Rendre intelligible la conflictualité cybernétique

Si l'on considère la conflictualité cybernétique comme l'état d'intensité des attaques cybernétiques, alors, plus cette conflictualité est haute, plus tout un chacun est potentiellement susceptible d'être la cible d'une attaque ou d'en être la victime collatérale. Un des problèmes importants de la conflictualité cybernétique est qu'elle n'est ni connue ni perceptible par le grand public. Aussi, une menace que l'on ne perçoit pas ne permet pas l'anticipation ou la mise en œuvre d'une posture défensive. Si les grands groupes de sécurité propose des indicateurs, ceux-ci ne sont que peu médiatisés ou pas compréhensibles par l'utilisateur standard.

Pourtant la population est habituée à connaître l'état du monde par le biais d'indicateurs synthétiques dont la signification et le mode de calcul restent obscurs ne serait-ce que le PIB ou le taux de chômage par exemple. Il faut noter dans ces deux cas que c'est principalement la variation de l'indicateur qui est médiatisé. Donner aux médias un indicateur simple dont les variations sont synonymes d'évolutions substantielles de la situation est certainement une bonne méthode pour permettre la sensibilisation de la population. Cela a été le cas avec les indicateurs environnementaux au cours des dernières années.

Les indicateurs existants sont de plusieurs natures.

Il existe des indicateurs instantanés fournis par les éditeurs de logiciel qui remontent le nombre d'infections virales ou la volumétrie des attaques. Il existe également des indicateurs économiques présentant une évaluation des pertes subies par les entreprises en million d'euros ou de dollars. Les uns comme les autres ne décrivent pas la réalité du commun et de ce fait ne font pas sens. Une simple recherche sur internet laisse entrevoir l'état des lieux dans ce domaine : il n'existe pas une mesure communément admise et même les sources pour bâtir cette mesure ne sont pas disponibles. Il faut imaginer un indicateur synthétique et intelligible.

Un indicateur ouvert appuyé sur des données ouvertes.

Afin de construire un indicateur digne de confiance et compréhensible nous estimons qu'il faut que sa méthode de calcul soit ouverte et documentée et qu'il s'appuie sur des données de confiance en sources ouvertes. C'est certainement ce dernier point qui est plus problématique. A notre époque les sources d'information sur les attaques sont pour le moins lacunaires et fort peu sont disponibles en sources ouvertes. Les états, et en particulier l'état français, se sont emparés de cette question. Le service cybermalveillance.gouv.fr est l'ébauche d'une réponse cette question, mais ne fournit pas à l'heure actuelle les éléments nécessaires à l'élaboration d'un indicateur.

Inventaire des attaques et des sources d'information

Le but avoué est donc bien la production d'un indicateur synthétique, lisible par tous, ou d'un ensemble raisonnable d'indicateurs qui pourraient être complémentaires et tout autant lisibles. Evidemment, avant de pouvoir proposer un outil pertinent nous avons d'abord effectué un inventaire des attaques mais aussi des sources d'information du domaine.

Si l'on commence par ces dernières, nous pouvons déjà les classer en plusieurs catégories. Il y a ce qu'on appelle les *cyberthreats live maps* qui sont des cartes dynamiques représentant les attaques qui se déroulent actuellement dans le monde. L'une des plus connues est la carte Norse : map.norsecorp.com. Ils utilisent des agents logiciels, les *honeypots*, qui sont des logiciels qui miment les services usuels du réseau et qui sont faits pour être les réceptacles des attaques. Ce sont donc des pièges idéaux pour recenser les attaques mais aussi identifier les attaquants. On peut aussi utiliser les sources ouvertes de données. Un certain nombre de sites, comme stucco.github.io ou

opendatasecurity.io, proposent des données ouvertes thématiques. Notre tour d'horizon est clair sur un point : ces données ne sont pas toujours facilement exploitables et leur intégration dans un indicateur agrégé demande forcément un long travail de traitement de masse.

Ces sources d'information nous permettent de dresser un premier inventaire des attaques. Evidemment nous connaissons tous les attaques les plus typiques comme les DDOS (attaques par déni de service), les défacements ou les déstabilisations. Mais il est surtout important de les caractériser pour pouvoir les inventorier dans un indicateur efficace. Pour cela, nous utilisons une matrice générique développée par les laboratoires Sandia (www.sandia.gov). Celle-ci permet de dégager des caractéristiques importantes pour nous comme la détermination persévérante d'une menace dans la poursuite de son but ou comme la capacité de la menace à maintenir un niveau de discrétion nécessaire tout au long de la poursuite de son objectif ou encore comme le niveau de compétence théorique et pratique de la menace.

Ainsi la détermination d'un ou plusieurs indicateurs doit exploiter ces caractéristiques reconnues. Dans l'état actuel de nos travaux, nous avons clairement identifié des points incontournables à la construction d'indicateurs pertinents. Ceux-ci doivent être dépendants de la cible (particulier, entreprise, type de système d'information visé) et ils doivent être typés. Par exemple, ils peuvent être géographiques, purement numériques pour quantifier tous les risques informatiques, juridiques pour recenser les affaires liées aux attaques du cyber, etc.

Ce travail basé sur les sources et les méthodes existantes nous a permis de dégager des grandes catégories que nous pourrons appliquer à un certain nombre de situations et que nous allons agréger pour créer un indicateur, que nous espérons pertinent, sur l'état de la conflictualité cybernétique.

Pour en savoir plus et pour découvrir les travaux des étudiants du Master mention droit du numérique parcours Cyberveille Cyberdéfense Cybersécurité, que nous remercions pour leur contribution vous pouvez consulter cyberconflictualite.com.

Pascal Chatonnay est auditeur de 184ème session en région. Il est enseignant-chercheur à l'Université de Bourgogne Franche-Comté (UBFC). Il est directeur du département Métiers du Multimédia et de l'Internet. Il est membre de l'équipe pédagogique du Master Cyberveille Cyberdefénse Cybersécurité.

Christophe Lang est directeur adjoint de l'Unité de Formation et de Recherche SJEPG (Sciences Juridiques Economiques Politiques et de Gestion). Il est enseignant-chercheur en informatique de l'Université de Bourgogne Franche-Comté (UBFC). Il est responsable des enseignements d'informatique au sein du Master Cyberveille Cyberdefénse Cybersécurité.