L'EUROPE JOUE À SE FAIRE CYBERPEUR

LE 10 NOVEMBRE 2010 ***OLIVIER TESQUET***

La semaine dernière, l'Union européenne a mené sa première simulation de cyberattaque d'envergure. Si vous n'en avez pas entendu parler, ne vous inquiétez pas: il reste encore quelques bugs.

Le 4 novembre, l'Union européenne a mené une vaste simulation de cyberattaque, impliquant les 27 pays membres, la Suisse, La Norvège et l'Islande. Vous n'avez pas entendu parler de cet exercice, *"le tout premier du genre au niveau paneuropéen"* ? Rien de plus normal. Cyber Europe 2010 (son nom de scène) a été mené dans la plus grande discrétion. A peine a-t-on vu passer **un court article récapitulatif** en provenance du bureau bruxellois du Monde. Aux manettes de ce wargame géant, l'**Enisa**, l'agence européenne pour la cybersécurité; à l'autre bout du fil, 150 fonctionnaires de 70 administrations différentes, 50 à Athènes (où l'Enisa dispose d'une antenne) et 80 disséminés à travers le continent.

L'espace de quelques heures, ces mêmes fonctionnaires ont subi 320 attaques en tout genre, censées préfigurer un assaut massif contre les connexions transfrontalières. Le tout pourrait sembler au mieux anecdotique, au pire insignifiant (après tout, rien d'illogique à se préoccuper de la protection des réseaux "officiels") si les États-Unis n'avaient pas impulsé une nouvelle stratégie en la matière. Matérialisée dans le **Cyber Shockwave** (février 2010) ou le **Cyber Storm** (septembre), exercices aux alias millénaristes inscrits en lettres rouges sur les *breaking news* défilantes de CNN, cette nouvelle doctrine a-t-elle franchi l'Atlantique pour atteindre nos rivages?

100 000 euros

Contacté par OWNI, Ulf Bergstrom, le porte-parole de l'Enisa, invoque le **Digital Agenda** diligenté au mois de mai par Neelie Kross, la Commissaire européenne à la société numérique, et tient à éclaircir certains points:

> ***Nous voulions travailler avec différentes hiérarchies, différentes structures, différentes procédures, d'où l'idée d'un exercice paneuropéen, afin d'améliorer notre coopération à l'avenir. Après la cyberattaque d'envergure contre l'Estonie en 2007 , un consensus est en train d'émerger sur la nécessité d'une collaboration entre les Etats membres de l'Union. D'ailleurs, le Traité de Lisbonne encourage précisément le travail d'équipe sur ce type de problématiques, parce que la technologie ne s'arrête pas aux frontières.***

Mais au moment de comparer l'initiative européenne à ses aïeules américaines (dans le petit monde de la cyberguerre, la temporalité est sensiblement différente de la réalité), Bergstrom prend les devants:

> ***Le Cyber Storm est un exercice national, tandis que Cyber Europe est un exercice paneuropéen. C'est un exercice opérationnel, pas le nôtre; il implique des acteurs industriels, pas le nôtre; il teste la capacité de réponse des systèmes, pas le nôtre; il arrive à maturité, avec un budget de plusieurs millions de dollars, quand le nôtre est une première financée à hauteur de 100 000 euros.***

Dans son bilan final, l'Enisa se félicite du déroulement des opérations, estimant qu'il s'agit d'une "étape-clé" dans l'élaboration d'une véritable stratégie européenne de cyberdéfense, concertée et surtout, budgétée.

L'Enisa, inutile?

C'est là que le bât blesse. Doté d'un budget **légèrement inférieur à huit millions d'euros** (ce qui représente **60% du budget de la CNIL**, estimé à 13 millions d'euros), l'Enisa ne dispose aujourd'hui que d'un – faible – pouvoir de recommandation. Basé dans les faubourgs d'Héraklion, à 2396 kilomètres du Berlaymont, le siège de la Commission, ce "centre d'excellence" emploie aujourd'hui 44 personnes, auxquelles il faut ajouter une vingtaine de spécialistes externes et d'intérimaires.

Ulf Bergstrom le concède, cette année, il ne s'est rendu *"que deux fois à Bruxelles"* , et pas forcément pour porter la voix des experts en SSI (systèmes de sécurité de l'information).

Mise sur pied en 2004, l'Enisa devait en effet arriver au terme de sa mission en 2009. Son bail a finalement été prolongé jusqu'en mars 2012, mais son futur proche s'inscrit en pointillés: demain, l'agence sera peut-être phagocytée par Europol, la police criminelle intergouvernementale.

Pour Nicolas Arpagian, professeur à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et auteur d'un **Que Sais-je** (si, si) sur la cybersécurité, l'Enisa s'inscrit dans une logique européenne particulièrement floue autour des ces questions:

> ***[L'Enisa] relève du même système de pensée que le Sommet mondial sur la société de l'information. Alors qu'il devait être un Kyoto du numérique, celui-ci a seulement prouvé qu'il était une hybridation de la Foire de Paris. A Genève en 2003 comme à Tunis en 2005, on a vu des seconds couteaux européens prendre la parole à quelques mètres seulement des stands des fabricants de solutions de sécurité.***

> ***La question de son rôle se pose d'autant plus que le G8 a été le premier à développer un outil de veille 24/7 (PDF), sorte de SAV des puissants. Dans ces conditions, sans garanties sur leur avenir, dès 2008, les fonctionnaires de l'Enisa, et c'est bien normal, se sont plus préoccupés de leur reconversion professionnelle que des dossiers qu'ils portaient.***

750 hackers contre 44 fonctionnaires

Pourtant, de source officielle, l'Enisa ne se conçoit pas comme une vulgaire hotline destinée à déclencher des alertes Amber et signaler la disparition de quelques lignes de code ou d'une poignée d'informations bancaires. *"A ceux qui pensent que les cyberattaques sont un concept abstrait, je rétorquerai que chaque année, des millions de personnes sont directement victimes de ces pratiques"*, **déclarait Neelie Kroos** il y a quelques mois.

Ni une ni deux, quelques semaines avant l'exercice Cyber Europe, un expert américain **s'était risqué à chiffrer le coût d'une attaque massive** contre les infrastructures informatiques de l'Union européenne: il avait avancé le chiffre de 86 millions de dollars, auquel il adossait 750 hackers payés à plein temps. C'est 10 fois le budget de l'Enisa, avec un effectif 1700% plus important.

Game over?

—

Crédits photo: Flickr CC ***dsb rola***, ***thrig***, *Enisa,*