Les budgets nationaux de cyberdéfense en croissance constante

En raison de la sensibilité des enjeux, peu d'Etats communiquent ouvertement sur les budgets alloués à l'élaboration et l'acquisition de capacités de cyberdéfense. Néanmoins, les stratégies nationales de cybersécurité, et les budgets qui y sont rattachés, peuvent englober les besoins liés à la mise en œuvre d'une cyberdéfense, ce qui permet de faire une estimation des investissements financiers des pays dans les capacités militaires de cyberdéfense.

Les Etats-Unis, leader incontesté

Selon l'*Office of Management and Budget* (OMB), depuis le premier mandat présidentiel de Barack Obama, le total des investissements fédéraux dans les technologies d'information et de communication est passé de 6,7 G$ pour l'année fiscale 2008 (FY2008), à 8,9 G$ pour la FY2014. A partir de 2011, les documents officiels de l'OMB font la distinction entre le budget de la cyberdéfense du *Department of Defense (DoD),* et celui des autres agences fédérales, dédié à la cybersécurité ainsi qu'à la lutte contre la cybercriminalité. Ainsi, pour le *DoD*, le budget alloué à la cyberdéfense pour la *FY2013* était de 3,9 G$, et la Maison Blanche a accordé des budgets supplémentaires, pour atteindre 4,7 G$ (FY2014). Si l'on observe attentivement les coupes budgétaires opérées dans le budget américain de la Défense, ainsi que dans le budget global, il ressort que les budgets alloués à la cybersécurité et à la cyberdéfense ont connu une hausse moyenne annuelle de 0,27% pour la période 2009-2014.

En Europe, des investissements croissants

A l'instar de la France, nos partenaires européens ont engagé des plans d'actions pour développer leur cyberdéfense.

Au Royaume-Uni, le *National Cyber Security Programme* planifie la répartition du budget national de 650 M£, annoncé dans la « Stratégie Nationale de Cyber Sécurité » (2011) couvrant la période 2011-2015. Ce programme prévoit des dépenses croissantes (105 M£ pour la FY2011, jusqu'à 210 M£ pour la FY2015), réparties à 60% pour les activités de « sécurité et de renseignement » du *Government Communications Headquarters* (GCHQ), 15% pour les « activités cyber du *Ministry of Defence* (MoD) », et le reste aux activités connexes (sécurisation des réseaux gouvernementaux, programmes de R&D).

Preuve que le gouvernement britannique considère ce programme de développement de capacités de cybersécurité et de cyberdéfense comme priorité stratégique, 210 M£ supplémentaires ont été alloués en 2013 pour la FY2015-2016, dans le cadre du NCSP.

En Allemagne, le *Bundesamt für Sicherheit in des Informationstechnik* (BSI), l'Office fédéral de sécurité des systèmes d'informations, rattaché au ministère fédéral de l'Intérieur (BMI), est l'agence chargée de coordonner les activités de cybersécurité. Ses prérogatives sont similaires à celles de l'ANSSI en France, et ne sont donc pas directement liées à la cyberdéfense. Le BSI dispose d'un budget annuel d'environ 80 M€ ; le budget de cyberdéfense de l'Allemagne n'est pas directement connu, mais il est suffisant pour permettre à Berlin de disposer de capacités cyberoffensives.

La France, des ambitions à la hauteur de ses moyens

Présenté au début du mois de février 2014, le « Pacte Défense Cyber » du ministère de la Défense français formalise les efforts de l'Etat français en terme d'investissements dans les capacités nationales de cyberdéfense. Ce plan prévoit une allocation d'environ un milliard d'euros réparti sur la période de la Loi de Programmation Militaire (2014-2019), soit un budget annuel prévisionnel d'environ 165 M€ consacré à la cyberdéfense française. Ce budget sera partagé à 50% pour les besoins capacitaires du ministère (ressources humaines, moyens techniques), et à 50% pour le secteur de la recherche et de l'innovation, permettant au secteur privé de bénéficier de subventions finançant les projets d'innovation technologique dans le secteur de la sécurité des systèmes d'information.

Ce « Pacte Défense Cyber » constitue le premier plan d'action du ministère de la Défense pour répondre aux besoins impérieux de cybersécurité dans l'environnement stratégique contemporain. S'ajoutent aux dépenses prévues dans ce plan d'action les efforts liés à la rénovation ou à l'acquisition de nouvelles capacités concourant aux fonctions stratégiques définies dans le Livre Blanc 2013 et précisées dans la LPM 2014 ; la majorité des composantes concourant à ces fonctions stratégiques constitue tout ou partie d'un système d'information devant être sécurisés et adaptés aux normes exigées pour les besoins d'interopérabilité (entre autres).

Cybersécurité, cyberdéfense, quelle différence ?

Si l'on reprend les définitions de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la *cybersécurité* est un « *État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* ». L'ANSSI définit la *cyberdéfense* comme l'« *ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels* ». Cela signifie que les autorités se réservent le droit de défendre ces systèmes d'information par des mesures de rétorsion dans le cyberespace, comme dans les domaines physiques (e.g. sanctions économiques, frappes cinétiques, etc.).

Les marchés de la cybercriminalité

A l'instar des marchés de la criminalité organisée internationale, le cyberespace a ses marchés de la cybercriminalité. La vente de failles de sécurité (0-day exploits) est devenue très lucrative (jusqu'à 260 K€ la faille) et constitue le cœur d'activité d'entreprises spécialisées. Les coûts globaux de la cybercriminalité sont assez délicats à évaluer; une étude de Norton Inc. de 2011 chiffrait à 388 G$ pour 24 pays analysés sur une durée d'un an. Une étude de MacAfee & CSIS de 2013 avance le chiffre de 300 G$ à 1000 G$/an. Cette estimation regroupe cependant les coûts de la cybercriminalité et ceux liés au cyberespionnage.

VINCENT JOUBERT
Chargé de recherche, FRS
v.joubert@frstrategie.org