Groupe académique de formateurs
HISTOIRE GÉOGRAPHIE GÉOPOLITIQUE SCIENCES POLITIQUES

Présentation des thématiques de Terminale

académie Clermont-Ferrand
RÉGION ACADÉMIQUE AUVERGNE-RHÔNE-ALPES
MINISTÈRE DE L'ÉDUCATION NATIONALE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION

THEME 6 – L'ENJEU DE LA CONNAISSANCE

Objet de travail conclusif

Le cyberespace : conflictualité et coopération entre les acteurs

- **Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.**

Le Livre blanc sur la défense et la sécurité nationale de 2013 a placé la **sécurité et la défense des systèmes d'information** au cœur des priorités stratégiques de la Nation.

Que faut-il protéger ?

Une des priorités affirmées par ce Livre blanc est de renforcer le niveau de sécurité des systèmes d'information essentiels au bon fonctionnement des **Opérateurs d'Importance Vitale** (**OIV**) et donc de la Nation. Un OIV est défini comme étant une personne morale publique ou privée qui gère ou utilise des établissements ou des ouvrages dont la destruction ou même l'indisponibilité obéreraient gravement le potentiel militaire, la force économique, la sécurité, voire la capacité de survie d'un État, ou mettraient en danger sa population (Journal officiel n°0219 du 19 septembre 2017, Vocabulaire de la défense : cyberdéfense). La liste des OIV (environ 250 dans les secteurs bancaire, santé, énergie, alimentaire, télécoms) est classée secret défense.

Qui en a la mission ?

L'Agence nationale de la sécurité des systèmes d'information (**ANSSI**) a pour mission d'établir les préconisations, de s'assurer du suivi des règles de sécurité, à la fois organisationnelles et techniques, des **systèmes d'informations d'importance vitale** (SIIV).

La France est le premier pays à s'appuyer sur la réglementation pour définir un dispositif efficace de cybersécurité de ses infrastructures d'importance vitale, qui sont indispensables au bon fonctionnement et à la sécurité de la Nation. En tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, l'ANSSI est chargée de piloter la partie cyber du dispositif et accompagne les OIV dans la mise en œuvre des nouvelles mesures.

Michel CHEMINAT, enseignant, responsable filière "Réseaux et Sécurité Informatique", ISIMA, Référent Enseignement de Défense et de Sécurité de l'université – Trinôme Académique de Clermont-Ferrand

L'ANSSI a participé à la rédaction des décrets qui fixent, pour les OIV, un certain nombre de mesures pour les systèmes d'information les plus critiques : le respect de référentiels de sécurité à appliquer par les opérateurs, la mise en place de dispositifs de défense adaptés, l'obligation de déclarer les incidents, et enfin la capacité pour l'État de vérifier par des audits le niveau de sécurité de ces systèmes (et en cas de crise grave, d'imposer les mesures nécessaires). Comme il s'agit de métiers très pointus, l'agence a mis en place des visas de sécurité qui permettent d'identifier des **prestataires de confiance**, des certifications de produits et services de sécurité. On peut citer l'exemple des sondes de détection de menaces pour lesquelles Thales et Gatewatcher ont reçues le visa de sécurité de l'agence (avril 2019) après des tests de robustesse et de confidentialité (sonde dite souveraine : matériel et logiciel développés en France).

Et au niveau européen ?

En parallèle, l'ANSSI a joué un rôle important dans l'élaboration de la directive ***Network and Information System Security*** (NIS, adoptée par les institutions européennes le 6 juillet 2016). Cette directive poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.

On retrouve aussi l'influence de l'agence dans l'adoption du règlement dit **Cybersecurity Act** adopté par le parlement européen le 12 mars 2019. Celui-ci traite de deux sujets distincts, mais complémentaires : l'adoption d'un mandat permanent pour l'**ENISA** (*European Network and Information Security Agency* - Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information) et la définition d'un cadre de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification.

Et sur le plan militaire ?

Pour compléter, sans être exhaustif, l'ANSSI joue aussi un rôle dans le domaine militaire. En effet, un partenariat en matière de cyberdéfense a été renouvelé le 13 novembre 2019 avec le commandement de la cyberdéfense (**COMCYBER**, créé en 2017) dans le cadre de la cyberdéfense des réseaux du ministère des armées.

La France a fait le choix d'un système séparant les capacités et missions défensives et les capacités et missions offensives. Florence Parly a annoncé en janvier 2018 que les armées françaises seraient dotées désormais d'une doctrine de **lutte informatique offensive** (LIO) renforçant sa politique de **lutte informatique défensive** (LID). Ces doctrines s'inscrivent dans le cadre de la **posture permanente de cyberdéfense** (PPC), créée par la loi de programmation militaire (LPM) 2019-2025. Assurée par le COMCYBER, cette posture permet de protéger 7 jours sur 7 et 24 heures sur 24 tous les réseaux du ministère des Armées afin d'anticiper et réagir à toute attaque contre les intérêts de notre défense.

Il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée à laquelle la France peut répondre par la **légitime défense** en vertu de l'article 51 de la Charte des Nations unies. Une cyberattaque pourrait être qualifiée d'agression armée dès lors qu'elle provoquerait des pertes humaines substantielles, ou des dommages physiques ou économiques considérables. Cela serait le cas d'une opération dans le cyberespace provoquant une déficience des infrastructures critique avec des conséquences significatives, ou susceptibles de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques et de faire de nombreuses victimes. Dans une telle hypothèse, les effets de cette opération seraient similaires à ceux qui résulteraient de l'utilisation d'armes classiques. Pour être qualifiée d'agression armée, la cyberattaque doit également avoir été perpétrée, directement ou indirectement, par un État.

Quelques notions complémentaires

La surveillance de l'ensemble des systèmes d'information, que ce soit dans la sphère publique, privée ou militaire engendre des ensembles de données devenus si volumineux qu'ils dépassent l'intuition et les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données. On parle alors de ***Big Data***. Ce concept regroupe une famille d'outils qui répondent à une triple problématique dite règle des 3V. Il s'agit d'un Volume de données considérable à traiter, une grande Variété d'informations (venant de diverses sources, non-structurées, organisées, open …), et un certain niveau de Vélocité à atteindre, autrement dit de fréquence de création, collecte et partage de ces données.

S'appuyant sur ces outils, la ***Data Science*** est la science des données. C'est la discipline qui permet d'explorer et d'analyser les données brutes pour les transformer en informations. Ce sont, entre autre, ces outils qui ont été utilisés pour **déstabiliser des processus électoraux** (Facebook – Cambridge Analytica, élections présidentielles américaines de 2016).

L'analyse de ces données fait de plus en plus appel à l'**Intelligence Artificielle** (IA), un ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines (des algorithmes) capables de simuler l'intelligence (définition Larousse). Le terme d'IA est apparu en 1950 dans un article publié par Alan Turing (1912-1954). Sous cette appellation générale d'IA est apparu dès les années 1980 le ***Machine Learning*** ou **Apprentissage Automatique** et ce n'est que depuis une dizaine d'année que de nouveaux algorithmes utilisant des **réseaux de neurones artificiels** ont permis des progrès importants. Cette dernière catégorie d'IA se retrouve sous la dénomination de ***Deep Learning*** ou **Apprentissage Profond**.
Dans le domaine cyber, l'IA est utilisée pour faire de la détection de virus ou d'intrusion sur un système informatique, mais aussi par les attaquants pour trouver des vulnérabilités.

Il est maintenant possible de créer une vidéo d'une personne et de lui faire tenir n'importe quel discours par exemple un discours de Donald Trump prononcé par Emmanuel Macron. Bientôt seules des IA performantes seront capables de détecter la supercherie.

Plus aucun traitement de l'information aujourd'hui ne se fait sans avoir recours à des outils **cryptographiques**. La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'**authenticité** d'un message (qui a envoyé ce message ?) ou encore assurer son **intégrité** (est-ce qu'il a été modifié ?). Il faut souvent rajouter la garantie d'avoir accès à ses données (la **disponibilité**).

Ce sont les mêmes outils cryptographiques qui ont permis la création des ***Blockchains***, ou chaînes de blocs. Il s'agit d'une technologie de stockage et de transmission d'informations sans organe de contrôle, une sorte de base de données répartie, sécurisée avec une traçabilité infalsifiable. Son utilisation est connue avec les **cryptomonnaie** comme le ***Bitcoin*** ou l'***Ethereum***, mais son usage peut s'envisager dans bien d'autres domaines. Citons deux exemples, les notaires et le cadastre. Que fait le notaire ? Il conserve, sécurise les données de ses clients, authentifie les échanges, garantit leur infalsifiabilité. On retrouve les caractéristiques principales d'une Blockchain. Côté cadastral, le Ghana teste un registre décentralisé fonctionnant avec la Blockchain pour palier à une déficience administrative.

Toujours avec des outils cryptographiques, il est possible de se cacher, de se rendre anonyme sur le web, on parle alors du ***Dark web***, l'Internet sombre. Le dark web rassemble un réseau de sites qui ne sont pas indexés par les moteurs de recherches traditionnels et accessible via des navigateurs web particuliers. Il n'est pas difficile d'accéder par exemple au réseau ***TOR*** (***The Onion Router***) et de rechercher des site web dont les adresses sont anonymes (à la place de .com ou .fr, le nom de domaine est en **.onion**).

Les cyberattaques auxquelles les États et les acteurs privés sont confrontés sont, par nature, difficiles à caractériser dans le cyberespace car les attaquants rebondissent de serveurs en serveurs sur le dark web (ceci est fidèlement décrit dans l'épisode 5 de la saison 4 de la série Le bureau des légendes). L'attribution d'une cyberattaque d'origine étatique relève d'une décision politique nationale.

Michel CHEMINAT, enseignant, responsable filière "Réseaux et Sécurité Informatique", ISIMA, Référent Enseignement de Défense et de Sécurité de l'université – Trinôme Académique de Clermont-Ferrand

PISTES POSSIBLES

- Utiliser un navigateur TOR (travail à la maison) et observer par où passe la connexion à un site web (en cliquant sur le i à gauche de la barre d'adresse). Réfléchir à un usage fréquent de TOR : contourner la censure de certains pays (exemple de BBC News).
- Echange de documents chiffrés entre élèves : tutoriel de la CNIL.
- Recherche sur des attaques cyber de l'actualité (la collectivité Aix-Marseille-Provence en avril 2020, Fleury Michon en avril 2019 …).
- Travail autour du film biographique sur Alan Turing, Imitation Game, sorti en 2014.

RESSOURCES INDICATIVES

- Sitographie

- Journal officiel, Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés).

- Site de l'ANSSI, textes relatifs à la protection des opérateurs d'importance vitale (OIV).

- Site du ministère des armées, Droit international appliqué aux opération dans le cyberespace.

- Site de l'ANSSI, page présentant le règlement européen Cybersecurity Act.

- Site de l'ANSSI, page présentant le Network and Information System Security Directive.

- Site de la CNIL, Comprendre les grands principes de la cryptologie et du chiffrement.

- Site du projet TOR pour télécharger le navigateur TOR et profiter d'une navigation privée sans suivi, surveillance ou censure.

- Adresse du moteur de recherche DuckDuckGo sur TOR : http://3g2upl4pq6kufc4m.onion

- Adresse du site web de la BBC sur TOR : https://www.bbcnewsv2vjtpsuy.onion