de normes non contraignantes de comportement responsable des Etats. Dans les faits, ce sont les règles américaines relatives à la gouvernance d'Internet qui se sont jusque-là imposées et appliquées dans tous les pays dans lesquels sont présents les géants américains du Web.

De l'extra-territorialisation au colonialisme numérique

La soustraction des datacenters localisés hors du territoire des Etats-Unis aux lois et autorités des pays dans lesquels ils sont installés constitue la forme la plus visible et la plus contestée de l'extra-territorialité du modèle américain de gouvernance d'Internet. Mais d'autres formes, plus informelles mais non moins efficaces, de ce que d'aucuns qualifient de « colonialisme numérique » sont également à l'œuvre, notamment via les moteurs de recherche des géants du Web. Ainsi, ceux de Google, Bing et Yahoo, représentent 99% du marché de la recherche en ligne en Europe, monopolisant les portes d'entrée de l'Internet et s'imposant ainsi comme « les relais du soft power américain ». [13] L'influence exercée par les géants du web se manifeste également de façon encore plus subtile, via la standardisation mondiale des interfaces, via par exemple le bloc de recherche de Google, la page perso de Facebook ou le pack Windows Office, qui permettent de diffuser « le message universaliste des Etats-Unis, convaincus d'avoir développé des modèles et des valeurs démocratiques qui peuvent s'appliquer à toutes les sociétés."[14] En réponse à ses pratiques, et par volonté de se soustraire à l'influence américaine tout en développant des solutions nationales capables de servir de relais d'influence sur d'autres zones géographiques, des alternatives russes et chinoise ont également vu le jour via Baidu, utilisé par plus de 500 millions d'internautes depuis une centaine de pays, et Yandex, qui détient plus de 60% des parts du marché national russe. L'affrontement dans le cyberespace se superpose à la compétition géopolitique existante entre les puissances, faisant du territoire numérique un « septième continent » théâtre d'affrontements d'un nouveau genre, combinaison de défense de la souveraineté nationale et de recherche d'extra-territorialité et d'influence.[15] Les prétentions extraterritoriales des Etats-Unis sont d'ailleurs devenues un point d'achoppement récurrent avec les Etats qui s'y voient soumis de facto, notamment les pays européens qui ont depuis quelques années entrepris une démarche inverse de « reterritorialisation ».

---

[13] Les Etats et la tentation de l'extraterritorialité
http://www.huffingtonpost.fr/charlesedouard-bouee/les-etats-et-la-tentation-de-extraterritorialite_b_6308190.html
[14] Idem
[15] Idem

Entre reterritorialisation et relocalisation.

En imposant l'application hors de leur territoire de normes et standards sur la régulation d'Internet, notamment ceux relatives à l'utilisation et à la (très limitée) protection des données personnelles, les Etats-Unis s'assurent en effet de la primauté de leurs propres normes et standards en matière de confiance et de protection des données, et s'octroient un levier d'influence considérable sur la gouvernance de l'Internet. Désireux de se libérer de cette tutelle, les Etats qui s'y voient soumis tentent désormais de « reterritorialiser » la régulation du cyberspace. Ils exigent notamment que la réglementation et le cadre légal dont dépendent les datacenters soient déterminés par leur localisation et non par la nationalité de la société à laquelle ils sont rattachés. Une démarche destinée à permettre aux Etats concernés de conserver la maîtrise des données produites et stockées sur leur territoire et à faire appliquer et respecter leurs propres standards en matière de protection des données. C'est aussi l'objectif du Privacy Shield qui encadre désormais le transfert de données entre l'Europe et les Etats-Unis et impose à ces derniers d'offrir aux données européennes stockées sur leur territoire un niveau de protection au moins équivalent à celui prévu par les législations européennes. Certains États travaillent également à des législations obligeant leurs entreprises, notamment les prestataires Cloud, à stocker leurs données sur le territoire national pour s'assurer que les données qu'ils contiennent ne soient accessibles qu'à leurs propres autorités et ne relèvent pas de la compétence d'un État concurrent. Par exemple, une loi russe de 2018 oblige les entreprises russes diffusant des contenus sur le web à conserver pendant un an sur le territoire russe les données relatives aux appels, messages textuels, photos, vidéos, et à les fournir aux agences gouvernementales qui les réclament. Les projets de Clouds souverains, destinés à soustraire les États concernés à la mainmise de géants du Net en grande majorité américains, participent de la même démarche.

Les données, par l'information qu'elles véhiculent et les infrastructures physiques qu'elles empruntent pour circuler, incarnent donc parfaitement la dualité du cyberespace, à la fois virtuel et physique. Elles concentrent ainsi tous les enjeux géopolitiques traditionnellement associés à la maîtrise d'un territoire : souveraineté, indépendance et gouvernance. Sources de tensions entre puissances reconnues et acteurs émergents sur la scène internationale, elles ne se contentent pas de transposer dans l'espace numérique des rivalités géopolitiques préexistantes mais génèrent également de nouvelles formes de conflictualité. Et tant qu'il n'existera pas de cadre normatif global ou de règles définies et acceptées par tous régulant l'Internet, la gestion de ces conflits de souveraineté et d'indépendance sur le cyberspace fera inévitablement l'objet d'une reterritorialisation destinée à re-ancrer les données dans un cadre territorial pour mieux les maîtriser et les contrôler.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** 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 **DGRIS** a confié à **CEIS** la réalisation de 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
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis.eu