



La Chaire cyberdéfense et cybersécurité Saint-Cyr, Sogeti, Thales a organisé, le mercredi 14 mai, un colloque sur le thème « (Re)bâtir la cyberconfiance entre partenaires et alliés ». Dans un contexte international où des Etats, des entreprises, des groupes d'individus exploitent à des fins stratégiques des données recueillies massivement, les intervenants ont tenté de répondre à la question capitale de la reconstruction de la cyberconfiance entre partenaires et alliés, dans un cadre juridique à ce jour incertain.

La sécurité des Etats repose en grande partie sur le renseignement technique et plus particulièrement sur le renseignement d'origine électromagnétique. C'est encore plus vrai pour les pays anglo-saxons depuis le 11 septembre. Les révélations d'Edouard Snowden sur l'existence de systèmes et procédés d'écoute (PRISM, Quantum, réseau d'écoute SIGINT), actifs et toujours légaux au regard des lois américaines, ont ébranlé la confiance entre partenaires traditionnels et alliés. Pourtant, la menace croissante du cyberterrorisme, de la cyberguerre et de la cybercriminalité contraint les alliés à travailler ensemble pour se protéger. Restaurer la confiance en est une condition *sine qua non*. Elle ne pourra revenir qu'accompagnée d'accords interétatiques et d'une législation internationale. Face à la cybermenace, l'enjeu est de trouver l'équilibre pour garantir la sécurité nationale tout en respectant la vie privée des citoyens.

Sur le plan juridique, la France et plus généralement l'Europe se différencient des Etats-Unis, au risque de se couper du reste du monde. Malgré la volonté européenne et nationale de protéger les libertés individuelles et d'anticiper les risques dans le cyberspace, une adaptation de nos lois à l'inéluctable interconnexion généralisée des systèmes et des individus est une question à laquelle nous ne pourrions échapper.

L'histoire nous apprend que les alliances se créent pour faire face à une adversité et des menaces communes. Il en est de même dans le cyberspace, même si ces alliances restent très liées aux intérêts des pays, notamment économiques. Elles sont appelées à se construire face à des menaces communes, et conduisent les pays alliés à partager leur vision et leur compréhension du monde. Pour autant, le besoin de communiquer et donc de se dévoiler ne pourra raisonnablement pas se faire dans un espace aussi large que l'Europe, constituée de pays aux intérêts culturels ou économiques divergents. Le partenariat est plus facile et donc plus réaliste de façon bilatérale.

La France peut jouer un rôle majeur dans l'organisation du cyberspace de demain. Il lui faut pour cela aller au-delà des crises de confiance telles que celles que nous vivons, et travailler sur des solutions industrielles innovantes, sécurisées, et évolutives, intégrées en amont dans les systèmes d'information. C'est à ce prix, en s'appuyant sur des industriels dynamiques, et avec une approche de partenariats à long terme, qu'elle restera un allié de confiance crédible sur la scène internationale.

Le colloque a permis de soulever les défis majeurs que pose le cyberspace, dans toutes ses dimensions : sociétale, juridique, diplomatique et industrielle. Instaurer un climat de confiance et de sécurité entre partenaires industriels et de Défense est une priorité ; la Chaire de cyberdéfense-cybersécurité a vocation à y contribuer.

---

La Chaire remercie ses partenaires

