RÉFLEXIONS STRATÉGIQUES

PRÉOCCUPANTS, INSPIRANTS, PASSIONNANTS… DÉCOUVREZ À TRAVERS CES ARTICLES RÉFLEXIONS STRATÉGIQUES, LES SUJETS ET EXTRAITS DE MÉMOIRES RÉALISÉS PAR LES AUDITEURS DU MBA MANAGEMENT DE LA SÉCURITÉ.

#CYBERATTAQUE #SOUVERAINETÉ #CONTINUUM

Optimisation de la lutte contre les cyber-criminalités : équilibre entre souveraineté et acteurs privés.

AUTEUR :
CAROLINE
JUIN 2020

Optimisation de la lutte contre les cyber-criminalités : équilibre entre souveraineté et acteurs privés.

Auteur : CEN Caroline, auditrice de la 6ème promotion.

« Arrêtons d'être naïf sur la souveraineté du numérique ». Par cette invective, Florian BACHELIER député d'Ile et Vilaine souhaite réveiller les consciences en invitant les décideurs à prendre toute la mesure de notre perte d'autonomie face au tout numérique. Pourtant le tintement de cette alarme résonne depuis plusieurs années. En 2014, Pierre BELLANGER alertait déjà les décideurs de la suprématie des Etats-Unis dans un monde du tout numérique.

Autrefois pouvoir du Roi, la souveraineté appartient désormais au peuple comme en atteste l'article 3 de la Constitution Française. La souveraineté nationale consiste en la capacité de l'Etat, en qualité de représentant du peuple, d'agir et de décider en toute autonomie sans être soumis à un autre Etat. Celle-ci, repose notamment sur les traités de Westphalie et la sacralisation des frontières. Elle s'exprime par un certain nombre d'attributs de pouvoir à savoir : celui de faire la loi, de rendre justice, de battre monnaie, de lever l'impôt et de faire la guerre. Cette conception de la souveraineté est remise en question par la transformation engendrée par le numérique. Fondé sur une tradition d'ouverture technologique et de circulation de l'information, Internet s'affranchit des frontières et transcende le pré carré autrefois réservé à l'Etat, par l'utilisation de protocoles universels qui en font le réseau des réseaux. Là où Marshall MCLUHAN parlait d'un village planétaire, John Perry BARLOW faisait un véritable plaidoyer pour enjoindre les Etats à ne pas empiéter sur le cyberespace. « Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté là où nous nous rassemblons (1) ».

Conçu comme une dimension parallèle, le cyber espace innerve désormais tous les pans de la société et transforme notre monde en profondeur. Pour s'en convaincre, il suffit de décortiquer la journée type d'un citoyen. Du matin au soir, nous sommes connectés (Cloud, montre connectée, aspirateur programmable, Bluetooth, applications pour smartphone, paiement en ligne, déclaration d'impôt, messagerie, visioconférence…). La fiction décrite par Dave EGGERS (2) est aujourd'hui une quasi-réalité. Quel que soit son environnement familial, professionnel, institutionnel ou amical, l'homme interagit au quotidien avec la machine et communique via des protocoles. Notre monde, nos usages et nos modes de vie sont devenus numériques. Cette transformation est caractérisée par une contraction du temps dont la vitesse de mutation est exponentielle. En 1969, 4 ordinateurs étaient connectés ensemble. Aujourd'hui, on estime à 24 milliards le nombre d'appareils connectés. Plus de 4,5 milliards de personnes utilisent Internet. En moyenne, la population mondiale passe 2h24 par jour sur les réseaux sociaux. En 2018, on estime à 33 zettaoctets la quantité de données créées dans le monde. Demain, l'informatique quantique bouleversera nos habitudes cryptographiques.

Optimisation de la lutte contre les cyber-criminalités : équilibre entre souveraineté et acteurs privés.

Auteur : CEN Caroline, auditrice de la 6ème promotion.

Cette révolution représente à la fois une formidable opportunité mais également un véritable champ de mines. Opportunité en ce qu'elle permet de décloisonner le monde, de réaliser des gains de temps, d'étendre les capacités de stockage et de perfectionner les capacités d'analyse pour anticiper les besoins et les risques. Elle représente également un risque pour notre souveraineté comme en témoigne le scandale Cambridge Analytica. Si l'analyse de la donnée permet d'anticiper les besoins, de prévenir les risques, elle permet également de prédire les comportements et de façonner l'opinion des foules par des campagnes d'influences ciblées, de nature à entraver le libre jeu démocratique. Ainsi le scandale Cambridge Analytica a laissé planer un soupçon d'ingérence russe (3) dans l'élection présidentielle américaine de 2016.

La transformation numérique est une véritable métamorphose qui bouleverse les équilibres géopolitiques. Dans cette ère du numérique, exclure l'Etat du cyberespace comme le souhaitait John Perry Barlow, reviendrait à remettre en question son existence même. Voeux pieux ou prémonitions, les attributs de la souveraineté sont aujourd'hui concurrencés par les GAFA (4) et autres géants du net. Dans ce jeu d'échec géostratégique, certaines entreprises privées ont désormais acquis les moyens de concurrencer les Etats par leur poids économique mais également par la richesse de l'information qu'elles détiennent. Est-ce à dire que l'Etat n'a plus sa place dans ce monde hyperconnecté ? Avons-nous trop tardé à réagir aux sirènes d'alarme qu'a fait retentir Pierre Bellanger ? S'il existe de multiples signaux attestant de l'affaiblissement de la souveraineté des Etats dans l'espace numérique, il ne faut pas oublier que la montée en puissance des GAFA est récente. Mais, il ne faut pas se leurrer sur la politique industrielle des Etats-Unis qui ont activement participé au financement des technologies clés qui font aujourd'hui la puissance de ces entreprises. La souveraineté de l'Etat ne peut être pensée sans une stratégie d'autonomie technologique et numérique. Comme le souligne Bernard Benhamou, « à mesure que les technologies numériques se développent dans l'ensemble des champs de l'activité économique et politique de nos sociétés, elles modifient les dynamiques de pouvoir entre les acteurs privés et les États, mais aussi entre les États eux-mêmes (5) ». Le cyber-espace est devenu un enjeu de géopolitique qui redessine le monde. Ce monde au mythe fondateur libertaire s'est mué en espace conflictuel dans lequel chacun veut affirmer sa souveraineté tout en imposant aux autres des règles extraterritoriales. La guerre froide s'est transformée en guerre économique et numérique où les USA ont acquis une position dominante et où la Chine prend son envol. Si nous ne voulons pas demain être une simple colonie des deux autres continents, il est temps de réagir (6). Entre le capitalisme de la donnée et la surveillance de masse du crédit social (7), le défi de demain consiste pour l'Europe à être en mesure d'incarner une troisième voie pour un Internet libre mais protecteur des personnes et des biens.

Optimisation de la lutte contre les cyber-criminalités : équilibre entre souveraineté et acteurs privés.

Auteur : CEN Caroline, auditrice de la 6ème promotion.

« À l'heure où les systèmes sont de plus en plus interconnectés, la transformation numérique est à la fois marqueur de progrès et catalyseur de risques (8) » tant pour le jeu démocratique que pour la sécurité des personnes physiques et morales. Or la notion de sécurité est au centre des prérogatives régaliennes. L'État tient son pouvoir du contrat social par lequel l'individu accepte une discipline collective fondée sur la loi en contrepartie d'une protection. Dès lors, si l'Etat n'est plus en mesure d'assurer la protection des citoyens face au cyber-menaces, son existence peut être remise en question. Or la cybercriminalité se caractérise par une augmentation continue de faits. Le rapport cyber-menace élaboré chaque année sous l'égide de la délégation ministérielle aux industries de sécurité et à la lutte contre les cyber-menaces (DMISC) dresse un panorama de cette cybercriminalité et des nouveaux défis induits par ces nouvelles formes de délinquance.

L'absence de définition universellement partagée par la communauté internationale est un premier frein à une lutte optimale contre les cyber-criminalités. Celle-ci est définie par la commission européenne comme « toute infraction qui implique l'utilisation des technologies informatiques (9) ». Selon l'ONU, la cybercriminalité désigne « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique (10)». Nous retiendrons la définition du groupe de travail interministériel sur la lutte contre la cybercriminalité qui a le mérite d'être simple et compréhensible par tout le monde. 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 ».

Généralement, on distingue 2 grandes formes de cyber-criminalités : les infractions facilitées par l'utilisation du numérique et les infractions spécifiques. Concernant les infractions facilitées, les délinquants reproduisent les criminalités traditionnelles sur les réseaux et adaptent leur mode opératoire pour tirer profit du numérique. Ils utilisent les réseaux de communication électronique pour toucher un maximum de victimes à faible coût (exemple : campagnes de phishing). Dans cette forme de criminalité, Internet n'est qu'un moyen, un amplificateur de la délinquance. En revanche, pour les infractions dites spécifiques, le système d'information en est la cible.

Aujourd'hui, les cyber-criminalités explosent et touchent aussi bien les particuliers, les collectivités territoriales, les associations que les entreprises. Cependant, pour limiter notre étude nous nous intéresserons qu'aux relations entre l'Etat, les forces de l'ordre et les entreprises. Le délinquant, en qualité d'agent rationnel, profite de toutes les opportunités offertes par les nouvelles technologies. Or, le cyber-espace lui permet de maximiser son gain par la multiplication du nombre de victimes, tout en réduisant le coût de son attaque et les chances d'identification par les forces de l'ordre (VPN, cryptomonnaie, extraterritorialité). Autrement dit, le cyber-délinquant n'a jamais été aussi loin de son juge et aussi proche de sa victime.

Optimisation de la lutte contre les cyber-criminalités : équilibre entre souveraineté et acteurs privés.

Auteur : CEN Caroline, auditrice de la 6ème promotion.

Plus inquiétant, avec le développement du crime as a service, la cybercriminalité n'est plus seulement une affaire de spécialistes. Dans ce contexte de plus en plus complexe où le numérique est devenu un moyen pour le délinquant mais également une arme qui bouleverse les équilibres géopolitiques, qu'attendons-nous pour réagir et repenser notre manière de lutter contre les cybermenaces ?

L'appel de Paris sera-t-il un énième appel au sursaut où le commencement d'une véritable révolution dans la stratégie de maintien de notre souveraineté numérique ? La France a déjà manqué certaines occasions majeures (11) de prendre l'ascendant, saura-t-elle aujourd'hui peser et légitimer sa place ? L'Etat a -t-il encore une légitimité et un rôle à jouer dans ce monde hyperconnecté ou a-t-il déjà perdu toute capacité à agir ? L'explosion de la cybercriminalité, n'est-elle pas le révélateur d'un Etat qui peine à protéger les personnes, les biens et les intérêts de la nation avec les instruments traditionnels (Droit, compétence juridictionnelle, coopération) ? Si la force de la souveraineté repose sur la nation, la solution optimale ne consiste-t-elle pas à s'appuyer sur les acteurs privés pour en démultiplier les effets et agir en amont de la criminalité ? Associer les acteurs privés de natures et de nationalités différentes, n'est-ce pas un pari risqué pour notre souveraineté ? L'Etat n'est-il pas un peu schizophrène à vouloir responsabiliser les entreprises sur le mode de la coopération tout en s'inquiétant du pouvoir détenu par les géants du net ?

Dans un monde en perpétuel changement, l'Etat doit se réinventer et penser la lutte contre la cybercriminalité différemment pour être en mesure de légitimer sa présence en assumant sa mission régalienne de protection des personnes et des biens. Si nous ne pouvons plus combattre la cybercriminalité sans l'aide des acteurs privés, il convient d'encadrer la production de coopération. Pour définir les contours de ce cadre, la France a tout intérêt à agir en symbiose avec l'Europe pour peser sur la scène internationale et à mobiliser l'ensemble des acteurs dans un but commun consistant à offrir un service et un écosystème de qualité pour mieux protéger les entreprises. Si elles veulent peser sur la scène internationale, la France et l'Europe ne peuvent se contenter d'une simple déclaration de valeur, elles doivent concevoir une autonomie stratégique au travers d'une approche systémique.

Comment concevoir et décliner au niveau gendarmerie, un continuum de cybersécurité qui permette de réinventer la lutte contre les cyber-criminalités en associant les entreprises, sans nous départir de notre souveraineté?

Après avoir fait le constat de la fragilité de notre souveraineté face à la transformation numérique, nous analyserons le rôle et les leviers à disposition de chacun des acteurs pour définir la meilleure stratégie de lutte contre les cyber-menaces.

Optimisation de la lutte contre les cyber-criminalités : équilibre entre souveraineté et acteurs privés.

Auteur : CEN Caroline, auditrice de la 6ème promotion.

Enfin, nous verrons comment la gendarmerie peut la décliner à son niveau en offrant un véritable service aux entreprises de nature à améliorer la lutte contre les cyber-criminalités. S'il existe de multiples signaux attestant de l'affaiblissement de la souveraineté des Etats, la transformation numérique peut également être une véritable opportunité (Titre 1). Dans un monde en perpétuel changement, l'Etat doit se réinventer pour être en mesure de légitimer sa présence en assumant sa mission régalienne de protection des personnes et des biens tout en étant le chef d'orchestre de cette transformation numérique (Titre 2). Le défi de la gendarmerie réside dans sa capacité à réinventer la lutte contre les cyber-criminalités en proposant aux entreprises un service coopératif de nature à améliorer leur sécurité (Titre 3).

(1) BARLOW, John Perry. « Déclaration d'indépendance du cyberespace », dans BLONDEAU Olivier, Libres enfants du savoir numérique Une anthologie du "Libre", Editions de l'Éclat, 2000, p. 47-54.
(2) EGGERS Dave, Le cercle, Ed Gallimard, Collection Du monde entier, 2016, 528 p. (3) MUELLER Robert, Report on the investigation into Russian interference in the 2016 presidential election, US Departement of justice, Mars 2019, consulté le 10/05/2020 sur https://www.justice.gov/storage/report.pdf
(4) GAFA ou GAFAM correspond à l'abréviation des géants du net Américain (Google Amazon, Facebook, Appel, Microsoft) (5) Interview de Bernard BENHAMOU
(6) MORIN-DESAILLY Catherine, « L'Union européenne, colonie du monde numérique ? », Rapport d'information pour la commission des affaires européennes du Sénat n° 443, 20 mars 2013, consulté le 02/02/2020 sur https://www.senat.fr/notice-rapport/2012/r12-443-notice.html
(7) SEL Pierre, « Comprendre le système de crédit social », Esprit, vol. octobre, no. 10, 2019, p. 25-28, consulté le 02/02/2020 sur https://www.cairn.info/revue-esprit-2019-10-page-25.htm
(8) LAHAUD Marwan, « Cybermenace : avis de tempête », Rapport de Institut Montaigne, Novembre 2018, 120p https://www.institutmontaigne.org/ressources/pdfs/publications/cybermenace-avis-de-tempete-rapport.pdf
(9) BOOS Romain, La lutte contre la cybercriminalité au regard de l'action des Etats, Thèse Droit Université de Lorraine, 2016, consultée le 03.02/2020 sur https://tel.archives-ouvertes.fr/tel-01470150/document
(10) Dixième Congrès des Nations Unies, « La prévention du crime et le traitement des délinquants », Vienne, 10-17 avril 2000, http://www.uncjin.org/.
(11) Louis POUZIN est parvenu à faire communiquer des ordinateurs selon le principe du datagramme.