D'une stratégie de cyberdéfense à un souci pour le cybercrime. Lenteurs et accélérations d'une mutation au cœur de l'état*

par **Frédéric OCQUETEAU**** et **Daniel VENTRE*****

Résumé
Bien que les instances internationales aient joué assez tôt leur rôle de lanceurs d'alerte au sujet des dangers liés à la cybercriminalité, la recherche scientifique critique ne s'est pas imposée d'emblée en Europe continentale sur ce thème. L'article explore surtout la situation française et évalue les raisons de son retard par rapport à d'autres contextes, américain, canadien et britannique. Il émet une série d'hypothèses inter-corrélées montrant comment les enjeux de la cyberdéfense militaire ont longtemps occupé le devant de la scène de l'État français bien avant ceux de la cybercriminalité. Il explique comment deux innovations institutionnelles de la fin des années 2000 ont opéré, sous le concept de cybersécurité, la jonction nécessaire avec les préoccupations civiles et comment la communauté des sciences humaines ne s'est que très récemment mobilisée à la faveur d'une prise de conscience de la Justice pour penser la protection des entreprises et des internautes vulnérables. Il montre enfin comment les sphères politico-administrative et scientifique pourraient se rejoindre dans des programmes de recherche où une certaine criminologie des marges aurait son mot à dire, à condition de ne pas se focaliser sur les seuls «auteurs» et «victimes» de la régulation pénale classique.

Mots-clés: cybercriminalité, cyberdéfense, cybersécurité, policing, politique de recherche, France, XXIe siècle.

Summary
Although international bodies have played their role in early whistleblowers about the dangers of cybercrime, critical scientific research did not initially imposed in mainland Europe on this topic. The article explores especially the French situation and assesses the reasons for the delay compared to other contexts, American, Canadian and British. It emits a series of assumptions inter correlated showing how the challenges of cyber military have long occupied the center stage of the French state, even before those of cybercrime. It explains how two institutional innovations of the late 2000s operated, under the concept of cyber security, the necessary connection with civil concerns. And how the humanities community has to very recently mobilized in favor of an awareness of Justice to think protecting businesses and vulnerable users. Finally, it shows how the politico-

* Cet article est tiré de la mise en commun de deux communications des auteurs (Ocqueteau, 2014; Ventre, 2014b) au sein de l'Atelier n° 1 du XIVe Congrès de l'AICLF «Hackers, Cyber-barbouzes et chercheurs», Liège, mai 2014.

** Sociologue, Directeur de recherches au CNRS (CESDIP).
*** Politiste, Docteur en science politique au CNRS (CESDIP).

administrative and scientific spheres could join themselves in research programs where some criminology margins have its say, provided they do not focus solely on the «offenders" and «victims» of classic criminal regulation.

Keywords: cybercrime, cyber defense, cyber safety, policing, research policy, France, twenty-first century.

Introduction

À la différence des pays de traditions criminologiques plus institutionnalisées comme les États-Unis (Brenner, 2010; Holt, Bossler, 2014), la Grande-Bretagne (Wall, 2007; Williams, Wall, 2013) ou le Canada (Leman-Langlois, 2008; Dupont, Gautrais, 2010; Dupont, 2014b), pionniers dans les recherches empiriques liées aux *technocrimes* puis aux *cybercrimes* (ou *computer crime*), la France, pas plus que les nations de l'Europe continentale, ne s'est encore véritablement mesurée à l'identification critique de ces phénomènes. Pourtant, dès la fin des années 1960, W. H. Ware (1967) de la *Rand Corporation* avait mis l'accent sur les risques que faisait encourir aux citoyens et aux libertés individuelles l'utilisation illicite des ordinateurs. La notion de *crime commis par ordinateur* avait été formulée dix ans plus tard par D.B. Parker (Parker, 1976). Ainsi, durant trente ans, ces objets de connaissance n'ont jamais réussi en France - pour ne citer que le pays que nous connaissons le mieux - à trouver un écho un tant soit peu stabilisé dans un corpus de théorisations universitaires et de pratiques institutionnelles spécifiques capables de se rencontrer au sein de l'État et de la société civile pour en faire un objet d'appropriation consensuel commun. Quelles en sont les raisons?

Il nous semble qu'une bonne partie des blocages tienne principalement à la nature historico-institutionnelle des États continentaux qui détermine encore largement les mécanismes de la curiosité scientifique critique. Or, avec l'apparition du *cyberespace (4)* (Musso, 2000; Ventre, 2011) et ses multiples possibilités d'émancipation et de dangers pour les États comme pour leur société civile, les *principes de sécurité et de liberté* qui régissaient les frontières de la pensée et de la pratique juridique de *l'État de sécurité* issu de la Révolution de 1789 (Gros, 2012), déjà bien fragilisés, se sont définitivement altérés (Ocqueteau, Ventre, 2011). Mais il y aurait cependant quelque chose de toujours rassurant à ne pas vouloir considérer toutes les implications sur lesquelles débouche cette fragilisation, et surtout à s'en remettre par principe aux États-nation (encore réputés «forts») pour leur laisser le soin de définir en toute confiance les principales modalités de la conjuration des dangers, plutôt que d'admettre leurs propres faillibilité, interdépendance et mauvaise coordination, tant que n'existe pas de réel accord sur le périmètre des «mauvaises» tendances à contenir.

On prétend volontiers aujourd'hui qu'en raison d'une offre technique qui évoluerait à grands pas, se vulgariserait et serait facilement accessible, le

nombre des cybercriminels toutes catégories confondues serait devenu tel que le *cybercrime ne serait plus une affaire de férus d'informatique*. Voilà une idée répandue qui justifierait que l'on s'alarme tous, alors que ce type de danger n'avait, durant longtemps, pas préoccupé des esprits critiques qui les avaient relativisés au point de n'en articuler aucun souci scientifique particulier. Il avait en effet été assez largement démontré, parmi des sociologues français pionniers des années 1980-1990 (Breton *et al.,* 1991), que les formes de déviance et de lutte spécifiques inhérentes aux éventuels dangers liés à l'apparition du cyberespace étaient étroitement dépendantes des valeurs véhiculées par la seule communauté des *praticiens de l'informatique* maîtrisant les instruments, atouts comme faiblesses. D'autres, dans une veine latourienne proche de l'anthropologie symétrique, plus sensibles aux formes de contrôles liées à l'invasion des systèmes socio-techniques au sein des sociétés post-modernes, avaient montré comment les systèmes régulaient eux-mêmes les comportements sociaux en projetant progressivement sur leurs usagers un consentement formé autour de menaces invisibles mais ubiquistes (Lianos, 2001). La criminologie avait été largement tenue éloignée de ces incursions restées sans lendemain. Les valeurs des informaticiens, relativement partagées par une infime minorité de «nouveaux» policiers spécialisés – des hackers plutôt décontractés du Net qui ne purent faire autrement que d'endosser un rôle contraint – vouaient ces deux catégories d'acteurs à agir dans un monde étrange.

Si, les décennies passant, la perception des vulnérabilités du Net devenait un souci pour un nombre toujours plus important de techniciens privés et publics se spécialisant, les instruments de la justice pénale n'apparurent jamais comme des solutions de prévention, voire de répression, très crédibles. La puissance des manifestes libertaires (Barlow, 1996) ayant présidé à la naissance du Net faisait encore très largement écran. Les entreprises publiques et privées apprenaient certes à faire face aux torts et dommages qu'elles créaient et subissaient en recourant à d'autres voies de prévention et de régulation effectives, alors que personne ne parvenait ni à prendre de hauteur suffisante pour mesurer l'efficacité d'un périmètre mou, ni à évaluer correctement les effets de la complémentarité de l'action respective des «sachants» de la sécurisation collective. Qu'il s'agisse des pratiques d'autodiscipline déontologique des entreprises (Ocqueteau, 2011), des mécanismes de corégulation privée/publique de professionnels unis face à l'expansion des risques du commerce en ligne, du recours aux assurances ou autres mécanismes indemnitaires en cas d'avaries, du recours aux conseils des Autorités administratives indépendantes (CNIL, HADOPI ou ARJEL, pour ne citer que la France), en passant par la jurisprudence de la justice civile ou bien encore par les pratiques transactionnelles des administrations spécialisées, rien ne permettait à la criminologie pénalocentrée en Europe, et encore moins en France, à partir d'une épistémologie solide, le loisir de féconder de véritables recherches critiques dans ce champ.

Ce qu'il manquait dans la rhétorique réductionniste de «l'auteur» et de la «victime» d'actes hostiles sévissant dans le cyberespace, ce n'étaient plus les valeurs des experts informaticiens ou de ses policiers du Net, mais une véri-

table pensée sur la place occupée par des opérateurs hébergeurs et fournisseurs d'accès, des techniciens jouant une partition intermédiaire fondamentale dans les mécanismes de la responsabilisation collective, dans un chaînon encore trop sous-estimé par les sciences humaines. Et pour une fois, ce furent les juristes, ces spécialistes de l'imputation des responsabilités collectives (Lupária, 2012; Feral-Schuhl, 2012; Bossan, 2013), qui montrèrent l'incontournable voie de centration. Opérateurs de communications électroniques, fournisseurs d'accès ou d'hébergements et éditeurs de services (d'outils de recherches et d'échanges), étaient devenus autant d'acteurs sur lesquels se focalisaient les nouvelles prises de conscience autour des forces et des faiblesses des pratiques d'entrée et de sortie au sein du cyberespace. Maîtrisant les données circulant sur le réseau, ils furent objectivement tenus pour responsables des équilibres extrêmement délicats de la liberté et des excès des internautes, posture qui les prédestinèrent à apparaître comme les meilleurs alliés ou les meilleurs ennemis de toutes les polices et justices du cybermonde.

L'objectif de cet article n'est pas de céder à la critique de l'essayisme d'experts publics et privés toujours plus imaginatifs dans les solutions partielles qu'ils proposent, mais plutôt d'expliquer pourquoi l'objet *cybercriminalité* a mis si longtemps en France à devenir un objet de connaissance critique, et pourquoi, dans le même temps, elle est restée un objectif de lutte secondaire pour les pouvoirs publics par rapport à d'autres priorités, celles de la *cyberdéfense* et de la *cybersécurité*, alors que les organisations internationales tentaient de convertir les États-nation à s'en préoccuper en priorité. C'est en effet sous l'impulsion des recommandations des instances internationales (ONU, 2000) ou européennes (Conseil de l'Europe, 2001), que l'imagination juridique dans la lutte contre les dangers criminels liés à l'existence du cyberespace commença à subir une inflexion significative, sans que la contribution des sciences sociales n'y ait jamais été véritablement associée. Elles ont désormais à prendre d'urgence le train en marche en repartant des apports du bâti normatif inflationniste qui s'est rapidement édifié sur des connaissances relativement vides ou peu solides. L'article formule en conséquence une série d'hypothèses institutionnelles inter-corrélées sur la lenteur et l'accélération de la prise de conscience française, et suggère *in fine* quelques pistes programmatiques pour que des sciences sociales à orientation criminologique se mobilisent à meilleur escient en vue d'aider à sortir le champ de son état de sous-questionnement chronique.

I - Faiblesses de la perception académique du cybercrime comme objet

Face à la complexité d'un monde qui s'édifie dans le cyberespace, il convient d'établir, à titre liminaire, un utile rappel pour contextualiser la préoccupation animant cette réflexion. Que les risques, les menaces, les dangers et les vulnérabilités soient objectivement devenus mondialisés, rien ne semble pour autant avoir véritablement changé dans la posture des États démocratiques dont la vocation implicite demeure de les combattre militairement, policièrement et judiciairement à partir de leur sol, quitte à empiéter drastiquement sur

la liberté des peuples ou de leurs citoyens (Ocqueteau, 2010). Alors que tout invitait à devoir repenser entièrement les modalités d'exercice de leurs missions régaliennes de surveillance et de contrôle dans le temps où se répandaient les outils technologiques mobilisés par les puissances pour dominer leurs concurrents dans le domaine économique ou militaire, l'enjeu devenait très gros de conséquences quant aux nouvelles manières de penser le destin collectif du monde (dé)régulé par les logiques conflictuelles qui s'y faisaient jour. L'explosion et l'emprise des technologies de l'information et de la communication par le biais de l'Internet, les possibilités de plus en plus sophistiquées de traçages électroniques (Mallet-Pujol, 2006) aussi bien des particuliers que des groupes sociaux spécifiques, l'essor fulgurant des systèmes biométriques qui prétendent définir «qui est qui» sans aucun risque d'erreurs, la fin de la notion de vie privée censément protégée et garantie par les États, tous ces phénomènes subvertissent progressivement les rapports de pouvoir, de domination et d'emprise traditionnels des États forts sur la cohésion de leur propre société civile.

À chaque fois qu'apparaissent sur le marché de nouvelles technologies industrielles de contrôle, de surveillance et de protection, et que se répandent le besoin et la demande afférents parmi les usagers potentiels (qu'ils soient États, entreprises, groupes de la société civile ou particuliers isolés), se nouent autant de nouvelles interdépendances de pouvoir potentiellement collusives ou conflictuelles quant à la hiérarchie des menaces à conjurer en priorité. Si bien que les sciences humaines, soucieuses de rendre compte de ces phénomènes sont elles-mêmes mises à rude épreuve, au point parfois de devoir assumer leur incapacité à pouvoir embrasser la totalité de ce réel-ci. Elles sont de surcroît affaiblies par des démentis rapides dans leurs exercices de prédictions à moyen terme, quand elles s'y risquent au fur et à mesure de la mondialisation des flux, du passage de l'informatique au numérique et de l'accélération du temps (Rosa, 2010). S'agissant *du contrôle* étatique à l'ère de la cyber navigation généralisée au sein de *l'infosphère* (Ganascia, 2009, 149) (5), de moins en moins de monde ne croit au répulsif idéologique des métaphores du *Big brother* ou du *Panopticon*, en dépit des révélations de l'affaire Wikileaks (Fenster, 2012; Sánchez Estorp, 2014) ou de celles de Snowden dite de «l'affaire Prism» (6) (Greenwald, 2014). De sorte qu'une résistance collective au sujet du cynisme dévoilé des États a peu de chances de s'organiser pour susciter des révoltes frontales à l'échelle planétaire, sinon à des échelons micro régionaux. C'est que les besoins de réassurance collective, puissamment orchestrés par un néocapitalisme anxiogène, se font de plus en plus impérieux, et exigent de disposer en permanence de circuits de dérivation sur de nouveaux épouvantails crédibles, les 'loups solitaires auto-radicalisés' par exemple, pour effrayer la nouvelle génération digitale.

Dans une enquête effectuée par l'un de nous, à partir des bases de données recensant les publications scientifiques, traitant de la *cybercriminalité* par rapport à la criminalité en général, depuis leur naissance, voici les résultats qui ont pu être mis à jour.

Bases supports (avec année de la première occurrence *Cybercrime*)	Occurrences *Crime*	Occurrences *Cybercrime*	Rapport en % *Cybercrime /Crime*
CAIRN (2001-)	9 906	31	0,3
ERUDIT (2000-)	7 457	11	0,1
ISIDORE (2001-)	10 612	48	0,4
JSTOR (1994-)	250 471	255	0,1
MUSE (2008-)	22 400	33	0,2
OPEN EDITION (2003-)	16 693	33	0,2
PERSÉE (2001-)	16 233	3	0,02
SAGE (1991-)	82 773	262	0,3
SCIENCEDIRECT (1995-)	85 037	1 712	**2,0**
SPRINGER LINK (1996-)	81 670	986	1,2

Source : D. Ventre (2014a)

Tableau 1: Contenu statistique des bases de données indexant les articles avec année d'apparition de la première occurrence cybercrime jusqu'à 2014.

Quand on s'attarde sur la base de données la plus productrice d'entre elles, ScienceDirect, s'agissant des seules entrées liées au cybercrime, il en résulte les enseignements suivants:

La courbe d'évolution de la production des «sciences sociales» (et singulièrement des «computer science») dédiées à la *cybercriminalité (7)* qui se dégage de la base ScienceDirect, se caractérise par trois pics notables: 2001; 2007; 2011-2013. Ces dates coïncident, pour la première, avec la signature de la Convention sur la Cybercriminalité (dite Convention de Budapest); pour la seconde (2007), aux cyberattaques menées contre l'Estonie; puis, pour la troi-

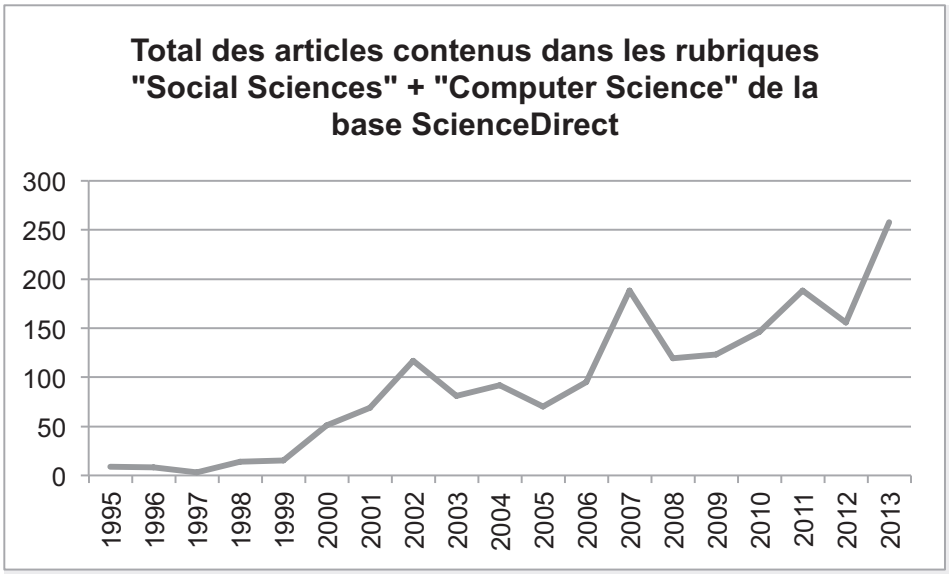

Schéma 1: Base de données ScienceDirect. Requête: «cybercrime». Nombre de publications annuelles relevant de deux disciplines: «social sciences» et «computer science» (janvier 1995 – décembre 2013).

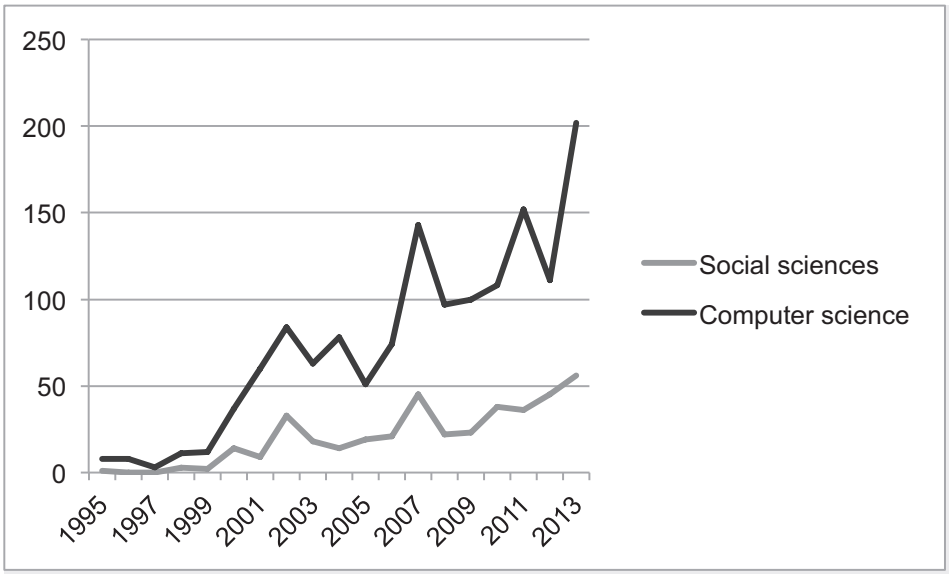

Schéma 2: Base de données ScienceDirect. Requête: «cybercrime». Ventilation de la progression des publications à partir des deux disciplines: «social sciences» et «computer science» (janvier 1995 – décembre 2013).

sième, à une succession d'événements très médiatisés, allant des révélations de WikiLeaks en 2010 aux révélations d'Edward Snowden sur la cybersurveillance américaine, en passant par l'opération Stuxnet (cyberattaques contre les infrastructures nucléaires iraniennes) en 2011. Sans que ces événements puissent expliquer à eux seuls leur impact sur les dynamiques de la production scientifique, il y a de bonnes raisons de croire néanmoins qu'ils ont joué un rôle significatif dans la prise en compte des enjeux de la cybersécurité pour la communauté de recherche internationale.

Il valait en outre la peine d'établir un inventaire des lieux académiques européens où se développent des recherches liées à cet objet de connaissance. L'enquête entreprise sur les centres de recherche européens a montré que leur production, en dehors du droit, était très largement reliée aux industries de la techno-prévention dans le champ pénal (technologies de surveillance à distance dans la rue, dispositifs de géolocalisation, ou bracelets électroniques sur personnes en semi-liberté…), bien que plutôt centrées sur les vulnérabilités du cyberespace et du Net (8). C'est particulièrement le cas des deux Universités françaises de Troyes et de Montpellier qui, s'appuyant sur des experts juristes, proposent des filières de formation continue à des acteurs opérationnels.

Quoiqu'il en soit, de la faiblesse de la capitalisation du savoir dans ces lieux de recherche académique, il ne faudrait pas en conclure que des connaissances quantifiées n'auraient pas été utiles dans la préparation de la prise de conscience collective. On note par exemple, parmi les premiers lanceurs d'alerte français au sujet des menaces informatiques, que le CLUSIF (9) par ses

	Universités	Industriels	Institutions
France	- Université de Technologie de Troyes - Université de Montpellier 1	- Thales - Microsoft France	-Gendarmerie Nationale -Police Nationale
Irlande	- University College Dublin Centre for Cybersecurity & Cybercrime Investigation (UCD School of Computer Science and Informatics)	- Microsoft - Irish Banking Federation - INFACT - eBay	- An Garda Síochána
Belgique	- KU Leuven (Interdisciplinary Centre for Law & ICT (ICRI) (The Institute of Criminal law) - CRIDS - Facultés Universitaires Notre-Dame de la Paix (FUNDP) - Tilburg University (NL) - UCL Crypto Group	- Atos Origin - Cisco - Computer Systems - Microsoft - Febelfin	- Federal Computer Crime Unit - National Institute for Criminology & Criminalistacs (INCC) - Instituut voor gerechtelijke opleiding - Institut de formation judiciaire - Service Public Fédéral Intérieur – (Federale Overheidsdienst Binnenlandse Zaken) - Federale Overheidsdienst Informatie - en Communicatietechnologie - (Service Public Fédéral Technologie de l'Information et de la Communication) - Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Bulgarie	Faculty of Computer Systems and Control at Technical University of Sofia, Bulgaria	- Microsoft - EMC - Computer Systems - GmBH / RSA	- General Directorate Combating Organized Crime within Ministry of Interior of the Republic of Bulgaria
Royaume-Uni	-Canterbury Christ Church University -Anglia Ruskin University -Kings College London -University of Bedfordshire -University of Greenwich -Liverpool John Moores University -University of Plymouth -De Montfort University -University of Coventry -University of Staffordshire		-Evidence Talks Ltd -Technology Risk Ltd -First Cyber Security Ltd -n-Gate Ltd -ManageMyProject (consultants)
Estonie	-Technology and Innovation Centre -Tallinn University of Technology		-Estonian Forensics Institute
Espagne	CNEC · Spanish National Centre of Excellence / Universidad Autonoma de Madrid		

Source recomposée: [http://www.2centre.eu/node/59].

Tableau 2: Lieux et institutions de recherches partenaires mobilisés par le projet européen «2 Centre - Cybercrime Centres of Excellence Network for Training Research and Education, 2010-2013».

enquêtes périodiques a joué un rôle non négligeable dans la prise de conscience de la vulnérabilité des entreprises et des particuliers. Mais au-delà du recensement quantifié des alertes par l'armada des conseillers stratégiques de prévention du «vol d'identité» ou des «atteintes à la réputation», les messages restaient confinés aux seules entreprises capables de les entendre et de s'y adapter. La montée des contentieux publics de masse, suscitant de nombreuses victimes individuelles escroquées ou atteintes dans leur vie privée, ne parvenait pas en revanche à être correctement enrayée.

On pourrait répondre à ce constat que l'enjeu de la prise de conscience politique n'était apparemment pas mûr en France, mais cette objection serait bien courte. Il faudrait au moins y ajouter que les notions pénales classiques assises sur la légalité des délits et des peines, ces outils du passé prétendant combattre les crimes du futur, ne se prêtaient visiblement plus à un enjeu partagé sur la maîtrise des dangers et des risques réels, en dépit des mises en garde du Conseil de l'Europe dans sa 1ère convention sur la cybercriminalité de Budapest le 23 novembre 2001 (Conseil de l'Europe, 2001). La perception collective des dangers de la navigation dans le cyberespace reste toujours relativisée, non parce qu'elle ferait l'objet de biais de perception psychologiques collectifs (Rochelandet, 2010), mais parce que les incitatifs idéologiques de la peur, trustés par trop d'experts privés ayant intérêt à formuler des diagnostics alarmistes pour accompagner une économie de services liés à la vente de matériels *techno sécuritaires* aux entreprises et aux particuliers, affrontent de puissantes résistances inhibitrices. Une résistance consensuelle à la victimisation d'actes dommageables propre au cybermonde ne fut pendant longtemps ni opératoire ni facilement opérationnalisable, et donc, d'un intérêt étatique assez inaudible. Il est pourtant manifeste que depuis presque trente ans (la première loi, dite Godfrain, sur la protection des données informatiques date de 1988), grâce notamment aux alertes de la CNIL, les *atteintes aux systèmes de traitement automatisés de données, les vols, destructions, et modifications de données* sont des incriminations entrées dans le livre 4 du code pénal français, en tant que nouveau corpus de délits ou crimes liés aux systèmes d'informations (Guillaneuf, 2011, 2012, 2013). Cette codification a eu son utilité: elle a au moins permis de situer les balises d'une *cybercriminalité* légalement saisie. Il est non moins avéré que le système de représentation pénal dominant par les juges chargés de la poursuivre en soit resté à la paralysie liée à des réflexes conservateurs, en dépit du vernis modernisateur dont on voulut bien affubler la délinquance astucieuse classique de l'escroquerie, de la contrefaçon, ou des fraudes à la carte bancaire. De ces atteintes classiques, on doit cependant noter une préoccupation émotionnelle de nature très différente venue de la pression de l'opinion publique, ayant suscité une réprobation et un désir de punition assez différents de la relative tolérance dont pouvaient bénéficier les dommages liés à la «délinquance astucieuse»: il s'agit de la *cyberpédophilie*. Cette préoccupation répressive a mordu sur une portion beaucoup plus vaste de la population, faisant rapidement consensus autour d'une criminologie articulée aux trois piliers classiques de Pinatel. Elle

avait matière à se ressourcer au sujet d'un nouveau crime vieux comme le monde (Ambroise-Rendu, 2014).

La connaissance quantifiée des *faits de cybercriminalité* parvenus à la connaissance des autorités à travers le prisme des catégories du droit pénal incriminateur a commencé à s'étoffer en France, grâce à la capitalisation annuelle de l'Observatoire National de la Délinquance et des Réponses Pénales, réceptacle de données provenant de toutes les administrations chargées de le renseigner (ONDRP-INHESJ, 2011, 773-901). La Justice y a elle-même abondamment puisé, alors qu'elle fut le dernier ministère régalien à définir les termes de son enjeu. La *cybersécurité* était en effet devenue de longue date un thème accaparé par l'Intérieur (au-delà d'un terrain d'entente entre agents de police judiciaire et magistrature éclairée), bien après que n'eurent été posés les fondamentaux de la *cyberdéfense,* plus de dix ans auparavant, objet dont, en France, Daniel Ventre fut un importateur dans le monde scientifique (Ventre, 2011, 2012, 2014b).

La *cybersécurité* est devenue un objectif de lutte fédérateur relativement précoce, grâce à la prise de conscience qui s'est opérée autour de la menace terroriste interne sur laquelle le gouvernement a demandé aux agences de la Direction centrale du Renseignement Intérieur - qui ont failli -, de s'y consacrer plus soigneusement. En dépit de toutes les passerelles que les analystes identifient désormais entre polices civiles et militaires dans la traque des dangers liés à la *cybercriminalité,* les querelles autour de l'ampleur et la hiérarchisation des menaces restent encore vivaces parmi ces administrations où la lutte des places pour le monopole de la définition des menaces légitimes le dispute encore aux considérations de compétence et d'efficacité, au cœur d'un État moderne qui prétend toujours à la maîtrise de sa souveraineté nationale.

II – L'enjeu cybercrime longtemps resté noyé dans celui de la cybersécurité

Il s'agit d'expliquer les raisons pour lesquelles, durant les dix dernières années, le monde militaire français s'est octroyé une longueur d'avance sur le monde policiaro-judiciaire avec la promotion du concept de *cyberdéfense* et de *cybersécurité* dans un contexte où l'État s'est montré beaucoup plus attentif à la nécessité de combattre (passivement et offensivement) des cyber-attaques majeures susceptibles d'affaiblir sa souveraineté. On peut mesurer la conversion progressive de la représentation des élites de l'État face aux usages de la *cyberdéfense* à partir du contenu de deux livres blancs ayant accompagné les lois de programmation militaire de 2008 et 2013. Après les attaques subies par l'Estonie qui marquèrent durablement les esprits en 2007, un premier Livre blanc de 2008 (Défense, 2008) prôna, en France, le passage d'une stratégie de défense passive à une stratégie de défense active, combinant la protection intrinsèque des systèmes, la surveillance permanente, la réaction rapide et l'action offensive. À ce moment-là, avait déjà été adoptée, par un décret du 23 février 2006, une vision biopolitique de la défense européenne par l'adaptation des États de l'Union aux dangers de leur affaiblissement, né des vulnérabilités

de leurs infrastructures critiques. Douze secteurs d'activités d'importance vitale (SAIV) furent identifiés en France comme devant particulièrement se protéger: trois secteurs étatiques (les activités civiles, militaires et judiciaires de l'État), trois secteurs de la protection des citoyens (santé; gestion de l'eau; alimentation), et six secteurs de la vie économique et sociale de la nation (les entreprises liées à l'énergie, transport, finances, industrie, communication, électronique) (10). Faits d'importance significative, naquirent dans la foulée du Livre blanc de 2008, deux innovations institutionnelles: le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) auprès du Premier ministre (Coursaget, 2010), et l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) par un décret du 7 juillet 2009. Nous formulons l'hypothèse que cette agence est rapidement parvenue à opérer la jonction opérationnelle entre les concepts de *cyberdéfense* et de *cybersécurité* dont l'État avait besoin en proposant une nouvelle doctrine ainsi définie: «*[la cybersécurité est] un ensemble des mesures techniques et non techniques permettant à l'État de défendre dans le cyberespace les systèmes d'information jugés essentiels*».

Sans cette doctrine finalement partagée et sans le travail de conviction souterrain du SGDSN et de l'ANSSI, il n'aurait guère été possible d'expliquer l'inflexion opérée cinq ans plus tard par la doctrine du deuxième Livre blanc de la Défense de 2013 (Défense, 2013), à la base de la nouvelle loi de programmation militaire pour les années 2014-2019. Laquelle fut accélérée par la survenue d'événements d'envergure mondialement médiatisée: d'une part, la sidération provoquée par la force des luttes subversives initiées par les réseaux sociaux («Printemps arabe»; *cyberhakers* libertaires de type Anonymous, etc.); d'autre part, le danger représenté par leur aptitude à dévoiler les secrets d'État apparemment les mieux gardés («affaire Snowden» et révélations de «l'affaire Prism» sur les capacités d'espionnage de l'intimité de chefs d'État en principe alliés). Le deuxième Livre blanc érigea le thème de la *cybersécurité* en nouveau référentiel majeur, en troquant définitivement celui de *cyberdéfense*, à la suite des conclusions du rapport confié par le gouvernement Fillon au sénateur J.-M. Bockel (2012), lequel hésitait encore entre les deux concepts lors de son officialisation. Le nouveau concept de *cybersécurité* était défini dans son rapport de la façon suivante: *l'état de sécurité recherché pour un système d'information qui doit permettre de résister à des événements issus du cyberespace, événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes offerts ou rendus accessibles par ces services. La* cybersécurité *fait appel à des systèmes d'information et s'appuie sur la lutte contre la* cybercriminalité *et sur la mise en place d'une* cyberdéfense (nous soulignons).

Autrement dit, on vit désormais se mettre explicitement en place l'idée d'un référentiel d'action entre la défense extérieure et la sécurité intérieure, comme un *continuum* en gésine depuis la naissance du concept de *sécurité/sûreté globale*, repérable en France depuis 2003 (Ocqueteau, 2006; Warusfel, 2011). Pour le politiste Florent Liéto (2014), la politique française de *cyberdéfense* se caractériserait par ce qu'il appelle un *procédé*. À rebours de nombre d'idées reçues

par les professionnels du champ propageant une doxa de la continuité de la défense du pays contre les attaques dont il serait la victime par l'intrusion d'ennemis extérieurs pour l'affaiblir, ce chercheur estime plutôt que la doctrine de la *cyberdéfense* française s'est fondée sur une double institutionnalisation, économique et stratégique, du thème du contre-espionnage industriel - lui-même transformé, à partir des années 1990, en rhétorique euphémisée *d'intelligence économique* -, sans qu'une connexion militaire et policière n'ait réellement été entreprise en terme d'action commune, sauf très tardivement. Il semble pourtant que l'année 2007 avec la crise estonienne (Ashmore, 2009; Herzog, 2011) ait constitué un tournant majeur, où des logiques d'action souterraines divergentes ou parallèles rencontrant des concurrences dans la position des leaderships au sein de l'État central, aient eu factuellement besoin de trouver à se relégitimer par de nouveaux référentiels plus consensuels entre eux.

La notion de «sécurité nationale» demeure tout à fait problématique au regard des standards historiques du positionnement des institutions régaliennes françaises. Les anciennes figures de l'*adversaire* et de l'*ennemi* départageant naguère le support institutionnel des menaces intérieures et extérieures se trouvent de plus en plus édulcorées (Conesa, 2011) face à l'apparition d'une menace majeure qui en a pulvérisé les frontières: la menace d'attaque *(cyber)terroriste* centrée sur les infrastructures critiques justifie le déploiement de plus en plus concerté des ressources militaires et policières, en France comme aux États-Unis. Un chercheur (Palluault, 2009) a pourtant montré comment l'administration Clinton avait, en réalité, préparé une politique de précaution autour des principales infrastructures critiques sans jamais avoir subi d'attentat terroriste majeur sur son sol, à la différence de la France, confrontée au problème depuis plus longtemps. L'administration Bush, construisant alors un «discours de guerre préventive contre l'ennemi», après les attentats de 2001, aurait su légitimer un Department of Homeland Security (DHS) qui n'aurait fait qu'intensifier, sous une allure publique plus offensive que défensive, les efforts de l'administration précédente pour protéger les infrastructures sensibles, y compris celles de l'information. Une décennie plus tard, une histoire a déjà été réécrite en France par un expert militaire satisfait de la convergence interministérielle prétendument réussie, qui la présente dans cette métaphore saisissante: *la cybersécurité (qui a détrôné la cyberdéfense) repose désormais sur trois piliers régaliens: le pilier du justicier (justice, police, gendarmerie, douane), le pilier du pompier (prévention et intervention de l'ANSSI), et le pilier du militaire (faiseur de guerre ou de paix à l'extérieur et/ou à l'intérieur de la Nation)* (Watin-Augouard, 2012, 31).

L'ANSSI, avons-nous dit, est devenue une agence tellement indispensable (passant de 100 agents de 2009 à 500 espérés en 2015) que ses diagnostics, rapports et conseils publics et privés inspirent et influencent directement l'actuelle normativité de la mise en protection des entreprises sensibles aux attaques de toute nature. Elles se préparent à fournir à l'État la possibilité de vérifier que les normes de résistance et de résilience aux attaques du *cyberterrorisme,* de l'espionnage industriel, du sabotage et de toute autres tentatives de

déstabilisation, soient plus effectives et efficaces que ce qu'elles n'auraient jamais été. Les conseils préventifs donnés par l'ANSSI depuis sa création aux entreprises sensibles font de moins en moins partie du domaine de leur libre appréciation. Ils se transforment en injonctions et quasi obligations imposées par l'État. L'actuel gouvernement s'apprête à obliger les opérateurs d'importance vitale (OIV) à déclarer à l'ANSSI les attaques, y compris formellement avortées, dont ils auraient été les victimes aux fins d'analyse, plutôt que de les sous-estimer en les tenant cachées à la concurrence.

III - Changements progressifs des postures de valorisation face aux failles du cyberespace

Toute l'œuvre du criminologue canadien Jean-Paul Brodeur (Brodeur, 2010) a consisté à montrer qu'en matière de *policing* public, le recours empirique à des actions considérées par le citoyen comme illégales constituait en réalité l'essence même d'actions ainsi analysées: *les agents de l'agir policier font partie de plusieurs organisations interconnectées autorisées, de manière plus ou moins contrôlée, à user de moyens généralement interdits au reste de la population, dans le but de faire respecter des règles et coutumes qui font la promotion d'un certain ordre social, que la société soit considérée dans sa globalité ou relativement à l'une de ses parties* (p.130, notre traduction). Ce qui inclut l'usage de la force pour les besoins des arrestations, l'accès privilégié à toutes sortes d'informations réservées, et, de manière plus générale, la capacité à recourir à tout acte de tromperie et de ruse justifiant la souveraineté de l'État. Il est clair que cette pétition documentée par toute une vie de recherche ressort, chez Jean-Paul Brodeur, d'une vision «réaliste» de l'action policière. Or, il en est une autre, plus «idéaliste» mais tout aussi vraie, qui consiste à lire le *policing* (le mandat de policer) par ses conditions de félicité. Elle consiste à considérer que l'atteinte de la noblesse de ses buts ultimes (tranquillité; ordre public par exemple), horizon défini en commun d'une société sans cesse remis sur le métier, est l'objectif par lequel les acteurs dédiés à leur mise en œuvre (se) justifient des (de leurs) pratiques légales et illégales octroyées pour les atteindre. C'est de cette distinction heuristique (réalisme/idéalisme) que nous partirons pour expliquer comment les thèmes de la *cyberdéfense* et *cybersécurité* ont précédé à l'agenda l'émergence du thème de la lutte contre *cybercriminalité* et, par voie de conséquence, à celui de la recherche critique.

3-1 - Le «réalisme» de la conquête par la cyberdéfense des puissants

À la fin de la guerre froide, le cyberespace s'est rapidement imposé comme un nouvel espace de conflits, d'insécurités et de menaces, dans lequel les États les plus puissants de la planète entendaient bien affirmer leur domination sur le reste du monde. Si le cyberespace offrit aux États-Unis des moyens décuplés pour maximiser leurs activités de renseignements, c'est au cœur même de son territoire ou de celui de ses alliés que de nouvelles fragilités sont apparues. La multiplication des *cyberattaques* contre les systèmes sensibles des États et de leurs infrastructures critiques les a contraints à considérer la sécurisation de

leurs systèmes de captation d'information comme une action prioritaire et à attribuer à des agences spécialisées le soin de les guider dans leurs missions de sécurité nationale. S'agissant de la défense de leur souveraineté, les États européens ont déployé des programmes de collecte de données et de surveillance pour mieux contrôler leurs flux migratoires. Il leur a fallu assurer dans un contexte international ouvert ultra concurrentiel, une certaine maîtrise de l'information économique, sociale et culturelle. Les acteurs publics et privés s'affrontent pour et par la maîtrise et l'exploitation de l'information ouverte et fermée, les systèmes étant de plus en plus utilisés à des fins agressives et défensives, d'autant que les *cyberattaques* sont désormais planifiées autant par des acteurs étatiques que non étatiques. Elles ne trouvent leur sens qu'en raison des stratégies qui les sous-tendent, mêlant savamment actions de renseignement, exploitation de l'information et des systèmes, opérations de déstabilisation dans le monde virtuel et réel selon des combinaisons très complexes.

La guerre de l'information comme la *cyberguerre* ne sont aucunement, dans la pensée réaliste, des vues de l'esprit. Il s'agit toujours d'imposer sa puissance: voir, contrôler, savoir, maîtriser l'information irriguant les systèmes décisionnels, militaires et civils. Les États sont de plus en plus souvent confrontés à des acteurs asymétriques portés à remettre en cause, via le Web 2.0, la légitimité de leurs attributs de puissance et le monopole de leur exercice. La technologie est devenue l'une des clés essentielles de l'enjeu de maximisation de la puissance. La réalité du théâtre des principales opérations militaires de la planète s'accompagne désormais de l'ISR (intelligence, surveillance, reconnaissance), indispensable complément de combat air-terre-mer, *via* la maîtrise des capacités satellitaires d'observation des drones militaires (Chamayou, 2013) et civils. Pour n'évoquer que les moyens européens disponibles, la «guerre réseau-centrique» s'appuie sur les systèmes GPS ou Galileo (Gros et *al.*, 2011) dont les capacités accroissent de manière démesurée la précision et la collecte de l'information située au sol. Le complexe militaro-industriel qui invente et vend aux armées ces systèmes est peu regardant sur les finalités de leurs utilisations. Ce sont les premiers garants de la puissance des États, mesurée à l'aune de leur meilleur accès aux nouvelles technologies de contrôle, de surveillance, de censure, et d'interceptions des communications, au nom de la *guerre préventive* contre le terrorisme, par exemple.

3-2 - L'«idéalisme» de la protection des internautes contre le cybercrime

Chaque État reste objectivement et subjectivement vécu par ailleurs comme un protecteur des populations de son territoire et des libertés de ses citoyens. À ce titre, la légitimité de la sanction des acteurs (organisés on non) qui attentent aux libertés anciennes et aux libertés nouvellement conquises par un accès décuplé à l'information disponible sur la Toile, reste un horizon assez peu discuté dans la société civile. Le mal et les malfaisants demandent toujours à être combattus par les administrations policières et judiciaires de *l'état de droit*, au sens large de ces termes. En France, la volonté de conjurer des dangers constitués par la *cybercriminalité,* un référentiel d'action publique devenu majeur, a mis

plus longtemps à se cristalliser dans son ordre interne. Mais depuis un petit lustre d'années, l'objectif a très rapidement mûri, au point d'avoir quasiment acquis ses lettres de noblesse médiatico-politiques, à défaut de les avoir acquises dans l'espace académique. On en veut pour «preuve» les deux indicateurs convergents suivants.

Dans l'espace médiatique d'abord…
Parmi les millions d'informations médiatiques qui circulent au sujet des menaces cybercriminelles, AEF Sécurité Globale, le segment spécialisé d'une agence dirigée par Raymond Soubie, occupe en France depuis quelques années une position majeure dans l'apport de connaissances à ce sujet. Cette agence offre une moisson riche et fiable d'informations factuelles diffusées à jets continus sur les questions de «*sécurité globale*». Une enquête menée par l'un de nous a passé au crible durant les 42 derniers mois (du 1er janvier 2011 au 10 juillet 2014), le contenu de cette rubrique, soit 9'506 dépêches publiées au jour le jour. Le système de capitalisation par accumulation des dépêches ventilées en deux grandes sous-rubriques a révélé 6'631 dépêches relatives à la «sécurité publique» (69,8 %) et 2'875 dépêches à la sécurité privée, industrielle et commerciale (30,2 %). Ces dépêches ont ensuite été triées par des entrées en mots-clés saisis à partir de leur titre et résumé liminaire. Au chapitre exclusif de la *cyberdéfense*, 24 dépêches se ventilent en informations relatives à la «sécurité publique» (n = 11) et à la «sécurité privée» (n = 13). Au chapitre exclusif de la *cybersécurité*, 173 dépêches se déclinent en informations relevant du secteur privé (n = 110 / 63,6 %) et du secteur public (n = 63 / 36,4 %) (11). De ces deux premières tendances, on peut déduire que les informations divulguées par le secteur industriel et commercial aux journalistes de l'AEF l'emportent sur les informations divulguées par les pouvoirs publics, ce qui n'a rien de très étonnant quand on sait que cette agence diffuse surtout une information payante vers un lectorat d'entreprises dotées, désireux de relayer ses stratégies de communication ou de bénéficier d'informations exclusives sur les tendances de son marché. L'intérêt de cette petite enquête réside surtout dans la mise en regard avec la sous-rubrique dédiée à l'entrée *cybercriminalité,* dont on a dit *supra* le peu de cas qu'en avaient fait jusqu'à présent les banques de données scientifiques*.* 135 dépêches de l'AEF concernent cette sous-rubrique, qui se ventile pour 89 d'entre elles (65,9 %) dans celle de la «sécurité publique», 46 concernant celle de la «sécurité privée» (34,1 %). Ce rapport inversé tendrait donc à prouver que ce thème serait devenu non seulement une stratégie de communication de l'État, mais surtout une préoccupation de lutte majeure pour les pouvoirs publics européens et français en l'espace de quelques années seulement, au point d'avoir détrôné l'espace médiatique général auparavant focalisé sur la *cybersécurité* sur ce support.

Dans la pratique des ministères, ensuite
Les pouvoirs publics ont fini par entendre les invitations pressantes pour agir parmi les experts publics les plus reconnus de la *cybercriminalité* [Quéméner

(Justice); Chambon (Police); Freyssinet; Watin-Augouard (Gendarmerie)]. Une feuille de route dûment signée à l'automne 2013 par Manuel Valls, ex-ministre de l'Intérieur et Christiane Taubira, Garde des Sceaux, au magistrat Marc Robert, a permis, au bout de six mois d'efforts interministériels, de produire un rapport original où se sont ajustées les représentations et actions professionnelles les plus disparates autour d'un diagnostic partagé. Dans les plus hautes sphères de l'État, la France, sous les injonctions de l'Union européenne, vient enfin d'y reconnaître un danger *sui generis* lié à la *cybercriminalité.* Le rapport de Marc Robert (Robert, 2014) officialisé en juin 2014, de vocation rassurante (12), met en avant le besoin de «protection des internautes», plutôt que celui de traquer et de châtier les cybercriminels. L'importance symbolique de son diagnostic ne doit pas être sous-estimée. Il affirme d'abord que la mesure du phénomène à conjurer par les ressources pénales est délicate, la *cybercriminalité* ayant besoin d'être fondée sur une définition légale assez large pour l'instant inexistante. En dépit d'une proposition frontale pour en définir l'objet (13), le rapport admet qu'elle demeure très insuffisante puisque la réalité saisie continuerait d'en être bifide. Ou bien le *cybercrime* ne serait qu'un moyen pour commettre une infraction de droit commun, sa spécificité résidant dans des actions spécifiques dirigées contre le système d'information lui-même (définition étroite). Ou bien, la *cybercriminalité* appartiendrait à des constellations d'infractions de droit commun commises au moyen des nouvelles TIC pour véhiculer des contenus illicites ou faciliter la communication de toute autre infraction classique (définition large). Le rapport prend acte que les solutions opérationnelles des différents ministères resteraient entravées par une faible connaissance des *victimes* et de leurs préjudices, en dépit des enquêtes annuelles de l'ONDRP auprès des ménages signalées *supra*, cet Observatoire ayant joué un rôle apparemment déterminant dans la préparation de l'identification des ressources utiles à la confection de ce rapport. Mais surtout, il montre que les services judiciaires restent encore plus démunis que les polices, en raison de la rareté des plaintes, des dénonciations et des saisines d'office liées aux *cyberdélinquances*. Seules, en effet, des données de quantification disparates, lacunaires et parcellaires parviennent à la connaissance des autorités judiciaires - il y a du mérite à le reconnaître -, alors que maintes d'entre elles sont saisies dans des dispositifs de prévention et de régulation non pénaux. Il nous semble que ce rapport est parvenu à synthétiser pour la première fois une véritable mise en mots des «auteurs» cibles concernés, ennemis ou adversaires de la société ou de l'État, par une ventilation de grandes catégories d'acteurs reflétant l'entendement du spectre des ministères régaliens: ceux qui s'attaquent aux membres de la société civile (les *cybercriminels de droit commun,* parmi lesquels les *cyberdélinquants sexuels*, les *cyberviolents* et les *cyberescrocs*); ceux qui s'attaquent aux entités étatiques et aux OIV (les *cybermercenaires*, les *cyberespions*, les *cyberterroristes*) et ceux des deux catégories précédentes qui se distinguent surtout d'après leur mode opératoire (ceux qui attaquent le matériel dans un objectif financier ou «politique», saboteurs et/ou détourneurs de données). Par le biais de cette récente opération de labellisation «consensuelle»

des cibles à combattre pour protéger la société et l'État, vient de se cristalliser, pour la première fois en France, une demande de connaissances «criminologiques» implicites, jusqu'à présent mal formulée par l'État.

Conclusion

Nous souhaitons plaider pour que la préoccupation d'une criminologie débridée au sujet du *cybercrime*, de la *cybercriminalité* et du *cybercriminel* puisse s'émanciper de son carcan pénal classique. À la condition que les chercheurs et analystes veuillent bien se pencher désormais non pas uniquement sur des profils de victimes, mais plutôt sur une meilleure compréhension des attitudes de protection de la société civile à l'égard des risques et des usages sociaux de la Toile, des différents sens qu'elle peut attribuer aux pratiques de *hacking* et des modalités de régulation des désordres, pertes et dommages que des attitudes sans doute trop négligentes sont susceptibles d'y engendrer.

Car le profil des *hackers* (Dupont, 2012; 2014a) n'est évidemment pas la fin de l'analyse du domaine du *cybercrime*, pas plus que la conduite du criminel ou de sa victime n'a jamais été la fin de la compréhension du système pénal. Il convient plutôt, en s'inspirant des apports de cette récente mission du *groupe de travail interministériel sur la lutte contre la cybercriminalité*, de s'en démarquer en focalisant l'attention sur quatre types de recherche programmatiques susceptibles d'en renforcer la légitimité, et cela, indépendamment des suites politiques qui lui seront données.

La première serait d'étudier les intérêts réellement défendus par les penseurs et les praticiens de la gestion des risques dans le cyberespace en effectuant des recherches en consortium sur ce que l'on pourrait appeler des «*gestionnaires du sens*» ou des «*entrepreneurs de morale*» de sécurisation des mondes réels et virtuels en réseaux et de chercher à mieux documenter comment, à travers l'abondante littérature journalistique ou techniciste, catastrophiste ou relativiste (littérature grise), s'y sont historiquement construits les schèmes perceptifs des menaces et des immunités face aux vulnérabilités.

La deuxième serait d'engager des recherches sur les réformes et les incidences des nouveaux dispositifs institués de lutte contre les risques au sein des agences de renseignement publiques et parapubliques. Et cela, quand bien même valoriseraient-elles de nouvelles formes de compétences dans le domaine de la *cyberdéfense* ou du *cybercrime*, en se centrant sur les conditions d'une meilleure élucidation de l'effectivité du travail de celles et ceux officiellement et officieusement en charge de sa mise en œuvre avec les hébergeurs et les fournisseurs d'accès.

La troisième serait d'engager, auprès des usagers et des populations les plus ou les moins *digitalisées*, des recherches socio-psychologiques sur les rapports d'interaction et d'apprentissages normatifs des machines robots avec les êtres humains. Il s'agit désormais de s'aventurer empiriquement sur des terreaux anthropologiques et civilisationnels au vu de la croissance phénoménale

des objets de la robotique interconnectés dans tous les moments de la vie quotidienne des individus.

La dernière serait d'engager des recherches sur l'économie du coût des processus technologiques et les recompositions des usages du travail de la sécurisation générale (14), à partir d'un fascinant paradoxe, à transformer en postulat de toute nouvelle recherche sur les usages publics et privés de sécurisation des technologies d'information et de communication. Car les TIC se présentent à la fois comme de nouveaux vecteurs de vulnérabilités pour les États, les entreprises et les citoyens, et simultanément comme des facteurs de solutions à leurs propres vulnérabilités. Il nous semble que, montrer toutes les implications économiques, culturelles et institutionnelles de ce paradoxe saisi par une multiplicité de sciences humaines, contribuerait à remettre à sa plus juste place le dispositif sur lequel sont assis les fondamentaux d'une *cyber-criminologie* trop pénalocentrée.

Bibliographie

AMBROISE-RENDU A.-C., (2014), *Histoire de la pédophilie, XIXe-XXIe siècle*, Paris, Fayard.

ASHMORE W. C., (2009), Impact of Alleged Russian Cyber Attacks, *Baltic Security and Defence Review*, 11, 4-40.

BARLOW J. P., (1996), A Declaration of the Independence of Cyberspace, [*on line*] [http://editions-hache.com/essais.pdf/barlow1.pdf].

BOCKEL J.-M., (2012), *Rapport d'information sur la cyberdéfense*, Paris, Sénat, Journal Officiel, n° 681.

BOSSAN J., (2013), Le droit pénal confronté à la diversité des intermédiaires de l'Internet, *Revue de science criminelle et de droit pénal comparé*, 2, 295-319.

BRENNER S. W., (2010), *Cybercrime: Criminal Threats from Cyberspace*, Santa Barbara, Praeger.

BRETON P., BERTRAND I., HEILMANN É., (1991), Entre l'ordre et le désordre: les valeurs paradoxales du monde de l'informatique, *Réseaux*, 48, 13-22.

BRODEUR J.-P., (2010), *The policing Web*, Oxford, Oxford University Press.

CHAMAYOU G., (2013), *Théorie du drone*, Paris, La Fabrique.

CONESA P., (2011), *La fabrication de l'ennemi, ou comment tuer avec sa conscience pour soi*, Paris, R. Laffont.

CONSEIL DE L'EUROPE, (2001), *Convention de Budapest sur la cybercriminalité* adoptée le 13 novembre [http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm].

COURSAGET A., (2010), La sécurité des activités d'importance vitale: premier bilan du SGDSN, *Sécurité et Stratégie*, 2010, 4, 5-18.

DÉFENSE, (2008), *Défense et sécurité nationale. Livre blanc,* Paris, O. Jacob-La documentation française.

DÉFENSE, (2013), *Livre blanc. Défense et sécurité nationale*, Paris, ministère de la Défense.

DUPONT D., (2012), Nouvelles technologies et crime désorganisé: incursion au cœur d'un réseau de pirates informatiques, *Sécurité et Stratégie*, 11, 25-38.

DUPONT D., (2014a), Skills and Trust, A tour inside the hard drives of computer hackers, *in* C. MORSELLI (ed.), *Crime and networks*, N.Y., Criminology and Justice Studies Series, Routledge, 195-217.

DUPONT D., (2014b), Les «cybercrimes» sont-ils solubles dans la criminologie? *Communication à l'Atelier 1 du 14e colloque de l'AICLF*: «Hackers, Cyber-barbouzes et chercheurs», Liège, 18 mai.

DUPONT B., GAUTRAIS V., (2010) Crime 2.0: le web dans tous ses états!, *Champ pénal/Penal field* [En ligne], Vol. VII | [http://champpenal.revues.org/7782; DOI: 10.4000/champpenal.7782].

FENSTER M., (2012), Disclosure's effects: WikiLeaks and Transparency, *Iowa Law Review*, 97, 753-806.

FERAL SCHUHL C., (2012), *Cyberdroit. Le droit à l'épreuve de l'Internet*, Paris, Dalloz-Praxis, 6e éd.

GANASCIA J.-G., (2009), *Voir et pouvoir: qui nous surveille?,* Paris, Les Essais du Pommier.

GREENWALD G., (2014), *No place to hide: Edward Snowden, the NSA, and the US Surveillance State*, London, Hamish Hamilton.

GROS F., (2012), *Le principe sécurité*, Paris, Gallimard Essais.

GROS P., VILBOUX N., KOVACS A., COSTE F., KLEIN M., MASSARD A., (2011), *Du network-centric à la stabilisation: émergence des «nouveaux» concepts et innovation militaire contemporaine*, Paris, IRSEM, Études de l'IRSEM, n° 4, ronéo.

GUILLANEUF J., (2011), La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet: éléments de mesure et d'analyse, *in* INHESJ-ONDRP, *La criminalité en France*, Paris, CNRS éd., 843-847.

GUILLANEUF J., (2012), La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet, *in* ONDRP-INHESJ, *La criminalité en France*, Paris, CNRS éd., 391-398.

GUILLANEUF J., (2013), La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet: éléments de mesure et d'analyse pour l'année 2012, *in* ONDRP-INHESJ, *La criminalité en France*, Paris, CNRS éd.

HERZOG S., (2011), Revisiting the Estonian Cyber Attacks: digital threats and multinational responses, *Journal of strategic security*, 4, 2, 49-60.

HOLT T. J., BOSSLER A. M., (2014), An assessment of the current state of Cybercrime Scholarship, *Deviant Behavior*, 35, 1, 20-40.

LEMAN-LANGLOIS S. (ed.), (2008), *Technocrime, technology, crime and social control*, Collumpton, Willan Publishing.

LIANOS M., (2001), *Le nouveau contrôle social: toile institutionnelle, normativité et lien social*, Paris, L'Harmattan.

LIÉTO F., (2014), «De l'intelligence économique à la cyber-défense. Aperçu socio-historique du discours d'insécurité des systèmes d'information en France, 1989-2011», *Communication à l'Atelier 1 du 14e colloque de l'AICLF*: «Hackers, Cyber-barbouzes et chercheurs», Liège, 18 mai.

LUPÁRIA L. (dir.), (2012), *Internet provider e giustizia penale: modelli di responsabilità e forme di collaborazione processuale*, Milan, Giuffré.

MALLET-PUJOL N. (dir.), (2006), *Traçages électroniques et libertés*, Paris, La documentation française, Problèmes politiques et sociaux, n° 925.

MUSSO P., (2000), Le cyberespace, figure de l'utopie technologique réticulaire, *Sociologie et société*, 32, 2, 31-56.

OCQUETEAU F., (2006), Sécurité nationale et sécurité globale: l'adaptation des services de renseignements français, *Canadian Journal of Criminology and Criminal Justice / Revue Canadienne de Criminologie et de Justice Pénale*, 48, 3, 435-452.

OCQUETEAU F. (dir.), (2010), *Polices et politiques de sécurité. Concilier efficacité et respect des libertés*, Paris, La Documentation Française, Problèmes Politiques et Sociaux, n° 972.

OCQUETEAU F., (2011), Chefs d'orchestre de la sûreté des entreprises à l'ère de la sécurité globale, *Champ Pénal/Penal Field*, VIII.

OCQUETEAU F. (2014), Comment l'enjeu de la cybercriminalité est-il entré dans le champ de préoccupation des pouvoirs publics français? *Communication à l'Atelier 1 du 14e colloque de l'AICLF*: «Hackers, Cyber-barbouzes et chercheurs», Liège, 18 mai.

OCQUETEAU F., VENTRE D. (dir.), (2011), *Contrôles et surveillance dans le cyberespace*, Paris, La Documentation française, Problèmes économiques et sociaux, n° 988.

ONDRP-INHESJ, (2011), «La cybercriminalité», *in La criminalité en France 2011*, Paris, CNRS éd., p 773-901.

O.N.U., (2000), *Résolution des Nations Unies sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles*, A/RES/55/63.

QUÉMÉNER M., FERRY J., CHARPENEL Y., WATIN-AUGOUARD M., (2009), *Cybercriminalité: défi mondial*, Paris, Economica.

PALLUAULT O., (2009), *Stratégie de la précaution, la construction de la protection des infrastructures critiques aux États-Unis, 1993-2003,* Paris, Thèse de science politique, Univ. Paris II-Assas.

PARKER D. B., (1976), *Crime by computer*, New York, Ch. Scribner's son, 1st ed.

ROBERT M. (dir.) (2014), «*Protéger les internautes», Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité
[http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf]
[http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite_annexes.pdf].

ROCHELANDET F., (2010), *Économie des données personnelles et de la vie privée*, Paris, La Découverte/Repères.

ROSA H., (2010), *Accélération, une critique sociale du temps*, Paris, La Découverte.

SABATHÉ J.-M., (2010), La mise en œuvre du décret SAIV par EDF, *Sécurité et Stratégie*, 4, 19-22.

SÁNCHEZ ESTOP J. D., (2014), WikiLeaks: Abbé Barruel to Jeremy Bentham and Beyond, A Short Introduction to the New Theories of Conspiracy and Transparency, *Cultural Studies*, 14, 1, 40-49.

VENTRE D., (2011), *Cyberespace et acteurs du cyberconflit*, Paris, Hermès-Lavoisier.

VENTRE D., (2012), Le cyber-guerrier: nouvelle figure combattante au service de la cyber-défense, *Sécurité et Stratégie*, 11, 39-48.

VENTRE D., (2014a), «Cybercriminalité: état de l'art de la recherche académique en Europe», *Communication à l'Atelier 1 du 14e colloque de l'AICLF*: «Hackers, Cyber-barbouzes et chercheurs», Liège, 18 mai.

VENTRE D., (2014b), *Impact de la cyberguerre sur les conflits armés,* Thèse de doctorat en science politique, St Quentin en Yvelines, Université Versailles St Quentin.

WALL D., (2007), *Cybercrime: the transformation of technology in the network age,* Cambridge, Polity Press.

WARE W. H., (1967), *The computer in your future*, Santa Monica, Rand Corporation.

WARUSFEL B., (2010), La protection des réseaux numériques en tant qu'infrastructures vitales, *Sécurité et Stratégie*, 4, 31-39.

WARUSFEL B., (2011), La sécurité nationale, nouveau concept du droit français, *in* COLLECTIF, *Les différentes facettes du concept juridique de sécurité – Mélanges en l'honneur de Pierre-André Lecocq,* Lille, U. Lille2, 461-476.

WATIN-AUGOUARD M., (2012), «La cybersécurité», Pour un ordre public du cyberespace, *Revue de la gendarmerie nationale*, 4, 31-36.

WILLIAMS M., WALL D., (2013), "Cybercrime", *in* HALE C., HAYWARD K., WAHIDIN A., WINCULP E. (eds), *Criminology*, 3rd ed., Oxford, Oxford Univ. Press, 247-266.

Notes

1 On doit la fortune de ce terme apparu en 1982 sous la plume de William Gibson et à son roman futuriste *Neuromancien.*

2 Une sphère imaginaire enveloppant la planète parcourue d'incessants flux d'informations au sein de laquelle vivent et coexistent les humains et les organismes informationnels (*orins*), participant tout autant de la biosphère que de la logosphère.

3 Du nom du programme de surveillance électronique mondial mis au point aux USA par la NSA (FISC), révélé par E. Snowden le 6 juin 2013.

4 Toutes choses étant égales par ailleurs, elle paraît consonante avec la série établie par le programme de Google (Ngram-Viewer) qui a indexé un million d'ouvrages de 1800 jusqu'à nos

jours. Quand on y croise les entrées *cybercrime* et *computer crime*, des pics sont atteints en 2001 et 2007, mais, à la différence de nos résultats sur les supports de revues, c'est le premier terme *cybercrime* qui y a pris le pas sur le second *computer crime*, dès 2001. https://books.google.com/ngrams/graph?content=cybercrime%2Ccomputer+crime&year_start=1800&year_end=2008&corpus=1&smoothing=3&share=&direct_url=t1 %3B %2Ccybercrime %3B %2Cc0 %3B.t1 %3B %2Ccomputer %20crime %3B %2Cc0.

5 À noter qu'un nouveau projet européen vient d'être lancé en 2014, où l'Université de Münster (Allemagne), partenaire principal au projet, se propose d'analyser les impacts économiques de la cybercriminalité. Cf. Programme ECRIME (Economic Impacts of Cybercrime).

6 Le CLUSIF (Club de la Sécurité de l'Information Français) est une association d'entreprises, collectivités territoriales et administrations fondée en 1985 dont la raison sociale est d'agir pour la sécurité de l'information, sensibiliser les acteurs, aider à mieux sécuriser les réseaux. Il publie depuis douze ans une enquête sur les menaces informatiques sollicitées auprès d'entreprises supérieures à 200 salariés et d'un millier d'internautes.

7 Sur ce dernier point, Warusfel, 2010.

8 L'ANSSI étant abondamment citée, de manière peut-être discutable, comme une agence de conseil relevant du secteur privé plutôt que du secteur parapublic, bien qu'elle ait été créée par les pouvoirs publics.

9 AEF Sécurité Globale, Dépêche n° 83661 du 8 juillet 2014: «*Notre premier objectif était d'être pédagogique*» (Marc Robert, président du groupe de travail sur la cybercriminalité).

10 *La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet* (Rapport M. Robert, 2014, p.12).

11 Comme semble en avoir pris récemment conscience la Commission Européenne en lançant le 10 décembre 2013, dans son programme Horizon 2020, sa demande de connaissances sur la contribution des sciences forensiques à la lutte contre le cyberterrorisme par exemple. Cf. European Commission Decision C (2014) of 2014: «Work programme 2014-2015 / 14. Secure societies – Protecting freedom and security of Europe and its citizens».