

La régulation des contre-mesures contre les cyber-attaques

Philippe BAUMARD

Professeur des universités, Université d'Aix-Marseille

Chaire Innovation & Régulation des Services Numériques, École Polytechnique

Résumé : La régulation du cyberspace constitue un effort international où se croisent intérêts publics, privés et souverains. En analysant le cas particulier de la régulation des contre-mesures, et la difficulté à obtenir la ratification d'un accord international sur le sujet, nous soulevons le problème de l'inadéquation du cadre de régulation face aux ruptures technologiques actuelles et à venir dans le domaine de la cyber-défense. L'article souligne en particulier la nécessité d'ancrer la réflexion sur la régulation dans le corps des sciences cognitives et comportementales, et dans le domaine du machine-à-machine.

Mots clé : cybercrime, accord international, régulation, ONU

En juin 2010, un code malicieux fut introduit dans le logiciel d'un composant *hardware* de la firme allemande Siemens destiné à intégrer le système de contrôle et d'acquisition de données (SCADA) d'un site d'enrichissement d'uranium à Natanz, en Iran. Ce code malicieux exploitait quatre vulnérabilités de Windows WinCC, dont on ignorait encore l'existence (vulnérabilité dite « *zero day* » ou « zéro jours »). Ce code malicieux permettait d'établir une communication externe, et de déclencher une instruction visant à paralyser, puis saboter, l'installation nucléaire dont il avait fait cible. Bien qu'une telle attaque ne constituât pas une première, elle possédait quelques caractéristiques qui ne sont pas étrangères au réveil des négociations internationales sur la régulation de la cyberdéfense en général,

et des contre-mesures, en particulier¹. Stuxnet est ce qu'on appelle une campagne de menace avancée persistante, ou *Advanced persistent threat* (APT). De telles cyberattaques sont ainsi nommées parce qu'elles reproduisent le comportement d'une attaque complexe, intelligente, avec des capacités de raisonnement et de déclenchement de commandes autonomes ou pilotées à distance. Cette famille de menaces n'est pas caractérisée par une technologie particulière, ni par une génération ou une typologie spécifique de technologies. Ses caractéristiques sont la programmation comportementale autonome (leur capacité à adapter leurs attaques), leur adaptabilité, et leur persistance (après une période de reconnaissance de leurs cibles, elles ont pour objectif de compromettre un système en y résidant de manière anonyme, ou en trompant la vigilance des systèmes de détection en augmentant leurs privilèges). Leur caractérisation s'établit plus sur la subtilité de leurs stratégies de raisonnement, que sur leur force brutale, jusqu'à éventuellement mobiliser Sherlock Holmes pour en décrire les stratégies d'attaque !²

Stuxnet avait pour objectif de reprogrammer, à des fins de sabotage, les contrôleurs logiques (PLCs) de la centrale nucléaire. Il était notamment capable d'autoréplication (en déclenchant sa propre installation à partir de supports externes amovibles), de s'exécuter à distance à travers un partage en réseau, de se mettre à jour par un réseau de *peer-to-peer*, de prendre le contrôle du centre de commandes, de cacher ses propres traces binaires, d'identifier les produits de sécurité résidant sur le réseau, de modifier puis de cacher les codes sabotés directement sur les contrôleurs industriels (PLCs) de Siemens³.

Cette dernière caractéristique, l'autoréplication associée à une élévation astucieuse de privilège, est une des causes de la formidable prolifération du Stuxnet, qui infecta près de 100 000 machines entre le jour de sa découverte (le 25 janvier 2010, si on ne prend pas en considération les versions dormantes de 2009), et le 29 septembre 2010, dont 14 sites industriels iraniens, et plus de 60 000 hôtes en Iran seulement⁴. Par son ampleur, la

1 Pour une documentation technique, cf. N. Fallière, Lima O. Murchu et Eric Chien (2011), *W32.Stuxnet Dossier*, Symantec. [http://www.h4ckr.us/library/Documents/ICS_Events/Stuxnet%20Dossier%20\(Symantec\)%20v1.4.pdf](http://www.h4ckr.us/library/Documents/ICS_Events/Stuxnet%20Dossier%20(Symantec)%20v1.4.pdf)

2 Pour une analyse détaillée de stratégies d'attaques utilisant des scénarios inspirés du héros fictif de Sir Conan Doyle, lire : Juels Ari and Ting-Fang Yen., "Sherlock Holmes and the case of the advanced persistent threat", *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET'12)*, USENIX Association, Berkeley, CA, USA, 2012.

3 Falliere *et al.* (2011), *op. cit.* p. 1.

4 Falliere *et al.* (2011), *op. cit.* p. 5.

sophistication de sa construction qui peut effectivement signer l'œuvre d'un État, ou de la coopération entre plusieurs États, Stuxnet est ainsi identifiée comme l'événement débutant la première cyber-guerre globale⁵. Stuxnet est un révélateur de la *possibilité* d'une guerre, mais surtout un très efficace démonstrateur des failles « systémiques » de l'industrie et des gouvernements : les systèmes de détection fondés sur l'identification des signatures de codes malveillants (repérage de codes malicieux dans un trafic de données) étaient inopérants face aux attaques intelligentes de ce type ; et le degré d'automation de Stuxnet (qui fut repéré par une entreprise de sécurité biélorusse car les machines n'arrêtaient pas de se relancer et de se mettre à jour !) faisait voler en éclat le sentiment de quiétude quant à une « sécurité maîtrisée ». Schouwenberg, qui fut à la tête de l'équipe de Kapersky ayant contribué à défaire Stuxnet, était sincèrement impressionné par l'élégance de sa programmation, qui combinait l'exploitation croisée de quatre vulnérabilités « zéro jours »⁶ avec des déclencheurs logiques particulièrement astucieux. La cyberguerre devenait une réalité palpable, et le cyberspace un domaine physique⁷ avec des conséquences sociétales et stratégiques facilement mesurables. Et comme dans *Le Rivage des Syrtes* de Julien Gracq, rien ne donne plus envie aux hommes de faire la guerre qu'un faible signal lumineux sur une rive éloignée.

Ce chapitre s'intéresse à un enjeu de la régulation du cyberspace qui concerne aussi bien les États que les entreprises, et qui, comme nous le verrons, est amené à se retrouver au cœur de nombreux conflits (commerciaux, économiques, armés) au XXI^e siècle. Il s'agit du domaine de la contre-mesure envers les cyberattaques. Les « contre-mesures » sont des réponses que l'on oppose à une action ou un événement de façon à les interdire, les prévenir ou enrayer leur prolifération à leur source. Ces trois modes

5 James P. Farwell & Rafal Rohozinski (2011), « Stuxnet and the Future of Cyber War », *Survival: Global Politics and Strategy*, 53 (1), p. 23-40, et pour un récapitulatif : Lindsay, J.R. (2013), « Stuxnet and the Limits of Cyber Warfare », *Security Studies*, Volume 22, Issue 3, pages 365-404.

6 Kushner, D. (2013), « The Real Story of Stuxnet », *IEEE Spectrum*, Vol 50, Issue 3, p. 48-53.

7 La doctrine du cyberspace comme « domaine physique » a été initiée aux États-Unis par Daniel Kuehl en 1997 : « *Information as an environment may be a difficult concept to grasp, but there is no arguing that there is a physical environment to which information is uniquely related: cyberspace. Cyberspace is that place where computers, communications systems, and those devices that operate via radiated energy in the electromagnetic spectrum meet and interact.* » Daniel Kuehl, « Defining Information Power, » *Strategic Forum*, no. 115 (June 1997) : 3.

de réponses impliquent une posture très différente. Les contre-mesures « d'interdiction » peuvent se contenter de mettre fin, *hic et nunc*, à une opération malveillante. C'est ce que font les logiciels de sécurité identifiant un code malicieux (« virus »), l'isolant, le plaçant en quarantaine, pour éventuellement le supprimer. Les contre-mesures dites de « prévention » vont enregistrer et caractériser ce comportement malicieux (par sa signature, sa reconnaissance comportementale) et s'assurer qu'il soit stoppé dès sa détection. Les réponses apportées à Stuxnet entrent dans ces deux premières catégories. Finalement, les contre-mesures dites « actives » ou « contre-offensives » vont prolonger cette interdiction temporaire par une recherche active de sa source d'émission afin de procéder à sa neutralisation.

DÉSACCORDS SUR LA CONTRE-MESURE ET SA LÉGITIMITÉ

Dans ce dernier cas, il n'existe pas de régulation internationale globalement ratifiée, en 2013, permettant d'établir quelles sont les règles d'engagement, les fondements de la légitimité de telles contre-mesures, et ne serait-ce même qu'un accord de principe entre les nations sur l'idée que la proportionnalité et la « contre-offensive » puissent être légalement justifiées⁸. Les contre-mesures peuvent être soit de nature logicielle, soit de nature humaine, et le plus souvent composée de ces deux types d'intervention. Une contre-mesure logicielle est un ensemble de lignes de commandes déclenché à partir d'un système de détection reposant sur un raisonnement analytique programmé (intelligence artificielle, corrélation statistique, bayésiens, etc.). La contre-mesure « humaine » consiste à mener le travail d'investigation et d'enquête (audit, *forensics*) par des moyens qui peuvent être humains (*social engineering*, entretiens, enquêtes sous couvert) ou informatiques (traçage inverse du chemin d'attaque, tests de pénétration, etc.). Cette seconde partie peut impliquer de retracer le chemin d'une attaque qui est passée par des serveurs physiquement localisés dans un ou plusieurs pays étrangers.

Le problème pourrait être anodin, ou devenir la simple prolongation des traités internationaux encadrant la criminalité, la guerre, les trafics humains et le grand banditisme si la nature même de l'information et des systèmes d'information ne rendait pas impossible cette simple évolution.

D'une part, il est difficile d'établir une destination criminelle *a priori* d'un système d'information, ou d'une information elle-même. Par exemple, le recours au secret et au chiffrement peut être une garantie du respect des

8 Dieter Fleck, (2012) "Searching for International Rules Applicable to Cyber Warfare — A Critical First Assessment of the New Tallinn Manual", *International Journal of Conflict & Security Law*, 18 (2) : 331-351.

[p. 177-195]

Philippe BAUMARD

Arch. phil. droit 56 (2013)

libertés individuelles et de l'anonymat tout autant que le signe d'une activité criminelle. De fait, les lanceurs d'alerte utilisent les mêmes technologies que les organisations criminelles pour rendre anonymes leurs communications et échanges (*Tor network*, « *darkpools* »). Le « cyberlibertaire », le « *whistle-blower* », le « résistant », le « rebelle » ou le « cyberterroriste » sont souvent une même personne selon qu'on la perçoit d'un côté différent de la barrière. On ne peut pas identifier l'intention de malveillance à partir de « l'arme » en possession du « cyberattaquant » pour la bonne et simple raison qu'une commande utilisée sur un réseau n'est pas une arme. Leur combinatoire complexe peut en devenir une, mais les techniques d'offuscation de code (qui consiste à masquer un code dans une forêt de codes placebo mais non pour autant dénué de sens) et de chiffrement sont si librement accessibles que le travail d'audit et d'investigation scientifique d'un code complexe peut prendre plusieurs semaines. Une approche fonctionnelle et typologique du caractère offensif ou criminel d'une information ou d'un système d'information est donc vouée à l'échec⁹.

D'autre part, l'architecture même des systèmes d'information, pour des raisons d'efficience, n'est pas délimitée par ses finalités mais par la performance d'opérations qui peuvent être distribuées, parcellaires, partagées, voire « fragmentées » de façon aléatoire des systèmes *peer-to-peer*. Dès lors, la géographie de l'information, de sa destination comme de sa création, devient le résultat d'un processus technique qui va permettre de dissimuler, que cela soit intentionnel ou pas, son origine, son but, sa chronologie et son propriétaire¹⁰.

ANONYMAT, ATTRIBUTION ET PREUVE D'INTENTIONNALITÉ

La difficulté réside dans l'interprétation de la *responsabilité* des différentes parties prenantes (opérateurs de télécommunications, États, fabricants de logiciels, etc.) dans *l'expression finale* qui peut résulter de ces cheminements complexes d'information. Dans l'article 32 de la Convention de Budapest (2001), l'obligation de communication d'information revient à la personne qui en a l'autorité légale ; mais est-ce la personne qui a accédé à cette

9 Talbot-Jensen, Eric (2010) "Cyber Warfare and Precautions Against the Effects of Attacks", *Texas Law Review*, Vol. 88, p.1533-1570.

10 Van Eeten Michel, Albert Nieuwenhuijs, Eric Luijff, Marieke Klaver & Edite Cruz (2011) "The State And The Threat Of Cascading Failure Across Critical Infrastructures : The Implications Of Empirical Evidence From Media Incident Reports", *Public Administration*, 89 (2), p. 381-400.

information ? Celle qui a fourni le moyen de transport ? Celle dont le pays est à l'origine du robot logiciel qui a assuré l'échange anonyme de pair-à-pair (P2P) de cette information ? Et dans le cas d'une attaque robotique, doit-on punir le fabricant du robot, le ou les différents pays ayant laissé ce robot opérer, ou simplement le dernier utilisateur « conscient » de ce robot ?... ou le robot lui-même ? (Interdiction par la catégorisation du logiciel robotisé en « arme de guerre »).

Ce travail de réflexion est mené par le Conseil de l'Europe, qui coordonne l'évolution de la Convention de Budapest sur le cyber crime de 2001, signée par 60 pays ; mais avec, selon l'UNODC, plus d'un tiers de la population mondiale en situation de connectivité, et une prévision de connectivité à 70 % de la population planétaire en 2017, la question des « contre-mesures » et de l'autorité à les conduire devient un enjeu qui dépasse de très loin la problématique de la coopération transfrontalière. La duplication ou la transposition par allégorie (maritime, territoriale, spatiale) d'un droit international *quelconque* à un droit de la cyber-défense est illusoire, sinon utopique.

Avec plus de 70 % des communications mondiales en 2013 étant de machine-à-machine sans intermédiation humaine, il peut être dangereux, du point de vue de la simple efficacité du droit, d'attribuer à ce monde de machines les règles d'encadrement et de contrôle du crime humain. D'autre part, la vitesse des microtransactions, la célérité avec laquelle une attaque peut être métamorphosée en une soixantaine de ses variantes, ne laissent aucune *avance* au législateur, à l'exécutif et aux forces de l'ordre pour résoudre des enquêtes judiciaires si les règles du jeu sont celles de la criminalité courante¹¹. Le problème est alors double : on ne peut exercer la loi car elle n'aura aucun terrain viable d'exercice, et lorsque ce terrain est rendu possible, on ne peut financer son déploiement ou le simple devoir d'enquête. Que ce soit en Europe, aux États-Unis, en Russie, en Chine, en Afrique ou au Brésil, très peu de cas de « cybercrimes » ont été effectivement traités par le système judiciaire, et beaucoup moins sont sanctionnés¹². Les mécanismes de coopération judiciaire, d'enquête et de police sont très souvent inopérants en matière de cybercriminalité, non pas par déficit de talents, - car contre une idée reçue les forces de l'ordre disposent de talents

11 Geers Kenneth (2010), "The challenge of cyber attack deterrence", *Computer Law & Security Review*, Volume 26, Issue 3, p. 298-303.

12 Goldsmith, Jack (2013), "How Cyber Changes the Laws of War", *European Journal of International Law*, Volume 24, Issue 1, p. 129-138.

décisifs dans ce domaine --, mais par le caractère impraticable de la coopération technique sur la cybercriminalité¹³.

Partager un « cas » de cybercriminalité revient à partager une vulnérabilité de son système de défense car la frontière de l'innovation bouge à chaque cas. Dès lors, si un État coopère avec un autre, il refusera de le faire sur les « zéro jours » (attaques dont la faille n'a pas été *identifiée*), de peur de révéler à d'autres États son état de l'art défensif, son réel degré de maîtrise de la cyberdéfense, voire une faille de cybercriminalité qui pourrait être exploitée à d'autres fins (espionnage d'État, cyberguerre). Le « zéro jour » est tout autant une vulnérabilité avouée dans ses propres défenses que la concrétisation d'une opportunité offensive, si l'on possède la solution pour résoudre, ou si l'on peut exploiter cette vulnérabilité chez un adversaire¹⁴. Comme chaque acteur cherche à créer des asymétries décisives face à des puissances étrangères qui ne sont pas toujours bienveillantes, il n'existe aucune incitation à divulguer une information sur ce type de vulnérabilités et de possibilités d'exploitation de failles. Dès lors, il est impossible aujourd'hui de résoudre ou répondre à une attaque d'origine transfrontalière (dont le cheminement implique plusieurs pays), tant l'accès transfrontalier à la donnée *réelle* est difficile¹⁵. Il ne s'agit pas ici des données elles-mêmes de l'attaque (le code de celle-ci), mais aussi les données concernant ses moyens de transport, les serveurs sur lesquels elle a pu laisser des traces exploitables, les machines qui ont, même involontairement, servi de vecteurs de diffusion et d'attaque¹⁶.

Contrairement aux armements traditionnels, les « armes » cybernétiques, mis entre guillemets tant cette expression est abusive, ne font pas l'objet d'une manufacture spécifique, d'un numéro de série, ou de l'utilisation d'outils de production spécialisés. L'énergie motrice d'une attaque, son « fuel » pour prendre une analogie anglo-saxonne, peut par exemple résider dans la bande passante que le système d'attaque a pu capturer. Il s'agit des

13 cf. Demchak, Chris C. et Peter J. Dombrowski (2011), "Rise of a Cybered Westphalian Age", *Strategic Studies Quarterly* 5, no. 1 p. 31-62.

14 Li, Frankie and Anthony Lai (2011), "Evidence of Advanced Persistent Threat: A case study of malware for political espionage", *6th International Conference on Malicious and Unwanted Software Proceedings*, p. 102-109.

15 Denning Dorothy (2000), « Reflections on Cyberweapons Controls », *Computer Security Journal*, 16 (4), p. 43-53.

16 Brunst, Phillip : "Legal Aspects of Cyber terrorism", in Centre of Excellence – Defence Against Terrorism (ed.) : *Legal Aspects of Combating Terrorism*. Amsterdam, IOS Press, NATO Science for Peace and Security Series, 2008, p. 63-76.

attaques en DDoS¹⁷ dont l'objectif est de générer un emballement de requêtes sur les machines visées afin de provoquer leur panne par saturation. Ce type d'attaque correspond le plus souvent au troisième des *Trente-Six Stratagèmes*¹⁸, c'est-à-dire à emprunter l'épée pour défaire l'adversaire, et il n'y a pas meilleure « épée » numérique que la bande passante anonyme, sous-utilisée et souvent mal protégée que l'on trouve dans le foyer de chacun, dans des établissements publics mal sécurisés (universités), avant même d'avoir recours à un service criminel spécialisé de location de telles capacités. Ces attaques se multiplient dès la fin des années 2000 visant les serveurs racines du Département de Défense (DoD) américain, ou les serveurs de l'Icann (février 2007), les systèmes de paiement, les systèmes de sécurité, ou comme ce fut le cas en Estonie en avril 2007, les services d'urgence. Les régulateurs sont prompts à attribuer ces attaques à des groupes organisés, voire à la criminalité organisée ou à des États adverses, mais la réalité technique est très différente de ces projections étatiques. Il est donc possible qu'une cyberattaque, même menée par un groupuscule par ailleurs financé par un gouvernement, repose intégralement sur des capacités (serveurs, bande passante) « empruntées » à des clients tout à fait innocents, et tout à fait ignorants d'avoir contribué au façonnage global d'une arme de guerre cybernétique.

Les cyberattaques résistent ainsi aux typologies et aux « classes » qu'on aimerait leur attribuer. Une attaque en DDoS peut avoir pour finalité sa fonction première : noyer des serveurs de requête afin de les mettre en berne, pour le « *fun* », pour la revendication politique, pour une bravade entre *hackers*... ou pour déstabiliser un État. Il n'y a pas de réelle corrélation entre l'ampleur des moyens mobilisés, le « faciès numérique » du cracker/phracker/hacker/cyberterroriste, qui sont, là encore, des dénominations qui n'engagent que l'éthique *personnelle* de ceux qui veulent bien les porter. La différence entre le *hacker* et le *cracker*, termes hérités des années pionnières du *hacking*, ne tient qu'à une volonté individuelle d'utiliser, ou pas, des moyens techniques hors d'un cadre et d'un propos éthiques. On n'est pas *hacker* par le type de technique, ou de signatures de code, que l'on laisse derrière soi, mais par la *destination* que l'on fait de son code, et la vision du monde qu'on lui attache.

17 *Distributed Denial of Service : Déni de service distribué.*

18 Kircher F. (1995), *Les Trente-Six Stratagèmes*, traduction et commentaire des traités de Tan Daoji (420-479), Paris : Payot/Rivages.

[p. 177-195]

Philippe BAUMARD

Arch. phil. droit 56 (2013)

DES CYBERGUERRES, MAIS PAS DE « CYBERFORCE »

Au-delà de la capacité d'anonymat de l'attaquant, le caractère indifférencié du corps d'expertise technique, des moyens technologiques, et même du support *culturel* (ou culture alternative) de ce qu'on appelle des attaques cybernétiques interdit donc toute catégorisation *ex ante*. Or, la régulation contemporaine de la guerre repose, avec l'article 2 (4) de la Charte des Nations Unies, sur la catégorisation *ex ante* de l'usage de la force : « Les membres doivent se retenir dans leurs relations internationales d'utiliser la menace ou l'usage de la force contre l'intégrité territoriale ou l'indépendance politique de tout autre état, ou de toute manière incompatible avec les engagements des Nations Unies »¹⁹. L'article 2 (4) est complété par l'article 51 de la Charte qui stipule que « rien dans la présente Charte ne doit altérer le droit individuel et collectif à l'autodéfense si une action armée est menée contre un membre des Nations Unies »²⁰. Qu'est-ce que la « force » en matière cybernétique ? Et à partir de quel moment, de quelle quantité de bande passante, de quelle caractérisation de l'attaque, peut-on parler de « force armée » cybernétique ?

Le préfixe « cyber » est lui-même utilisé avec tant de déclinaisons, que les traités internationaux s'intéressant à la régulation des espaces numériques ont échoué à se mettre d'accord sur sa signification ou son étymologie. Le terme cybernétique est bien entendu un héritage des travaux des pionniers de cette discipline, comme Miller, Gallanter et Pribram²¹, et dont l'origine, dans les années 1940, est la volonté d'une étude systématique et scientifique de l'interaction du vivant et des machines²². Son projet initial, dans les pas

19 "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." – Charte des Nations Unies, Article 2, Paragraphe 4.

20 « Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations », Charte des Nations Unies, Article 51. Cf. Oscar Schachter, "The Right of States To Use Armed Force", 82 *Mich. l. rev.* 1620, 1624 (1984).

21 Miller, G.A., Galanter, E., & Pribram, K.H., *Plans and the Structure of Behavior*. New York : Holt, Rinehart & Winston, 1960.

22 Le terme « cybernétique » a pour origine les articles de A Rosenblueth, N Wiener, J Bigelow. "Behaviour, Purpose and Teleology", *Philosophy of Science* 10 1943, et celui de WS McCulloch, WA Pitts. "A Logical Calculus of Ideas Immanent in Nervous Activity", *Bulletin of Mathematical Biophysics*, vol. 5 1943. Pour une note de la naissance

d'Alan Turing, est de montrer qu'une manipulation symbolique autonome peut être conduite par une machine. Déjà, Polanyi posait dans son article de 1952 la question de l'expérience de la conscience et du jugement responsable qu'il considère comme un critère beaucoup plus pertinent que l'opposition pensée-calcul pour opposer hommes et machines²³. Il rejoignait en cela les réflexions de McKay, dans le même volume qui affirmait que la libre volonté des hommes ne pouvait être assimilée à l'indétermination des machines. Un système cybernétique est donc, dans cette perspective, un système capable d'un comportement délibéré poursuivant un propos conscient, que ce dernier soit le résultat de sa propre évolution ou qu'il lui ait été appris par l'homme. La cybernétique de Wiener, dont il invente le terme en ignorant qu'Ampère l'a déjà utilisé en 1873 pour désigner l'art de gouverner, n'était pas une science du contrôle et du signal, mais plutôt une science du gouvernement de la vie par la maîtrise de ses communications, humaines et/ou machines²⁴.

Une « arme cybernétique », si on s'en réfère à l'étymologie, est donc un dispositif visant à pervertir ou détruire les systèmes de commandement des systèmes de support du vivant et/ou les machines les composant. On peut d'ores et déjà noter que cette définition ne présuppose pas l'implication d'un pilotage ou d'une commande directe de nature humaine. De fait, les avancées dans le comportement artificiel et le raisonnement autonome des machines permettent aujourd'hui d'envisager l'existence d'un système cybernétique totalement autonome, conduisant aussi bien des opérations offensives que défensives²⁵. En ce sens, les attaques DDoS sont bien des agressions cybernétiques, mais toute agression utilisant une technologie de l'information ne peut pas être définie comme une « cyberattaque ». Un acte d'espionnage, qu'il soit mené par des moyens humains (*humint*) ou électroniques (*sigint*) reste un vol ou un détournement d'information. Ainsi, la définition de la Maison Blanche qui englobe toute organisation qui poursuit des buts criminels par le biais de technologies de l'information ou

de la cybernétique : Michael Polanyi (1952), "The Hypothesis of Cybernetics", *The British Journal for the Philosophy of Science*, Vol 2, No 8, p. 312-315. L'article offre une synthèse d'un débat sur la cybernétique menée dans le même journal par K.R. Popper (Vol 1, p. 194-195), J.O. Wisdom (Vol. 2, p. 1), D.M. MacKay (vol 2, p. 120), F.M. Walshe (Vol 2, p. 161-163), et W. Mays (vol 2, p. 249-252).

23 M. Polanyi, *op. cit.*, p. 315.

24 Lire à ce propos : D.J. Clark, *Enclosing the Field: from 'Mechanization of Thought Processes' to 'Autonomics'*, thèse de doctorat, Université de Warwick, septembre 20002, p. 88-91.

25 Baumard, P. "Using Machine Foreknowledge to Enhance Human Cognition", in P. Naim, O. Pourret et B.G. Marcot (Eds), *Bayesian Belief Networks: A Practical Guide to Applications*, New York : Wiley, 2008, p. 365-375.

en s'y connectant, tend à assimiler toute nouvelle forme de criminalité à de la « cybercriminalité », y compris les manipulations d'opinion, les déstabilisations par des campagnes de guerres de l'information, ou le vol de propriété intellectuelle, qui sont très éloignés d'une activité « cybernétique » *stricto sensu*. Ainsi, dès sa création en novembre 2001, la Convention de Budapest sur la cybercriminalité intègre les actions de vol d'identité, les attaques contre l'intégrité d'un système, le vol de données, la fraude, les contenus offensifs, la violation de copyright, les crimes « informationnels » de natures xénophobes et racistes, aussi bien que le « cyberterrorisme », défini par la Convention de Budapest comme l'usage de technologies de l'information pour propager la terreur²⁶.

On retrouve dans la Convention de Budapest cette velléité de faire de la guerre de l'information une « guerre de la connaissance »²⁷ qui est déjà dans l'arrière-plan des doctrines de cyberdéfense américaines à la fin des années 1990. Cette volonté d'imposer une *Pax Cybernetica* américaine éloigna un peu plus la Convention de Budapest de la lisibilité nécessaire à établir un usage de la force selon l'article 2 (4) de la Charte des Nations Unies. À vouloir créer un accord-cadre qui couvre tous les aspects du cyberspace, de l'expression de la violence symbolique jusqu'à l'acte de sabotage des infrastructures vitales d'un pays, la Convention de Budapest a échoué à atteindre un but qui était inconciliable : celui de mettre sur une même échelle de force le voyeurisme numérique, la pornographie, la liberté d'expression et l'attaque en sabotage d'une centrale nucléaire²⁸. Là encore, la régulation bute non pas sur la question de l'attribution, mais sur celle de l'établissement de preuve d'une *intentionnalité*. Le résultat est un cadre de régulation qui substitue la coercition à l'observation réelle et factuelle de la force comme légitimation de l'intervention. Dès lors, un tel cadre de régulation est prompt à

26 Titiriga Remus (2013), "Cyber Attacks and International Law of Armed Conflicts : A 'Jus Ad Bellum' Perspective", *Journal of International Commercial Law and Technology*, Vol. 8 No.3 p. 179-189.

27 Baumard, P. « From Information Warfare to Knowledge Warfare: Preparing for the Paradigm Shift », in Col. Alan D. Campen, USAF, Douglas H. Dearth and R. Thomas Goodden (Eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, Virginia : Armed Forces Communications and Electronics Association (AFCEA), 1996, p. 147-160. Lire également dans la même collection : MacIntosh, JP "Connectivity : The Space, Tempo and Exploitation of Risk in the Information Age", in Campen, AD & Dearth, DH (Eds), *Cyberwar 2.0 : Myths, Mysteries and Reality*, AFCEA Press : Fairfax VA, 1998.

28 Lire à ce propos la synthèse de Waxman Matthew C. (2011), "Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)", *Yale Journal of International Law*, Vol. 36, p. 421-459.

instaurer un climat de guerre froide²⁹. Dans le cas de Stuxnet, ou de Flame, deux campagnes d'attaques avancées avec des objectifs industriels précis, on peut effectivement parler d'un usage d'une « force de coercition » ou d'une « force d'interférence », car même si l'attribution n'a pas été concluante, le caractère ciblé de l'attaque, jusque dans la programmation et les codes de Stuxnet et Flame, montrent la spécificité de la construction de l'attaque pour obtenir un effet de force. Mais l'interférence obtenue par un agent humain infiltré qui révèle un dispositif d'écoute électronique, ou par les fuites systématiques de WikiLeaks, sont des « forces » bien plus déstabilisatrices à l'échelle d'une nation qu'un sabotage avorté sur une centrale nucléaire. C'est là qu'entre en jeu l'article 51 de la Charte des Nations Unies, et la « permission » de répondre soi-même, au titre de l'autodéfense, à une « attaque armée », remettant en cause « l'intégrité territoriale ». Le problème est, bien sûr, qu'il est difficile de se décider à répondre lorsqu'on ne possède pas d'échelle d'évaluation des délits et des peines, et lorsque l'on ne sait pas si « l'État d'en face » ne possède pas lui-même une échelle de réponses très différente³⁰ ; et comme le souligne Gaycken, cela ouvre la voie à un nombre incalculable de guerres déclenchées par des parties tierces, sans même que les belligérants n'en aient réellement conscience³¹.

DÉSACCORD SUR LES PÉRIMÈTRES ET SUR L'ONTOLOGIE

Dès lors, en matière de cybernétique, la guerre fera-t-elle loi ? Les tensions que connaît en juillet 2013 la négociation internationale pour une régulation de la cyberdéfense pourraient laisser présager que l'on cherche à préparer une guerre et à lui trouver ses supports juridiques. La Convention de Budapest de novembre 2001, qui effectivement devait réguler la cybercriminalité n'a toujours pas été ratifiée par la Chine et la Russie en juillet 2013. S'il n'y a pas de traité signé par les Russes et les Chinois, c'est à cause du problème, assez essentiel, de « définition » de la cybersécurité et de la cyberdéfense. D'un côté, les Occidentaux séparent la cybercriminalité (lutte contre la criminalité dans le cyberspace), la cyberdéfense (actions stratégiques des États dans ce milieu) et la cybersécurité (encouragé en cela par les

29 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 37 *Colum. J. Transnat'l L.* 885, 905 (1999).

30 James A. Lewis, "Multilateral Agreements To Constrain Cyberconflict", *Arms Control Today*, June 2010,

31 Gaycken, Sandro, (2010), "The Necessity of (Some) Certainty - A Critical Remark Concerning Matthew Sklerov's Concept of 'Active Defense'", *Journal of Military and Strategic Studies*, Vol. 12, No 2, p. 4-6.

industriels, qui espèrent un cadre de régulation aménagé)³². D'un autre, les Russes considèrent de longue date que ces notions n'existent pas individuellement, mais qu'il y a une seule et entière « sécurité de l'information », incluant autant le contenant que le contenu. Toutes les initiatives de régulation ont feint d'ignorer l'obstacle, jusqu'à la dernière initiative d'établir un glossaire commun pour tous les membres de ce tour de table mondial³³. Mais les Russes ou les Chinois ne peuvent renier leurs engagements constitutionnels respectifs, qui sanctuarisent cette conception d'une information, contenant et contenu, perçue comme une entité inséparable.

Rien, pourtant, ne laissait présager que les règles de l'engagement et de la légitimité de la guerre soient durablement transformées par l'avènement d'une société numérique. Comme le souligne Goldsmith, personne dans la première décennie d'existence du « réseau des réseaux » ne s'est jamais soucié de questions de sécurité. Jusqu'en 1988, lorsque Robert Tappan Morris, un étudiant de Cornell, introduisit un ver dans l'internet naissant dont le but expérimental était de mesurer la taille du réseau, et qui finit par mettre hors d'usage 10 % des 60 000 machines qui composaient alors le net³⁴. C'est en 1988 que naît le premier programme officiel de la DARPA sur la sécurité des réseaux, avec comme perspective celle de la résilience à des scénarios d'attaques sur les infrastructures... Mais c'est à Berlin, déjà, que se sont cristallisés les vrais enjeux et questions futures de la cybersécurité autour de l'affaire « Hagbard », pseudonyme de Kar Werner Koch, et de la naissance du Chaos Computer Club en 1981 autour de Markus Hess, Hans Heinrich Hübner ou Otto Brezinski³⁵. Le détournement de la technologie n'est pas dissociable de la poursuite d'un but politique, et dès lors, pour les Russes autant que pour les Américains qui s'affrontent dans cette première cyber-guerre autour de la chute du Mur de Berlin, l'espace numérique naissant est déjà un terrain de conflit géopolitique.

Si la finalité politique d'une campagne de déstabilisation ou de sabotage n'est pas difficile à établir, au moins *a posteriori*, il est très difficile de définir ce qui constitue un « acte de guerre » du point de vue cybernétique. Le Chaos Computer Club, dès sa fondation, poursuit un but de démonstration des dangers potentiels d'un mauvais usage des technologies de l'information pour la liberté d'expression, les libertés individuelles et la démocratie,

32 Cf à ce propos l'étude de l'ONDC : http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

33 <http://www.unodc.org/unodc/en/commissions/CCPCJ/session/22.html>.

34 Goldsmith, 2013, *op. cit.*, p. 129.

35 Hafner Katie, John Markoff (1995), *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, NY : Simon & Schuster.

s'invitant au débat politique par la prouesse technique. Ces démonstrations sont nombreuses entre 1981 et 2013, et la plus symbolique est sans doute l'opération visant à démontrer la facilité avec laquelle les machines à voter électroniques néerlandaises pouvaient être interceptées en moins de trois minutes par un petit groupe organisé pour en changer les résultats. Réalisé en 2006 en coopération avec une fondation néerlandaise pour les libertés individuelles, cet exploit du CCC a abouti à une révision de la cour constitutionnelle néerlandaise de l'encadrement du vote électronique³⁶, puis à l'abandon du vote électronique³⁷. On comprend dès lors qu'on ne puisse aveuglément appliquer une image du droit public, ou du droit privé, dans le domaine « informationnel » sans prendre auparavant quelques précautions. Doit-on juger l'action du CCC sous l'angle du droit commun, et dès lors, l'interdire et la sanctionner dès ses premiers pas ? Ou doit-on la juger par sa finalité de « lanceur d'alerte », et dès lors, en saluer la prouesse et la noblesse sur sa finalité ?

LES AMBIGUITÉS DU CYBERCRIME

La première ambiguïté de l'exercice d'un jugement sur un crime informatique réside donc dans sa « non déterminabilité » *ex ante*. L'opération menée par le CCC pour démontrer le caractère manipulable des machines de vote est exactement la même que celle qu'aurait menée un gang criminel qui poursuivrait le but de manipuler les résultats d'un vote national³⁸. Le vecteur lui-même n'est pas caractérisable *a priori* comme porteur d'une intention malveillante. Ce qui serait vrai pour un virus, un code malicieux visant à paralyser ou détruire un système logique, ne l'est jamais pour un détournement de fonctionnalité ou de finalité d'usage³⁹.

Avant même de pouvoir établir l'auteur d'un crime informatique (« attribution »), il est difficile d'établir l'intention réelle d'un test, d'une découverte et d'une exploitation de faille, d'une ingénierie inversée, ou d'un détournement de fonctionnalité mal protégé, - ce que l'on peut regrouper

36 Pour une documentation plus détaillée, lire *Die Datenschleuder*, publication du CCC, accessible sur <http://ds.ccc.de/>

37 Jacobs Bart, Wolter Pieters (2009), "Electronic Voting in the Netherlands : From Early Adoption to Early Abolishment", *Foundations of Security Analysis and Design V, Lecture Notes in Computer Science*, Volume 5705, p 121-144.

38 Jacobs et Pieters, *op. cit.* ; Libicki Martin, (2009), *Cyberdeterrence and Cyberwar*, RAND.

39 Reich Pauline C., Stuart Weinstein, Charles Wild & Allan S. Cabanlong (2010), "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity", *European Journal of Law and Technology*, Vol. 1, Issue 2.

sous le vocable « hacks ». Ainsi, les approches qui consistent à vouloir caractériser *a priori* les acteurs du cyberspace entre les « wicked » et les « bien intentionnés »⁴⁰ dénotent soit une grande naïveté et méconnaissance du sujet, ou, tout au contraire, une position politique affirmée cherchant à promouvoir une forme de « délit de faciès numérique » dans le cadre de régulation.

La seconde ambiguïté réside dans la téléologie présumée de l'agression informatique : si son but est le système informatique de l'adversaire, ce système peut-il être assimilé à l'adversaire lui-même ? Faut-il dès lors établir un encadrement légal entre les machines et leurs propriétaires, pour identifier ces « actes de guerre » ou « actes criminels », ou faut-il laisser ce délicat sujet dans le « brouillard de guerre » ? Certains auteurs assimilent l'homme, la machine et l'ennemi sans aucune inhibition : l'un vaut indistinctement l'autre⁴¹. D'autres préfèrent y voir un *distinguo*, et encourager l'émergence d'un cadre normatif spécifique à l'usage de la force sur les réseaux informatiques⁴². Mais l'agression par des moyens informatiques est-elle vraiment similaire à un acte de guerre ? Peut-on comparer une « cyberattaque » à un usage de la force armée selon l'article 2-4 ou une « attaque armée », selon l'article 51, de la Charte des Nations Unies ? Qu'en est-il de la frontière – juridique, économique, sociale – entre la cyber-guerre et le crime informatique ?

La question est moins triviale que le laisse entendre sa formulation. Elle pose non seulement la question de la neutralité des technologies de l'information, mais surtout celle de la frontière entre droit privé, droit commercial et droit public dans le cyberspace. Si l'on considère la technologie informatique comme un élément neutre, on doit dès lors accepter

40 Notamment : Demchak, C.C. (1992), "Complexity, Rogue Outcomes and Weapon Systems." *Public Administration Review* 52 (4), p. 347-55, et Demchak, C.C. (2011), *Wars of Disruption and Resilience : Cybered Conflict, Power, and National Security*, Athens, Georgia : University of Georgia Press.

41 Cf. Ezekiel Alan W. (2013), "Hackers, spies, and stolen secrets : protecting law firms from data theft", *Harvard Journal of Law & Technology*, Volume 26, Number 2, p. 649-668.

42 C'est notamment l'axe adopté par la proposition de cadre de régulation par le centre d'excellence de l'OTAN de Tallin : Schmitt, Michael N (Ed). (2013), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Tallinn, Estonia : NATO Cooperative Cyber Defence Centre of Excellence et Cambridge University Press.

l'idée que l'établissement de la preuve, de l'attribution de l'agression, ne peuvent plus être résolus par un simple audit informatique⁴³.

UN STATU QUO QUI FAVORISE LE « BROUILLARD DE GUERRE »

Réguler le cyberspace, c'est s'acheter un passeport d'ingérence dans les affaires internes de ses voisins. C'est du moins comme cela que sont perçus de nombreux articles de ce traité, notamment l'article 32 qui concerne l'accès transfrontalier aux « données » lors de crises, d'incidents, ou d'investigations. Les Russes et les Chinois y sont particulièrement opposés. Mais il n'y a pas que cela. La régulation de la contre-mesure, c'est-à-dire de la légitimité à engager des représailles et à estimer sa proportionnalité, est évidemment au cœur des différends⁴⁴. L'Ouest pousse une vision de l'attribution des attaques proche de celle du droit commun, qui associerait donc la responsabilité des crimes à leur origine géographique, et le « droit de réponse » à une forme d'extraterritorialité accordée par ces traités. Mais, depuis leur rédaction, les technologies ont changé et l'attribution géographique des campagnes d'attaques avancées modernes est quasiment impossible⁴⁵. On finirait par avoir un cadre de régulation efficace contre le petit crime commun, suffisamment naïf ou mal équipé pour ne pas masquer son origine d'attaque, et incapable d'encadrer les attaques d'États, ou celle du crime organisé, capables de soustraire technologiquement à la régulation.

Certains partenaires de ces négociations y voient une « carte blanche » donnée aux nations qui ont un avantage technologique pour mener une « guerre limitée » ou une « guerre sale » électronique permanente.⁴⁶ Le problème est qu'en matière de crime numérique, détenir l'arme, le mobile et le lieu du crime est loin d'être suffisant pour établir une intentionnalité et l'identité du coupable ! Les cyberguerres répondent à un paradigme dominant qui est celui de la guerre limitée ou du conflit contre-insurrectionnel : les moyens y sont empruntés, détournés, déplacés et

43 Shackelford Scott (2009), "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkley Journal of International Law* (BJIL), Vol. 25, No. 3, p. 192-250.

44 Cf. Lewis James A., (2005), "Aux armes, citoyens: Cyber security and regulation in the United States", *Telecommunications Policy*, Volume 29, Issue 11, p. 821-830.

45 Van Eeten Michel et Johannes M. Bauer (2009), « Emerging Threats to Internet Security : Incentives, Externalities and Policy Implications », *Journal of Contingencies and Crisis Management*, Volume 17, Issue 4, pages 221 – 232.

46 Li, Sheng (2013), « When Does Internet Denial Trigger the Right of Armed Self-Defense ? », *Yale Journal of International Law*, Vol. 38, No. 1, p. 179-216.

subversifs par nature⁴⁷. L'usage intensif de capacités robotiques (*botnets*, etc.) rend complexe la tâche d'établir une intentionnalité ou une source. Le modèle proposé par le cadre de régulation actuel est celui des conflits conventionnels, incluant, par exemple, des notions comme l'escalade du conflit. Mais qui aujourd'hui seraient les premières victimes d'une « escalade », par exemple sur les infrastructures vitales, d'un cyberconflit ? Probablement ceux qui dépendent, d'un point de vue économique, des infrastructures numériques. Les Chinois ou les Russes ont fait des choix stratégiques différents en matière de développement d'infrastructure nationale d'information. Ils ont des réseaux suffisamment compartimentés, en partie avec des technologies propriétaires, développées depuis le milieu des années 1980 ; certes, sans doute plus lentes, mais beaucoup moins sensibles à une escalade de dommages en cas de conflit.

Le problème de fond de la régulation reste la machine, c'est-à-dire le point d'ancrage de l'économie numérique. Pourquoi les Américains sont-ils si pressés sur le sujet ? Ils mettent en avant l'enjeu du vol de propriété intellectuelle avec une perte de 4,8/5 milliards de dollars selon le rapport du Congrès⁴⁸, ce qui est une estimation faible, avec des rapports alarmistes sur les infrastructures critiques par ailleurs. Cet empressement cache une vulnérabilité majeure, provenant de l'industrie elle-même. Aujourd'hui, le point de création de valeur, le point d'ancrage des modèles économiques, et le point de confrontation des cyberconflits est le même : votre machine, ma machine. Avec un commerce électronique bientôt dominant les transactions commerciales, une formation des opinions directement dépendante d'interfaces hommes-machines (Google, Facebook ou MSFT parmi d'autres), le levier de création de richesse nationale se trouve être, aussi, le potentiel champ de bataille numérique⁴⁹. C'est ce qui explique sans doute la divergence des agendas entre les majors qui veulent un modèle où chaque citoyen est le simple titulaire d'une licence d'exploitation de ses propres données personnelles et le modèle de souveraineté sur la propriété intellectuelle, qui suit une logique nationale. La transparence et l'accès que réclament les États ne sont pas forcément dans l'intérêt des industriels du numérique, et vice-versa. Cela a conduit certains exploitants à refuser de continuer ce genre d'échanges, non par préoccupation pour la défense des libertés

47 Allen, P. D., et C. Demchak (2003) "The Palestinian-Israeli Cyberwar." *Military Review*, 83 (2), p. 2 52-59.

48 www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

49 Baumard, P. « Numérisation, liberté et sécurité », *Politique internationale*, no 135, p. 371-377, 2012.

personnelles, qu'ils continuent de bafouer allégrement, mais pour éviter que la régulation internationale de la cyber-défense vienne perturber leur modèle économique.

TROIS DOCTRINES, UN SEUL CYBERESPACE

La question de la contre-mesure est avant tout la question de la part que l'on souhaite laisser à l'automate et aux algorithmes de raisonnement autonomes dans la société de demain, et de la part que l'on souhaite réserver au privilège d'être humain. L'état de l'art technique est incapable aujourd'hui de rattraper la courbe de production et d'inventivité des technologies capables de perturber, déstabiliser, espionner, détourner ou détruire des infrastructures d'information globales, pervasives, et historiquement non conçues pour gérer de tels problèmes de sécurité. Il semble que les régulateurs courent après des ennemis imaginaires, et qu'ils aient eux-mêmes créé l'aporie dans laquelle se situe, depuis 2001, la négociation pour établir un cadre réglementaire et légal au cyberspace.

La production des contre-mesures, que sont aujourd'hui les très inefficaces « découvertes de failles », passe par une organisation de marché déficiente : celui des « exploits » (espace de marché numérique fermé où sont achetées les découvertes de vulnérabilités « zéro jours ») ; mais c'est, trop souvent, un marché de dupes qui a connu une inflation sans précédent dans les cinq dernières années, sans améliorer l'efficacité de la défense⁵⁰. Que ce soit du point de vue de son équation économique, ou de celui des progrès technologiques de la ligne de défense, la stratégie qui consiste à vouloir appliquer les articles 2 (4) et 51 de la Charte des Nations Unies à la gestion du cyberspace risque bien de provoquer l'inverse du résultat escompté. L'enjeu des « contre-mesures » pose ainsi la question de savoir si c'est le plus compétent, le souverain, ou le gestionnaire des infrastructures qui doit prendre les armes et répondre à l'attaquant. La doctrine de la « compétence » est celle des technologistes. Elle pousse bien sûr à l'extraterritorialité des fournisseurs, et derrière eux, du ou des pays qui en sont les hébergeurs ou actionnaires. Ce scénario est souvent identifié comme celui des États-Unis,

50 Ransbotham, S. Mitra, and J. Ramsey, "Are Markets for Vulnerabilities Effective?," *MIS Quarterly*, vol. 36, no. 1, p. 43-64, 2012 et R. Anderson, C. Barton, R. Bohme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," *Proc. of WEIS'12*, 2012. Les découvertes de vulnérabilités exploitables ("exploits") peuvent s'échanger sur des places de marché anonymes entre 20 et 300 K\$ (marchés criminalisés), tandis que la déclaration légitime de découvertes de failles envers les fournisseurs est généralement récompensée entre 2 et 5 K\$ en 2013.

où la suprématie du secteur américain de la cybersécurité et de l'appareil d'État pour la cyberdéfense permettrait d'établir un modèle qui consiste à confier au fournisseur de la technologie de cybersécurité la responsabilité des contre-mesures. Cette doctrine s'oppose au modèle « souverainiste » vertical des Russes qui ne sépare pas l'information en contenants et en contenus. Les Chinois, sur ce point, suivent les Russes, et même les dépassent en en faisant un objectif affiché de sécurité économique nationale. Les Européens tentent de faire front commun sur les interceptions, sur la protection des données personnelles avec le projet étudié actuellement par la Commission Européenne.

Les positions à l'intérieur de l'Europe sont bien sûr très variées. Les Allemands, dont les souvenirs douloureux sont encore récents, ont une perception différente de la nôtre de la protection des données personnelles. Cela se traduit effectivement dans leurs événements domestiques (flou des images sur Google View, refus du recueil de données personnelles, émergence du Parti pirate promoteur de ces thèmes). Les Français, on le sait, ont une relation différente à la donnée privée, souvent perçue comme paradoxale au pays des droits de l'homme. Il y a sans doute là une carte diplomatique que nous n'avons pas su jouer, tant nous sommes absents, du point de vue stratégique, des corps doctrinaires dominants. La régulation de la cyberdéfense et de la cybersécurité est un enjeu qui ne mobilise pas l'opinion, et, pourtant, il s'agit de la régulation la plus transformatrice des cinquante prochaines années. Réguler le recours à la sanction, à la protection et à l'interdiction dans le monde numérique, c'est définir les frontières des sociétés civiles demain, et très certainement, les positions de puissance économique et politique de ces sociétés.

philippe.baumard@polytechnique.edu