Cyberdéfense : perspectives européennes

L'Union européenne tente de préserver sa souveraineté technologique par une politique cohérente de cyberdéfense. La part croissante du marché numérique constitue en effet un avantage, mais aussi une vulnérabilité.

La coopération européenne en la matière a fait l'objet d'un colloque organisé, le 16 mai 2013 à Paris, par la Commission des affaires étrangères, de la défense et des forces armées du Sénat. Y ont notamment participé : le sénateur Jean-Marie Bockel, auteur d'un rapport d'information sur la cyberdéfense ; Giuseppe Abbamonte, chef d'unité à la DG Connect de la Commission européenne ; l'ambassadeur Jean-François Blarel, secrétaire général adjoint du ministère des Affaires étrangères ; Cornelia Regall-Grothe, secrétaire d'Etat du ministère fédéral allemand de l'Intérieur ; Sir Peter Ricketts, ambassadeur britannique en France.

La Commission européenne. Selon Giuseppe Abbamonte, le marché numérique de l'Union européenne (UE) se monte chaque année à 500 Md€, soit 1.000 € par personne. Mais les menaces sont diverses : criminelles, motivations politiques, terrorisme, catastrophes naturelles et… même câbles grignotés par des rats ! Chaque jour, la sécurité de 148.000 ordinateurs se trouve compromise, entraînant un préjudice possible d'environ 250 Md€. Toutefois, les efforts de sensibilisation entrepris portent leurs fruits. En 2012, 38 % des internautes ont modifié leur comportement : moins d'achats en ligne et vigilance quant à la diffusion des données personnelles. L'UE a défini une doctrine : créer les conditions pour une coopération entre tous les Etats membres avec l'instauration d'autorités nationales compétentes ; diffuser une culture de prévention des risques informatiques ; promouvoir la cybersécurité au sein des secteurs publics et

privés. Toutefois, note Giuseppe Abbamonte, la coopération ne fonctionne que parmi les pays du Nord-Ouest de l'UE, faute de confiance mutuelle au sein de la totalité des Etats membres. « *Or,* dit-il, *s'il y a un maillon faible, cela affaiblit toute la chaîne* ».

En France. Le cyberespace est difficile à appréhender au niveau diplomatique, explique Jean-François Blarel. Les Etats réagissent de façon ambivalente, entre la promotion de la liberté des acteurs (utilisateurs, entreprises et pouvoirs publics) et un contrôle politique. Pour la France, il s'agit d'éviter les escalades, comme celle des Etats-Unis vis-à-vis de la Chine, et qu'internet devienne un espace de conflit. L'ONU, l'OSCE (Organisation pour la sécurité et la coopération en Europe), l'UE et l'OTAN traitent du cyberespace. Ainsi, le sommet de l'OTAN à Lisbonne (2010) a considéré que l'article V sur la solidarité entre pays membres peut être invoqué, en cas d'agression caractérisée et identifiée. Par ailleurs des forums « ad hoc » se forment en dehors des instances internationales officielles (Londres 2011, Budapest 2013 et Séoul 2014). La France tente de coopérer avec deux groupes de pays : ceux partisans d'un traité international sur la cyberguerre et le rôle de l'Etat (contrôle) et ceux (dont la France) favorables au dialogue entre l'Etat, les utilisateurs et les grands groupes fournisseurs de tuyaux d'accès à internet. Sur le plan bilatéral, la France agit avec l'Allemagne, la Grande-Bretagne, les Etats-Unis et l'UE pour créer un climat de confiance. Elle se manifeste aussi au sein des instances internationales, dont l'ONU d'où, estime l'ambassadeur, découleront peut-être des relations de confiance entre les Etats. Déjà, 15 d'entre eux élaborent des normes de conduite et des mesures en ce sens pour éviter l'escalade.

En Allemagne. Cornelia Regall-Grothe dirige aussi depuis 2010 l'Office fédéral des systèmes d'information (500 agents et budget annuel de 80 M€)… qui subit 5 attaques par jour ! En Allemagne, les dommages se chiffrent en milliards d'euros. Devant la difficulté à déterminer les objectifs des cyberattaquants (espionnage militaire ou sabotage économique), les autorités procèdent par déduction et misent sur la prévention aux niveaux de l'Etat, des entreprises et des utilisateurs. Depuis 2011, les mesures portent sur la protection des infrastructures critiques et les systèmes de sécurité informatique. Un Conseil de cybersécurité regroupe des représentants de la Chancellerie, des ministères des Affaires étrangères, de l'Economie et de la Technologie, des Länder, des entreprises et du monde scientifique. Il étudie les progrès technologiques et les vulnérabilités. Les

responsables des infrastructures critiques du pays, surtout les télécommunications, ont l'obligation de mettre à jour tous les deux ans leurs plans de sécurité informatique et de signaler toute attaque. Malgré les limitations budgétaires, les programmes de recherche et développement bénéficieront d'une enveloppe supplémentaire de 30 M€ sur cinq ans. La coopération européenne (France et Grande-Bretagne) vise à renforcer la souveraineté technologique de l'UE en matière d'équipements fiables.

En Grande-Bretagne. Sir Peter Ricketts a participé à l'élaboration du Livre blanc (français) 2013 sur la défense et la sécurité nationale. Selon lui, l'approche britannique consiste à concilier l'optimisation de l'usage d'internet, vecteur de croissance (58 Md€ d'achats en ligne par an) et les besoins de sécurité informatique. Le « Government Communications Headquarters » (GCHQ), agence chargée du renseignement technique, dispose de 700 agents pour la cyberdéfense et bénéficie d'une rallonge budgétaire de 750 M€ entre 2011 et 2015. Il s'agit de renouveler continuellement les systèmes pour anticiper sur ce qui se passera sur internet et réagir en temps réel. Face à la cybercriminalité, une nouvelle unité mutualise les moyens de maintien de l'ordre, police et cybersécurité. Les entreprises, petites et grandes, profitent de la protection publique pour développer leur activité en ligne et augmenter ainsi leur chiffre d'affaires. Elles sont aussi incitées à échanger leurs informations en matière de cybersécurité. Enfin, la coopération internationale, excellente avec la France et l'Allemagne précise l'ambassadeur, porte aussi sur l'aide financière dans ce domaine aux petits pays émergents.

Loïc Salmon

Cyberdéfense : une complexité exponentielle

Suite à la publication du Livre blanc 2013 sur la défense et la sécurité nationale, le sénateur Jean-Marie Bockel a donné les indications suivantes en matière de cyberdéfense sur laquelle il a publié un rapport en 2012 : l'Agence nationale de la sécurité des systèmes d'information devrait disposer de 500 agents en 2015 ; l'Union européenne fixe la norme de cybersécurité ; obligation de déclaration en cas d'incident significatif dans les infrastructures critiques ; maintien de l'autonomie stratégique de la France ; lutte contre le pillage du patrimoine culturel et économique ; la sécurisation des données informatiques constitue un secteur à forte croissance ; nécessité d'un dialogue avec la Russie et la Chine

dans une dimension mondiale et selon des règles à définir sur des enjeux industriels et technologiques.