L'Europe de la sécurité numérique : très juridique, mais guère technologique, et encore insuffisamment économique

Par Nicolas ARPAGIAN *
Directeur scientifique du cycle « Sécurité numérique » de l'Institut national des hautes études de la sécurité et de la justice (INHESJ)

Si l'Europe revendique à raison son statut d'économie de la connaissance et de solides ressources génératrices d'activités à forte valeur ajoutée, elle reste très en retrait en matière de sécurité numérique. L'essentiel de sa production en la matière est constitué de textes (des directives ou des règlements européens) établissant des obligations de sécurisation des infrastructures informatiques. Mais les « 28 » n'ayant fait émerger aucun acteur global de la cybersécurité, la lutte contre la cybercriminalité est menée essentiellement par des polices nationales. Et l'Agence de l'Union européenne en charge de sa cyberprotection, l'ENISA, peine encore à assurer son avenir financier. Dès lors que les États membres de l'Union européenne utilisent l'arme numérique pour assurer la défense de leurs intérêts stratégiques (sécurité de leurs opérateurs d'importance vitale, collecte de renseignements économiques ou diplomatiques…), ils rechignent à doter l'Europe d'outils intégrés et performants pour peser réellement face aux grandes puissances du monde numérique, que sont les États-Unis, la Chine ou la Russie.

L'Histoire de la construction européenne a démontré que le Vieux Continent semble plus à même de bâtir une alliance économique et juridique que de devenir un acteur politique ou militaire de premier plan. Ce qui est préoccupant pour l'avenir, c'est que l'Europe s'est appropriée rapidement – son pouvoir d'achat le lui permettait – tout l'appareillage numérique dernier cri (*cloud computing*, équipement haut débit, commerce en ligne, réseaux sociaux, *smartphones*…), mais sans se doter d'une véritable autonomie en la matière. Les Européens sont des clients des grandes plateformes du secteur numérique (notamment des GAFAM : Google, Apple, Facebook, Amazon et Microsoft), mais sans avoir été en mesure de proposer de véritables alternatives d'origine européenne. Or, le poids de ces multinationales est tel qu'il leur permet désormais d'imposer des conditions générales d'utilisation élaborées unilatéralement et mises à jour à leur convenance, sans avoir à en passer par de réelles négociations. Ces contrats, qui sont majoritairement rédigés en anglais et imposent très souvent la saisine d'un tribunal états-unien en cas de contentieux, constituent désormais la véritable architecture juridique d'un Internet planétaire.

Malgré sa puissance économique, son expertise normative et sa position prétendument de force liée à son statut de client, l'Europe n'occupe assurément pas la place qui devrait être la sienne dans la sphère numérique. C'est certainement le fruit des décennies 1970 et 1980, durant lesquelles les élites du Vieux Continent n'ont pas réellement pris au sérieux le potentiel des technologies de l'information, à l'instar de la révision de la politique informatique intervenue après l'élection de Valéry Giscard d'Estaing à la Présidence française en 1974 [1], qui conduisit à une très forte réduction budgétaire des investissements dans les réseaux de communication permettant l'échange des données, notamment dans le projet Cyclades.

** L'auteur s'exprime ici à titre strictement personnel.*
(1) Lire à ce propos l'interview du professeur Louis Pouzin dans la Revue de La Société de l'électricité, de l'électronique et des technologies de l'information et de la communication *(REE N°4/2013 81) : https://www.see.asso.fr/node/5217/file_preview/file_text_text*

Une sécurité numérique « européenne » conçue… nationalement !

Le collectif européen n'a pas abordé le sujet de la cybersécurité de l'Union européenne de la manière la plus opérationnelle possible. L'ENISA (*European Network and Information Security Agency*) [2] a vu le jour en 2004. Mais la faiblesse de ses moyens financiers (10 millions d'euros de budget annuel), la localisation de son siège en Crète (loin des instances de décision) et la modestie de son mandat politique ne lui permettent pas de concevoir une véritable approche mutualisée en matière de sécurité numérique. En mars 2016, son directeur, l'Allemand Udo Helmbrecht, a même lancé un cri d'alarme, indiquant que son agence, grevée de dettes, « ne disposait pas des fonds nécessaires pour faire travailler des experts sur des sujets aussi stratégiques que les objets connectés (IoT) et [qu'elle] devait se contenter de deux personnes pour plancher sur les enjeux du *cloud computing* » [3]. L'agence doit quémander des sommes supplémentaires pour tenter de maintenir son activité et payer ses loyers. Un contexte qui n'encourage guère les meilleurs spécialistes à venir se mettre spontanément à son service. Le maintien de cette situation depuis plus d'une décennie démontre la volonté des États membres de conserver en propre leurs ressources et leur expertise en matière de cybersécurité. Les chancelleries n'envisagent pas de mutualiser leurs savoir-faire à l'échelon de l'Union, et ce aussi bien dans le domaine de la défense que dans celui de la lutte contre les attaques numériques.

Une triste singularité européenne

Si l'Europe dispose encore de champions mondiaux dans les secteurs de l'automobile ou de la pharmacie, elle a nettement délaissé le champ numérique. Les plateformes états-uniennes ont trouvé dans le Vieux Continent un lieu d'épanouissement privilégié : des consommateurs nombreux, solvables, friands de nouvelles technologies, et des législations nationales disparates qui permettent de mettre en concurrence les États membres pour savoir lequel d'entre eux hébergera le siège européen des activités de ces multinationales.

(2) www.enisa.europa.eu
(3) « L'agence de cybersécurité veut quitter la Crète », SUPP (Catherine), Euractiv, *25 mars 2016 : www.euractiv.fr/section/innovation-entreprises/news/cash-strapped-eu-cybersecurity-agency-battles-greece-to-close-expensive-second-office/*

Photo © Jean-Claude Moschetti-REA

Déplacement de Jean-Yves Le Drian, ministre de la Défense, au Centre DGA MI, près de Rennes, octobre 2014.

« Le ministère français de la Défense ne laisse guère de place au doute quand sa page officielle consacrée à la cyberdéfense européenne annonce depuis le 10 août 2011 : "Malgré la mention des enjeux cyber dans ses textes officiels et la mise en place de structures et d'exercices dédiés, l'Union européenne est à la traîne, comparée à une autre alliance, l'Otan. Dans les faits, il y a peu de coopération" ».

Dans le même temps, des pays comme la Chine ou la Russie ont su se doter de leurs propres réseaux sociaux, de leurs propres systèmes de messagerie instantanée, de leurs propres sociétés d'e-commerce, voire de leurs propres spécialistes de la cybersécurité.

En Europe, seule la République tchèque (10 millions d'habitants) est parvenue à mettre sur pied son leader national, SEZNAM (www.seznam.cz), qui dame le pion à Google en étant le premier moteur de recherche à être utilisé par les Tchèques. Il n'y a donc pas de fatalité technique, mais bien l'expression d'un libre choix de consommation des internautes qui permet de faire émerger des acteurs locaux. L'adéquation entre la demande et le service rendu reste le meilleur moyen d'attirer et de fidéliser des utilisateurs, qui n'ont que rarement le critère de la nationalité comme déterminant dans leur choix de navigation.

Déjà connue pour sa forte capacité normative, l'Europe s'est dotée de plusieurs réglementations dans le domaine de la sécurité numérique. La directive européenne 2013/40 [4] vise à harmoniser le droit pénal des États membres pour encadrer les atteintes aux systèmes d'information. L'intitulé même de la Stratégie de cybersécurité de l'Union européenne [5] résume bien à lui seul tout le paradoxe de l'approche des 28, qui appellent de leurs vœux « un cyberespace ouvert, sûr et sécurisé », des qualificatifs que les experts de la cybersécurité jugent le plus souvent antinomiques.

Alors que les États-Unis disposent de leur célèbre *Federal Bureau of Investigation* (FBI), lequel est compétent à l'échelle des 320 millions d'Américains, les 510 millions d'Européens ne disposent pas d'un service analogue de sécurité intérieure. Pour répondre à la spécificité internationale de la cybercriminalité, Europol a ouvert en 2013 un *European Cybercrime Center* [6] basé à La Haye. Il a vocation à faciliter l'échange d'informations et la collecte de bonnes pratiques. C'est certes un point de contact pour les services de police et de gendarmerie, mais ce n'est en aucun cas une force de sécurité intégrée permettant d'agir de manière autonome sur l'ensemble du territoire de l'Union européenne. Là où les mafias de tout poil bénéficient pleinement de la mobilité numérique et font du saute-frontières un des atouts de leur impunité pénale, les défenseurs de l'ordre public sont dans une large mesure contraints par leurs législations et leurs procédures respectives.

Une cyberdéfense européenne étique

Les sites Internet gouvernementaux sont souvent des canaux d'une communication tout en retenue et empreinte de beaucoup de diplomatie. Pourtant, le ministère français de la Défense ne laisse guère de place au doute quand sa page officielle [7] consacrée à la cyberdéfense européenne annonce depuis le 10 août 2011 : « Malgré la mention des enjeux cyber dans ses textes officiels et la mise en place de structures et d'exercices dédiés, l'Union européenne est à la traîne, comparée à une autre alliance, l'Otan. Dans les faits, il y a peu de coopération ».

Ce n'est pourtant pas faute d'en avoir parlé ou d'avoir inscrit ce sujet au menu de nombreux colloques et autres réunions de sociétés savantes. Depuis plus d'une décennie, les diplomates européens semblent vouloir rompre avec le précédent fâcheux du traité de 1952 qui prévoyait la création d'une Communauté européenne de défense (CED). Son rejet deux ans plus tard, en 1954, par l'Assemblée Nationale française, a durablement ancré dans les esprits la hantise qu'une armée constituée à l'échelon européen ne vienne remettre en cause les indépendances nationales.

Pourtant, à la lecture de documents gouvernementaux du début du XXIe siècle, la maturité des esprits qui se manifestait à ce sujet laissait entrevoir quelque espoir : « Selon le rapport de la Commission de Défense sur la guerre informatique transmis en 2008 à l'Assemblée européenne de sécurité et de défense, c'est l'Agence européenne de Défense (AED), qui devrait mettre en œuvre *au niveau des capacités et de la recherche et technologie* une doctrine de la cyberguerre européenne » [8]. Plus de huit ans après, cette doctrine européenne se fait toujours attendre. Et la Politique de sécurité et de défense commune (PSDC) de l'Union européenne est encore très modeste tant dans son volet conventionnel que dans sa dimension cyber. Cette situation a été résumée d'une phrase fin 2015 par le vice-amiral Arnaud Coustillière [9], officier général cyberdéfense à l'État-major français des Armées : « Il faudrait une défense européenne avant d'avoir une cyberdéfense européenne ». Les révélations, à l'hiver 2015 [10], des interceptions des communications de membres du gouvernement français par les services de renseignement allemand (le BND) au profit de l'administration états-unienne, dévoilent les intérêts croisés qui caractérisent la famille européenne. Les alliés politiques demeurent des concurrents économiques. Le principe « Les États n'ont pas d'amis, ils n'ont que des intérêts », exprimé en son temps par le Général de Gaulle, est plus que jamais d'actualité.

---

(4) Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32013L0040&from=FR

(5) Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, 7 février 2013. http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=fr

(6) https://www.europol.europa.eu/ec3

(7) http://www.defense.gouv.fr/portail-defense/enjeux2/cyberdefense/la-cyberdefense/bilan-et-evenements/2011-cyberdefense-enjeu-du-21e-siecle/international/voir-les-articles/union-europeenne-la-lente-mise-en-place-d-une-cyberdefense-commune

(8) « Union européenne : la lente mise en place d'une cyberdéfense commune » – Site du ministère français de la Défense, 10 août 2011. http://www.defense.gouv.fr/portail-defense/enjeux2/cyberdefense/la-cyberdefense/bilan-et-evenements/2011-cyberdefense-enjeu-du-21e-siecle/international/voir-les-articles/union-europeenne-la-lente-mise-en-place-d-une-cyberdefense-commune

(9) Colloque « L'intégration du Cyber dans la planification des opérations et des missions de la Politique de Sécurité et de Défense Commune de l'Union européenne » – 3 et 4 décembre 2015 à Bruxelles, chaire « Cyberdéfense et cybersécurité » Saint-Cyr.

(10) « Laurent Fabius aurait été espionné par les services secrets allemands », Le Monde, 11 novembre 2015 : http://www.lemonde.fr/europe/article/2015/11/11/laurent-fabius-aurait-ete-espionne-par-les-services-secrets-allemands_4807321_3214.html

Le basculement vers la société numérique avec des systèmes d'information qui irriguent les organisations administratives et économiques tend à gommer la frontière entre le monde de la défense et celui de la sécurité. Dès lors que la captation d'informations peut être réalisée à l'insu de sa cible, les cyberattaques occupent désormais une place de choix dans les arsenaux d'États, voire d'entreprises, qui optent pour de discrets prestataires à leur aise dans l'exécution de ces basses œuvres numériques. Dans le cyberespace, pas de défilés militaires pour exhiber ses derniers équipements et procéder à des démonstrations de force ! Ici, la vraie puissance se laisse deviner. Et le silence est la règle tant que la preuve irréfutable de la responsabilité n'est pas apportée. Sur ce théâtre d'opérations, l'Europe a renoncé à allier ses forces et chaque État élabore son propre attirail [11], comme s'il s'agissait de l'ultime démonstration de leur souveraineté déclinante...

(11) « Internet et la fiscalité vont imposer le fédéralisme à l'Europe », ARPAGIAN (Nicolas), Les Echos*, 19 août 2015 : http://www.lesechos.fr/19/08/2015/LesEchos/22004-028-ECH_internet-et-la-fiscalite-vont-imposer-le-federalisme-a-l-europe.htm*