Plaidoyer pour la cyber-intelligence comme nouvelle discipline scientifique

ROBERTO FERNANDEZ

Assistant de Solvay Brussels School

Comme annoncé, le gouvernement fédéral belge vient de créer le «Centre Cyber sécurité Belgique» (CCSB). Cet organe aura pour tâche la supervision et le suivi de la cyber-sécurité dans une approche intégrée et centralisée. La Belgique se dote dès lors d'un moyen supplémentaire en matière de coordination des différents services de l'État (Sûreté de l'État, Service de renseignement militaire, Centre de crise, Computer Crime Unit).

Cette décision intervient dans un contexte de forte montée en puissance des cyber-risques. À titre illustratif parmi de nombreux exemples, rappelons les cyber-attaques de ministères fédéraux (Affaires étrangères et Finances).

Dans un monde de plus en plus digitalisé, interconnecté et interdépendant plus aucune catégorie d'usagers n echappe au risque d'une cyber-attaque De l énergie aux télécommunications en pas sant par les institutions finan cières de nombreux acteurs pu blics et prives sont desormais des vecteurs d'un risque systémique en cas de cyber-attaque.

L'étude 2014 de Verizon souligne tant l'ampleur de la cyber-sécurité que son caractère transversal sur l'ensemble de l'activité humaine (secteur public, santé, transport, énergie) avec une prédominance des attaques contre les marchés financiers. Sur 1.367 cyber-incidents analysés par Verizon en 2013, les marchés financiers représentaient 34% des attaques contre une dizaine de pour-cent pour le secteur public ou de l'énergie. Ce rapport souligne également l'explosion du cyber-espionnage (à des fins politiques ou commerciales).

Le nœud le plus faible

La cyber-attaque introduit une nouvelle dimension à la sécurité. La sophistication des cyber-attaques a atteint un perfectionnement tel qu'elles peuvent porter atteinte à l'intégrité et la confidentialité des données sans être détectées en temps utile. Par conséquent, la cyber-sécurité pose une double question: cognitive et politique.

Au regard de sa complexité, la cyber-sécurité ne pose-t-elle pas une question cognitive du «comment» appréhender cette nouvelle réalité? Comment la mesurer et la quantifier? Mais la cyber-sécurité ne soulève-t-elle pas également de nombreuses questions politiques relatives à la place de l'État dans la gouvernance du cyber-espace?

L'émergence de la société du réseau, reliant l'activité politique, économique et quotidienne, a imposé une nouvelle réalité. Ce nouveau paradigme offre autant de perspectives d'innovation que de challenges de sécurité comme ce fut le cas, dans le passé, avec des innovations telle l'énergie nucléaire.

La complexité de la société du réseau nous pousse à réfléchir sur les moyens scientifiques d'analyse et de mesure de cette nouvelle réalité. En effet, l'analyse et la mesure sont les pierres angulaires de toutes politiques de sécurité et de gestion des risques

Les premiers pas de l analyse en cyber-securité ont ete exclusive ment dominés par l'expertise informatique Or cette approche res trictive porte en elle une double li mitation

Tout d'abord, cette approche s'est focalisée sur la sécurité IT prise à titre individuel (de tel ministère ou de telle entreprise) sans intégrer correctement la dimension du network. En effet, dans la théorie du réseau, une attaque se fera systématiquement sur le nœud le plus faible dans une économie dite «data supply chain». Ainsi, si une cyber-attaque vise le vol de données diplomatiques partagées entre plusieurs chancelleries européennes sur des sanctions à l'égard de la Russie, le nœud considéré comme le plus faible fera l'objet de l'attaque. La cyber-attaque du ministère belge des Affaires étrangères confirme que la cyber-sécurité doit se penser dans une approche d'interconnexion et interdépendance des données.

Ensuite, cette approche «informatique» a surévalué la valeur ajoutée de la standardisation de normes de sécurité IT. De nombreuses recherches ont souligné les limites d'une approche de standardisation de normes de sécurité dans un environnement complètement dérégulé et faisant preuve d'une extrême créativité. Ainsi, aucun standard technique ou patch de sécurité ne peuvent prévenir d'une attaque «zero day». De plus, des vulnérabilités en matière de cyber-sécurité peuvent résulter de choix stratégiques d'entreprises dans leur manière d'organiser leurs activités et de la commercialisation de produits.

Cette double limitation de l'approche «informatique» de la cyber sécurité soulève le besoin d'une approche plus large et pluridisciplinaire.

Approche multidisciplinaire

Dans cette optique, des chercheurs soulignent le rôle central de l'expertise scientifique et des services de renseignement comme moteur clé de l'analyse en matière de cyber-sécurité. En effet, l'approche IT est dominée par des solutions tactiques ne pouvant déboucher sur une stratégie de cyber-sécurité au niveau des états et des grands acteurs économiques.

Par nature, les outils ICT ne font que répondre aux requêtes du Business visant à développer de nouveaux produits et services; comme par exemple le paiement en ligne ou le cloud computing... Dès lors, l'ingénierie informatique au sens strict ne peut répondre aux enjeux de gouvernance et de sécurité au niveau network. Ces enjeux de réseau impliquent

par nature une approche scientifique multidisciplinaire et politique (dont le renseignement).

Ainsi, au-delà de l'enjeu cognitif de l'analyse scientifique, la cyber-sécurité soulève un double paradoxe impliquant une réponse politique.

Le premier paradoxe tient au rapport État/secteur privé. La majeure partie des infrastructures ICT sont aux mains d'opérateurs privés dans le secteur des télécommunications, de l'énergie, de la finance. Dès lors, il se pose la question clé de la régulation et du contrôle de ces opérateurs ayant entre leurs mains la quasi-totalité des infrastructures nécessaires au fonctionnement d'une collectivité nationale Par conséquent, les Etats doivent faire face au paradoxe de devoir assurer la cyber sécurité d infrastructures ICT largement non regulees appartenant a des operateurs prives

Le deuxième paradoxe est d'ordre géopolitique avec une domination nord-américaine tant dans la propriété des infrastructures de «web» par des sociétés nord-américaines que par les moyens colossaux d'espionnage du gouvernement américain.

Au regard de cette double dimension (la dimension cognitive de la compréhension d'une nouvelle réalité d'une part, et, d'autre part les enjeux géopolitiques et de régulation), n'est-il pas opportun de promouvoir une nouvelle discipline de recherche académique relative à la cyber intelligence?

L'ingénierie informatique au sens strict ne peut répondre aux enjeux de gouvernance et de sécurité au niveau network. Ces enjeux de réseau impliquent par nature une approche scientifique multidisciplinaire et politique.