efcse.eu

UNION EUROPEENNE ET CYBERSECURITE

Auteur : Philippe MULLER FEUGA – Membre du comité scientifique de l'EFCSE
30 mars 2019

Sécurité nationale et renforcement des compétences de l'Union européenne

Accéléré par la disparition de l'URSS (1991) concomitante à la transformation numérique de nos sociétés, le phénomène de mondialisation bouscule les équilibres du *« monde ancien »*. Faute d'une politique de recherche et d'innovation volontaire couplée aux attentes des marchés, l'Union européenne (UE) a perdu successivement la bataille des infrastructures de l'Internet, puis celle de ses acteurs maîtres des flux d'informations ou *big data*, et demeure sur la défensive avec les équipementiers comme Nokia Corp. et Ericsson AB dans l'optique d'un déploiement de la 5G, voire de la 6G. Incapable d'appréhender les enjeux géostratégiques du numérique, elle se trouve menacée d'une *« colonisation numérique »* contre laquelle doivent se protéger les Etats membres au premier ressort.

Sur les chemins de la puissance, ces pertes d'influence raniment la question des *« buts de guerre »* (guerre économique ou *unfair competition* ?), par suite de l'entrée du cyberespace comme nouveau lieu de conflictualité perçu comme une menace sur la sécurité nationale par la prise de contrôle de l'information ou des *data*. La bataille pour l'hégémonie *« digitale »* est engagée entre acteurs *« tech giants »*, les GAFAM américains et les BATXH chinois dont la capitalisation boursière est sans commune mesure avec les capacités des acteurs européens, tels le suédois Spotify ou les français OVH ou Qwant (moteur de recherche).

Dès lors, le renforcement des compétences de l'Union européenne, comme celles de l'agence ENISA chargée de la sécurité des réseaux, est-il illusoire, ou peut-il contribuer à la naissance de tels géants comme s'interroge le magazine *Forbes « Time to give European tech giants the investment required to compete with Silicon Valley »* (3 décembre 2018) ?

Enjeux géostratégiques et compétences de l'UE

Sous prétexte de mieux lutter contre la cybercriminalité dans sa communication COM (2017) 477, la Commission européenne (CE) souhaite renforcer les pouvoirs de l'ENISA, agence de cybersécurité européenne. Le principe de subsidiarité est rappelé au § (37) du Règlement (UE) n° 526/2013, et précise les limites des compétences de l'agence ENISA : « Dans l'exécution de ses tâches, l'Agence devrait renforcer les compétences, non leur porter atteinte, et ne devrait ni retirer, entraver ou empiéter sur les pouvoirs et les tâches des autorités règlementaires nationales ». Ce qui justifie la position ferme d'Etats membres comme la France ou l'Allemagne, reposant sur les conditions d'application de l'article 346 TFUE : « la cybersécurité est autant la sécurité des États que celle des entreprises. En outre, quand ces dernières relèvent de secteurs sensibles comme par exemple l'énergie, les transports ou le secteur bancaire, c'est bien de sécurité nationale dont il s'agit ». Le Sénat dans sa proposition du 9 novembre 2017 a conclu que ce principe n'est pas respecté.

L'enjeu est clair : au-delà de la mise en œuvre progressive de politiques de coordination ou de convergence, les compétences attribuées aux agences européennes tout autant qu'à la Commission trouvent leurs limites dans les articles 3 à 6 du TUE. En l'espèce pour l'ENISA, il s'agit de lutter contre la « cybercriminalité ». A contrario, ce qui n'est pas attribué

comme « compétence exclusive » à l'Union appartient aux Etats membres (art. 5 § 3 TUE). Ils exercent leur souveraineté, et assurent leur défense et sécurité nationale – dans ses deux principales composantes, sécurité économique et sécurité numérique complétées par leur résultante, l'intelligence économique (IE). D'où la question : dans quelle mesure la prise de décision liée à l'autonomie stratégique d'un pays doit-elle être préservée sans aucun risque de détournement ou d'aliénation consécutif à une convergence des politiques au niveau européen ?

Souveraineté et sécurité nationale sont au cœur du débat. Avant toute mise en œuvre de politique commune de l'Union, en l'espèce relative à l'ENISA, se pose la question du positionnement de certaines agences, d'autorités administratives indépendantes, d'autorités publiques indépendantes nationales, ainsi que d'établissements publics administratifs. En sachant que les agences nationales en l'espèce, l'ANSSI en France et le BSI en Allemagne, ont des capacités de certification liées à la défense nationale, la question est bien celle de la sécurité nationale. Ces entités parapubliques agissent au nom de l'Etat, et exercent des attributions en matière de défense ou de sécurité de personnes et biens qualifiés de « sensibles » ou de « vitaux » ; elles peuvent être considérées comme porteuses d'enjeux « stratégiques » pour l'Etat membre facilement évaluables. Quels sont ces enjeux, et sont-ils partie prenante des « intérêts stratégiques de l'Union » identifiés par le Conseil européen ?

Dans le même ordre d'idée, la Communication COM (2000) 6 intitulée « Vers un espace européen de la recherche » a été présentée comme une réponse à la perte de compétitivité européenne observée depuis le traité de Maastricht (1992). Cette perte pourrait être compensée grâce à l'action potentielle de recherche de l'Union européenne. Sept ans après le lancement des « autoroutes de l'information » d'Al Gore (décembre 1993), l'UE tente de coordonner les politiques de recherche nationales avec celles de l'Union, portées depuis 2014 par des agences exécutives issues de la DG XIII Recherche et Innovation. L'objectif est de créer un tout cohérent, notamment dans des domaines sensibles, toujours plus nombreux, de la « recherche duale » – comme l'aéronautique, le spatial, les matériaux avancés, la super-conductivité, le quantique ou les technologies numériques qui donnent lieu à des applications à la fois civiles et dans le secteur de la défense hors périmètre PESC (Politique Extérieure et de Sécurité Commune) –. Une telle recherche « duale » relève davantage de grands pays ayant une base technologique et industrielle de défense (BITD) solide, non sans sous-estimer l'apport ciblé des autres pays membres ; la maitrise de la bande passante, du déploiement de la 5G ou de la 6G, de l'utilisation de l'Intelligence artificielle (IA), de la R&D, de la non-compromission des réseaux devient incontournable au niveau des Etats membres à défaut d'une souveraineté européenne.

Les différentes stratégies conduites par Bruxelles – des programmes ESPRIT ou EUREKA, en passant par les Stratégies de Lisbonne ou les programmes-cadres de l'Europe 2020 pour « une Europe plus performante » – ont toutes échoué dans l'affirmation de la puissance européenne. Dès lors, faut-il accuser le cloisonnement des systèmes publics de recherche nationaux, ou faut-il craindre une perte de créativité ou de savoir-faire et de réactivité dans les Etats membres par la mise en place de mécanismes européens, perte qui pèse inévitablement sur notre autonomie stratégique et l'entière maitrise de nos processus de décision ?

Transformation numérique et sécurité nationale

Dans ces deux domaines, numérique et recherche, intimement imbriqués, la circulation des connaissances et des personnes entre le monde académique et celui des entreprises est un impératif. Mais doit-elle gêner tout processus de décision politique de pleine souveraineté tant que les institutions de l'UE, sans réel pouvoir souverain comparable, n'aura pas réconcilié ce décalage normatif ? Dans les secteurs de la défense et de la sécurité nationale, la prise de décision politique

repose sur l'information la plus complète – désormais accessible, ainsi que sur la meilleure compréhension des aspects géoéconomiques et géopolitiques. La data est devenue l'enjeu à la fois dans le processus de décision et en termes de compétitivité. Il n'est pas certain que les responsables européens en soient conscients malgré l'approche du Président Juncker dans son discours par nature rhétorique sur l'état de l'Union « We need protection without protectionism » (septembre 2018). Subtilité du verbe illustrée par l'affaire Kuka Robotics sous contrôle du chinois Midea (mai 2016), mais incertaine sur le dossier Alstom-Siemens (février 2019) ! Discours suivi de l'ébauche de mesure prise dans l'urgence sous la pression des Etats membres comme la France, l'Allemagne ou les Pays-Bas, à commencer par l'étude (février 2019) de la mise en place d'un dispositif de contrôle des investissements étrangers en Europe (IDE). Exemple type de faiblesse : depuis le Traité de Lisbonne (2009), les mouvements de capitaux, donc les investissements étrangers, relèvent de la politique commerciale de l'UE, pouvant être limités par un Etat membre que s'ils portent atteinte « à l'ordre public ou à la sécurité publique » selon l'article 65 (TFUE).

En d'autres termes, cet article « ne porte pas atteinte » à un certain nombre de droits garantissant la souveraineté nationale dans l'urgente nécessité de protéger les « intérêts de la Nation ». Le 18ème Rapport sur la Sécurité de l'Union (mars 2019) en décrit les mesures de convergence prises, mais de manière sectorielle : « Stronger and smarter information systems for security, border and migration management » ; certaines prérogatives de l'Union et de l'agence ENISA en cybersecurity limitées à la lutte contre le terrorisme ou la cybercriminalité (pp. 5-6) ; complétées par des dispositifs de protection en termes d'authenticité comportant identité et signature par le Règlement eIDAS de 2014 ; de mesures de résilience au cours de campagnes électorales (p. 10-11) ; d'autres dispositifs comme celui collectant les informations auprès des passagers aériens, ou PNR en 2016 (pp. 11-14) ; ou la directive de 2016 visant à assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'UE, ou NIS (p. 14) ; et les infrastructures vitales des opérateurs de services essentiels, ou OSE (p. 16). Ces mesures en termes de « sécurité » apparaissent interprétées par Bruxelles de manière restrictive en évitant la sphère souveraine de sécurité nationale ou de défense jamais citée dans ce rapport, mais avec la tentation de la contourner.

La conjugaison des deux articles 65 (TFUE) et 346 (TFUE) soulignent l'importance des « intérêts essentiels de sécurité » comme élément ou « zone de souveraineté » d'un Etat membre tel qu'il apparaît à l'article 355 (TFUE). Les cibles recherchées par ces IDE quelle que soit leur origine sont les actifs informationnels de sociétés ou d'opérateurs rattachés à la mise en œuvre de politique dans les domaines de défense, de sécurité ou d'ordre public selon des critères clairement établis : soit par la nomenclature budgétaire issue de la LOLF (par destination selon le découpage en mission-programme-action), soit par un financement assuré majoritairement par l'État (directement sous forme de subventions ou indirectement via des ressources publiques affectées, yc fiscales), soit par un contrôle public direct ou non (APE, CDC ou BPI) qui ne se limite pas à un contrôle économique ou financier, mais relève de l'exercice d'une tutelle ayant capacité à orienter les décisions stratégiques avec participation ou non au conseil d'administration. Question d'autonomie stratégique à réévaluer, nullement limitée à « la sécurité publique ». Question de clarté dans le périmètre défini : tout dépend de la définition retenue en termes d'exercice de la souveraineté !

Dans le cadre européen à partir de 1993, l'exclusion de la dimension extérieure dans la construction du marché unique interdit toute réflexion en matière de guerre économique, toute doctrine de puissance économique, toute politique industrielle en faveur de « champions européens » à l'inverse de pays animés d'une volonté de puissance, tels les États-Unis, la RP de Chine, la Russie, le Japon, la Corée du Sud ou l'Australie, mais aussi la Turquie, l'Iran, la Corée du Nord, etc. Les premiers ont su réagir très tôt et adopter une législation contraignante face à l'« economic espionage » (1996), la seconde ayant institué un capitalisme d'Etat sous idéologie marxiste a su poser les bases juridiques d'une politique de

sécurité nationale – sur les intérêts économiques du pays, mais aussi par un soutien au parti – par l'adoption de la loi sur le renseignement national (juin 2017) invitant tout citoyen de collaborer avec les « organes » de renseignement. En conséquence, les Etats membres comme la France sont en opposition avec l'UE : ne disposent-ils pas d'outils « souverains » capables d'autoriser les investissements étrangers en relation avec le concept de « sécurité nationale » élargie, comparable au comité pour l'investissement étranger aux Etats-Unis ou CFIUS ?

Autonomie stratégique conçue en termes de puissance

Cette approche par défaut conteste l'interprétation stricte imposée par la Commission ou la Cour de justice (CJUE), mais se trouve justifiée par l'art. 346 (TFUE) : il s'impose aux renseignements (data) dont la divulgation serait contraire aux « intérêts essentiels de la sécurité » des Etats membres. La mobilisation des moyens civils et militaires engagés en fonction de la gravité d'une crise désormais « hybride » relèvent de la sécurité nationale des Etats membres faute d'une puissance affirmée côté européen, et en l'absence d'une souveraineté de plein exercice reconnue pour construire une Europe de la défense. Or, la défense n'est pas soumise aux règlements européens. Elle doit « en toutes circonstances » assurer « la sécurité et l'intégrité du territoire, ainsi que la vie de la population » aux termes de l'art. 1 de l'ordonnance de 1959 « portant organisation de la défense nationale ». Et ce, à un moment où la France adopte une doctrine de lutte informatique offensive (LIO) hissant, selon le chef d'état-major des armées (CEMA), le numérique au rang des armes classiques (mars 2019). La cybersécurité – partie intégrante de notre sécurité nationale – peut-elle dès lors dépendre d'un organe central (ENISA), par ailleurs doté d'un pouvoir de sanction, hors contrôle ? Il s'agit d'assurer une pleine autonomie de décision faisant valoir nos « intérêts fondamentaux », comme la France a su l'affirmer au sein de l'OTAN.

L'Union européenne (UE), première puissance commerciale du monde dotée de quelques parcelles de souveraineté, est rattrapée par une guerre commerciale, doublée d'une rivalité technologique entre deux grandes puissances, les Etats-Unis

(EU) et la RP de Chine. Le dossier Broadcomm Ltd/Qualcomm Inc. porté par le CFIUS (mars 2018) et celui de Huawei confondu dans un possible détournement des sanctions américaines contre l'Iran (janvier 2019) sous couvert d'influence hégémonique autour de la 5G illustrent cette rivalité. Celle-ci n'est qu'un aspect de l'approche hybride globale d'une guerre économique tous azimuts (guerre des changes ou des taux, guerre des normes ou standards, guerre de l'intelligence artificielle, guerre de l'information, etc.). Bref, une guerre « hors limites » issue de la réflexion chinoise (1999) sous influence du général et stratège chinois Sun Tzu transposée à l'ère de la mondialisation et du cyberespace en pleine expansion. Dès 2003, la cyberguerre a commencé, de plus en plus prégnante et organisée, d'une part en s'appuyant sur des hackers ou proxies interposés, d'autre part en ayant la capacité d'une censure interne d'Internet comme en Chine adoptée entre 1994-1996 et concrétisée par l'édification et le renforcement du Bouclier doré (Golden Shield ou Great Firewall), ou d'une déconnexion de l'Internet mondial comme le teste la Russie en avril 2019, ou comme le fait l'Iran. Stratégies de fermeture à opposer à celle ouverte des exercices américains Cyber Storm conduits par le département de sécurité (DHS) post 11 septembre 2001 afin de tester la capacité à lutter contre les cybermenaces économiquement déstabilisatrices

Selon certains experts, cette expansion joue désormais en faveur de la Chine de Xi Jinping, à la fois ambitieuse par son programme industriel et high tech « Made in China 2025 », et par la toile des « routes de la soie » qu'elle tisse à horizon 2049. Et devenue impatiente ayant pour objectif la constitution d'un centre-monde systémique concurrent à l'ordre mondial actuel au point de vouloir bousculer la doctrine de Deng Xiaoping « cacher ses capacités et attendre son heure » (to hide your capacities and bide your time) et de passer aux actes. L'UE n'a aucune stratégie face à une situation conflictuelle due à la contestation de l'hégémonie occidentale composée d'un noyau dur, les Etats-Unis, et d'un ventre mou, l'Union

européenne. Une Union européenne traumatisée par ses expériences du XXème siècle court et tragique (1917-1991, avec ses totalitarismes), devenue volontairement consensuelle et pacifique, voire naïve car actrice du renoncement politique à la volonté de puissance et à la souveraineté numérique. Pourtant, de part et d'autre de l'Atlantique le nombre des cyberattaques comme les virus Wannacry ou NotPetya (2017) ou celle visant l'organisme international des adresses Internet ICANN (février 2019), ou les exploits zero day sont croissants, affectant des entreprises, des secteurs entiers, voire des zones géographiques de plus en plus larges, fonction directe de la taille des réseaux et des possibles interconnexions.

Avec les nouvelles formes de guerres hybrides ou de guerres asymétriques, la réactivité doit être forte pour assurer la défense de notre souveraineté, à défaut de celle de l'UE. Or, les champs de bataille se dessinent autour des principales couches de l'Internet présentes dans toute architecture numérique ayant chacune leurs propres vulnérabilités telle la couche physique (celle des équipements, supports, câbles et nœuds de connexion se structurant en axes d'importance inégale où passe le trafic de données) pouvant relever d'un contrôle souverain ; cette première couche répond à la couche logique composée de protocoles et de codes contrôlés par des administrateurs gérant les droits d'accès, restrictifs ou non, pour assurer l'interopérabilité sur le web ; et la transmission des informations ou data , troisième couche ou couche sémantique, à sensibilité inégale, mais créatrice d'une rente et d'avantages compétitifs. Celle-ci est également porteuse de « secrets » ou de confidentialité le plus souvent cryptés au nom d'« intérêts fondamentaux de la nation ». La fonction sécurité n'étant pas intégrée by design chez les éditeurs de logiciels, la sécurisation de chacune de ces trois couches dont la couche logique est donc indispensable pour conserver la souveraineté numérique : elle relève de la mobilisation immédiate de tous les acteurs nationaux, personnes physiques ou personnes morales, sans attendre les décisions consensuelles ou les textes administratifs au niveau européen ; elle repose sur les moyens techniques, la mise en conformité et une organisation efficace en matière de gestion des « informations sensibles » (IGI 1300, et autres dispositifs de protection tels la PPST, le SAIV ou la procédure IEF) sous l'égide des services étatiques ou par délégation auprès des OIV nationaux sans dépendre d'organismes extérieurs hors contrôle souverain. Active sur tout le spectre critique de la « sécurité nationale », elle assure l'autonomie stratégique de nos forces et la défense de nos « intérêts fondamentaux ».

Conclusion

La transformation du web 1.0 aux web n.0 ou à l'Industrie 4.0, la mise en réseaux sociaux ou économiques et la convergence des systèmes IT et OT industriels (ICS, Industrial Control System) poursuivent les transformations des champs de la défense et de la sécurité dont les principaux acteurs doivent assurer notre autonomie stratégique. Il est loisible pour Huawei d'expliquer aux Européens que leur intérêt n'est pas de « suivre l'Amérique dans sa guerre contre Huawei. Cela ralentirait l'innovation et augmenterait son coût [du déploiement de la 5G]. Cela porterait atteinte aux intérêts des consommateurs ». Mais l'entreprise chinoise oublie de préciser que tout Etat souverain doit préserver ses capacités de décision et d'action de manière autonome, tout particulièrement dans le cadre de ses infrastructures de communication et de la maitrise de l'information.