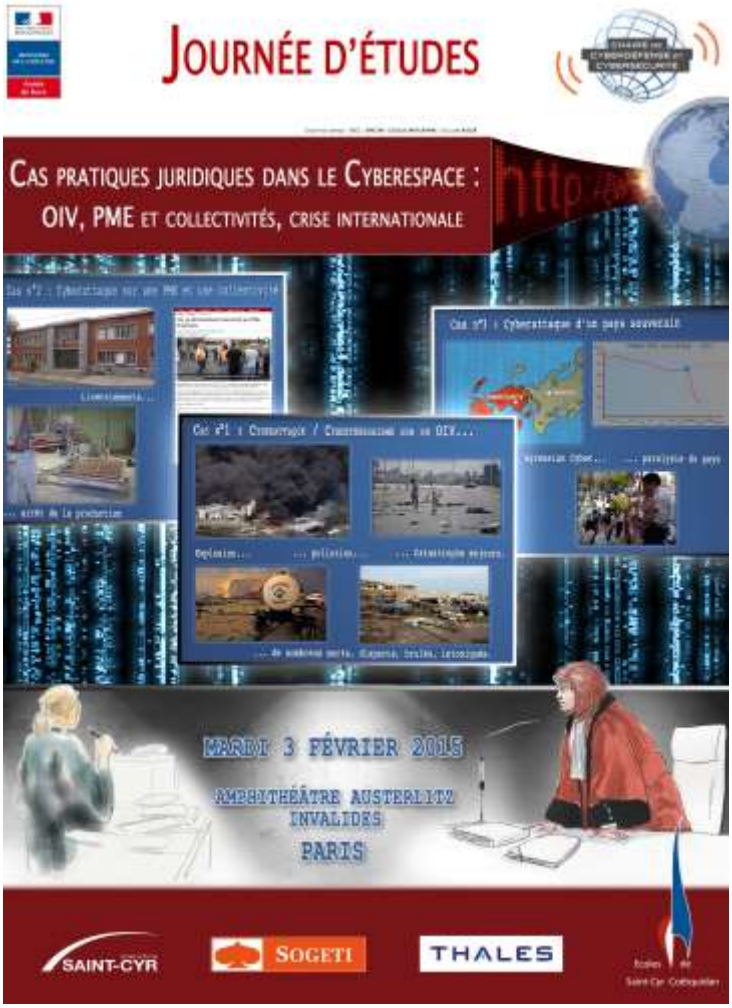
Résumé de la journée d'études du 3 février 2015

Cercle National des Armées, et les Invalides, Paris.



Si les effets dévastateurs que les Cyberattaques peuvent faire peser sur nos systèmes d'information commencent à être appréhendés, tout comme les catastrophes au niveau national ou international que ces dernières peuvent engendrer, force est de constater que le cadre juridique à appliquer en de telles circonstances reste parfois complexe. Alors même que les frontières nationales du Cyberespace sont parfois imprécises, faut-il en rester aux lois nationales ? Lesquelles sont à appliquer ? A partir de quels faits juridiques ou seuils de gravité les lois internationales entrent-elles en vigueur ? Quelle qualification de ces attaques dans ces trois scénarios, quelles règles de droit et lois nationales et internationales s'appliquent ?

La chaire Cyberdéfense et Cybersécurité Saint-Cyr / Sogeti / Thales a ainsi organisé le 3 février 2015 à Paris un exercice de recherche appliquée, de forme originale, à la conjonction des questions de Défense et de Sécurité, lequel a rencontré un franc succès pour le public présent, et généré un fort enthousiasme de la part des intervenants qui se sont impliqués dans cet exercice.

Il s'est agi d'effectuer des exercices pratiques d'expertise juridique appliqués à trois scénarios fictifs mais réalistes, couvrant un large panel des risques et menaces Cyber, tant que le plan local, national ou international, avec des tribunaux simulés pour la circonstance, avec ses plaidoiries, expertises et jugements. Cet exercice se voulait aussi interactif, le public ayant la possibilité de poser des questions après le jugement final.

Les scénarios ont ainsi couvert l'actualité des menaces Cyber qui pèsent sur nos organismes d'importance vitale (OIV), sur nos entreprises, et sur notre Etat.

***

Présentée en introduction par Christian Daviot de l'ANSSI, l'imminente publication des décrets d'application de la Loi de Programmation Militaire (LPM) relatifs aux obligations imposées aux OIV, et aux sanctions applicables en cas de non-respect, introduisait tout naturellement le thème du premier scénario, lequel traitait d'une attaque de grande ampleur sur un OIV.

Le détail des différents scénarios a été présenté par des élèves officiers de l'Ecole Spéciale Militaire de Saint-Cyr.

Cas n°1 : cyberattaque et cyberterrorisme sur un OIV :

1ère phase du scénario : un OIV a été la victime de plusieurs incidents ayant provoqué l'arrêt total de l'activité de l'entreprise, et des manquements à la sécurité ont été relevés. Un sous-traitant était en charge de la mise en place des systèmes de sécurité informatique.

L'arrêt de l'activité étant très préoccupant au niveau sécuritaire, un procès a lieu visant à déterminer les responsabilités et les manquements observés lors de la gestion de l'incident par l'entreprise.

Le procureur, représenté par Franck Pavéro, prend la parole et présente ses accusations. Il demande d'abord que l'affaire soit traitée avec rigueur du fait de l'activité sensible de l'OIV et des problèmes de sécurité publique qui en découlent. De plus, il souligne que la société n'est toujours pas à jour quant aux mesures de sécurité à implémenter**.**

Aussi il demande que les responsabilités de l'entreprise soient engagées, et demande une condamnation exemplaire pour non déclaration de l'incident aux autorités, de la responsabilité des personnes morales, pour faute, négligence ou imprudence ayant entrainée l'exposition d'autrui au danger.

Maître Cécile Doutriaux, qui représente les intérêts de l'entreprise, explique dans sa plaidoirie que la société a été mise en demeure de réaliser d'importants travaux pour sécuriser ses systèmes d'informations. Conformément à l'article L.1332-6-1 de Code de la Défense, le coût de ces travaux sont intégralement mis à la charge de l'entreprise, qui a dû faire face à une dépense élevée et imprévue.

La société a été victime d'une intrusion informatique avant l'achèvement des travaux de mise en conformité. C'est exclusivement la survenance d'un élément extérieur, totalement imprévisible, qui l'a empêchée d'exécuter ses obligations administratives. Concernant la déclaration d'incident « sans délai » préconisée par la loi, plusieurs experts ont établi que l'intrusion informatique se serait produite plusieurs mois avant de pouvoir être détectée. Par conséquent, la société était dans l'impossibilité de déclarer un incident dont elle-même ignorait l'existence. De plus, si on examine les législations des différents pays européens, la France est le pays le plus exigeant vis-à-vis des opérateurs d'importance vitale, puisque la LPM ne distingue pas selon que l'OIV est une grande entreprise ou une PME, une société privée ou une administration publique.

Par ailleurs, l'arrêt d'urgence de l'entreprise, consécutif à cette intrusion informatique, a eu un impact humain, organisationnel et financier important (chômage, paiement des expertises…). La faire payer davantage la soumettrait à de nouvelles difficultés. Ainsi l'avocat se demande quel est l'objectif de la condamnation : obliger la société à déposer le bilan ou rechercher les réelles responsabilités des différents acteurs ? En effet, les prestations effectuées par le sous-traitant doivent faire l'objet d'une analyse approfondie. Il demande enfin le renvoi de l'affaire pour solliciter auprès du juge d'instruction un complément d'informations nécessaire à la manifestation de la vérité et requiert la déclassification de certaines données, afin déterminer avec précision la responsabilité de chacun des acteurs.

Le président du tribunal, dont le rôle est assuré par le général Marc Watin Augouard prend enfin la parole et rend ses conclusions. Il reconnait la responsabilité de l'entreprise sur l'absence de déclaration d'incident aux services du 1er ministre. Les responsabilités de l'entreprise et de son sous-traitant sont avérées pour la mise en danger d'autrui, bien que cette accusation manque d'éléments. En conséquence, le président ordonne le renvoi de l'affaire pour complément d'enquête.

2ème phase du scénario : l'intrusion dans le système de sécurité de l'OIV a permis l'introduction d'un virus en son sein, qui a été activé pour provoquer l'explosion de l'usine, entrainant des morts et la fuite de fumées toxiques. La piste terroriste est validée après enquête.

Le procureur fait l'exposé de ses accusations. Il considère que le sous-traitant a pu agir à l'insu de l'entreprise parce que le système lui en donnait la possibilité, et pointe ainsi la responsabilité de celle-ci dans le manque de précautions dans l'élaboration du système de sécurité. Ainsi l'acte terroriste n'est pas de sa responsabilité directe, mais l'entreprise est responsable du fait qu'elle a créé et maintenu les conditions nécessaires à l'exécution de l'attaque. L'entreprise est considérée par le procureur comme seule responsable de la création des conditions de l'incident, et son sous-traitant est poursuivi pour incompétence et négligence ayant entrainé la mort.

L'avocat de la défense rappelle, lors de son intervention, que l'explosion n'est pas due à l'intrusion elle-même, mais à l'activation du virus comme une bombe logique dans les systèmes informatiques. Ainsi les accusations de mise en danger délibérée et immédiate d'autrui ne sauraient tenir. L'avocat souligne de plus que si l'organisation terroriste se revendique comme un Etat par conséquent, la juridiction nationale saisie n'est pas compétente pour juger l'affaire. Il admet toutefois, que compte tenu de l'importance des dommages et des pertes humaines, la société entend assumer ses

responsabilités, mais exclusivement à la mesure des manquements qu'elle a commis, et la responsabilité pour non déclaration de l'incident est admise.

Une expertise juridique est menée en la personne du commissaire de 1ère classe Pascal Brangetto**.** Il rappelle que si un Etat se rend coupable d'une telle attaque, elle est considérée comme un conflit armé. Dans le cas d'un groupe terroriste, si celui-ci agit depuis le territoire d'un Etat, on peut demander à ce dernier de mettre fin à ses activités par des mesures policières, voire militaires.

Caroline Brandao, représentant le Comité International de la Croix-Rouge, intervient ensuite afin de préciser les difficultés que posent de telles situations. Elle souligne que dans cette affaire, le droit national doit s'appliquer car il ne s'agit pas d'un conflit armé. La situation et le droit pourraient évoluer dans le cas de l'allongement de l'action dans le temps, et d'une montée en intensité dans les évènements. La caractéristique d'une cyberattaque réside dans le fait qu'elle ignore les principes de distinction et de proportionnalité du droit des conflits armés (DCA).

Le président rend enfin ses conclusions et considère que le jugement de l'acte terroriste doit être renvoyé devant la cour d'Assise de Paris. Ensuite, le sous-traitant est reconnu coupable d'homicides et blessures involontaires. Enfin, aucune personne physique n'est reconnue coupable de la création de dommages directs, mais coupable de la création de leurs conditions.

Cas n°2 : attaque conjointe sur une PME et une collectivité territoriale :

Scénario : Une entreprise bretonne se voit contrainte de fermer une antenne de son activité afin de faire face à la concurrence, entrainant le licenciement des employés de cette antenne. Le neveu de l'un des employés, afin de venger son oncle, va lancer une cyberattaque contre l'entreprise, ainsi qu'à l'encontre de la mairie de la ville qui avait accordé à l'entreprise des moyens de stockage. L'attaque a par ailleurs parmi l'installation d'un logiciel qui transférait des informations à un concurrent étranger de l'entreprise.

Un jeune hacker a été interpelé dans un cybercafé et a été reconnu coupable de l'attaque. S'ouvre alors son procès. Celui-ci débute avec la qualification juridique des faits. Pour maître Charlotte Barraco-David, qui ne retient pour cette analyse que les faits spécifiques liés au cyber, le jeune hacker se rend coupable d'usurpation d'identité numérique, de collecte déloyale de données à caractère personnel, d'atteinte au secret des correspondances, d'accès ou maintien frauduleux dans système traitement automatique de données (STAD), d'entrave au fonctionnement d'un STAD, d'introduction, de suppression, et d'extraction frauduleuse de données, et enfin d'entente établie en vue de participation à une fraude informatique à un STAD.

Anne Souvira prend ensuite la parole afin de présenter le point de vue de l'enquêteur et les difficultés qui se présentent à lui lors d'une telle enquête. Elle indique que les éléments de preuves qui vont prouver les infractions se situent dans les systèmes d'information. La difficulté réside dans le fait qu'une entreprise de sécurité informatique corrompt généralement les preuves par son intervention dans les systèmes. De plus, une telle enquête est très technique et demande beaucoup temps. Enfin, une coopération policière internationale se doit d'être mise en place pour poursuivre le concurrent étranger qui récoltait des renseignements sur l'entreprise.

L'avocat de la partie civile, maître Marie-Hélène Tonnellier, prononce ensuite sa plaidoirie en faveur de l'entreprise. Il souligne l'intention malveillante du jeune hacker ne fait pas de doutes puisqu'il a commis des usurpations d'identité à trois reprises. La collecte déloyale de données et l'atteinte à la confidentialité des échanges renforcent la gravité de l'acte, et démontre à nouveau le caractère malveillant de l'acte. Le vol de données, et la modification de certaines de celles-ci doivent être pris en compte pour imposer une peine exemplaire contre le hacker.

La défense, représentée par maître Corentin Pallot, prend la parole et rejette les accusations d'usurpation d'identité et d'atteinte au secret de la correspondance. Il tente de démonter les accusations en entrant dans une analyse très technique des textes afin de tenter de disculper son client de ces accusations. L'avocat admet que le jeune hacker a commis des infractions, mais ceci dans le seul but d'une conception assez naïve de se rendre justice soi-même. Aussi les peines demandées par la partie civile sont considérées comme excessives, et la défense demande d'application d'une peine pédagogique.

Le jugement est rendu par Myriam Quéméner et considère le jeune hacker comme coupable d'usurpation d'identité, de collecte déloyale de données et d'atteinte au secret des correspondances. Les condamnations rendues sont importantes et visent à faire revenir le jeune hacker à la réalité.

Cas n°3 : cyberattaque d'un pays souverain et crise internationale :

Scénario : Un pays, la Bordurie, mène une cyberattaque contre son voisin, la Transyldavie, afin de servir ses intérêts géopolitiques. L'attaque comporte plusieurs phases. La première consiste en la mise en place de virus et logiciels espions dans les systèmes de sécurité du pays afin de le désorganiser et de récolter des informations sur les plans de défense du pays. La seconde phase provoque le dysfonctionnement de réseaux électriques et de communications civils et militaires, entrainant la mort de plusieurs civils. La troisième provoque la désactivation d'un bouclier antimissile, et la dernière vise des personnes politiques du pays. La Transyldavie va réagir en organisant une riposte du même type, entrainant elle aussi des morts. L'escalade de la violence aboutit en final à la mise en place d'opérations militaires classiques.

Une cour internationale de justice est rassemblée, et maître Cécile Doutriaux, qui défend les intérêts de l'Etat transyldave prend la parole. Elle explique que la responsabilité de l'attaque revient bien à l'Etat bordure, et que la chaine de décision est éloquente à ce sujet. Elle souhaite en conséquence que la Bordurie soit condamnée de manière exemplaire compte tenu de l'ampleur de l'attaque et de la gravité de ses conséquences pour le pays et sa population. Ensuite, elle soutient que, bien que les deux premières phases de l'attaque n'aient pas eu de conséquences majeures pour la sécurité interne du pays, les deux dernières phases ont eu, quant à elles, des conséquences beaucoup plus graves, permettant de considérer l'attaque comme une agression armée, et donc de justifier par la légitime défense la contre-offensive menée. Elle demande enfin une sanction sévère de l'Etat attaquant.

Eric Pomès, le défenseur des intérêts bordures, prend ensuite la parole pour répondre à l'argumentaire transyldave. Il soutient que son pays est victime des apparences dans un premier temps, et d'une attaque dans un second temps. En effet, rien ne permet, selon lui, de prouver

l'allégeance des attaquants à la Bordurie, et donc la responsabilité de l'Etat bordure. En conséquence, la riposte, présentée comme une contre-offensive par la Transyldavie, est considérée par la Bordurie comme une attaque armée illégale, qui nécessite la condamnation de la Transylvanie.

Une expertise, visant à établir si le droit international humanitaire est applicable dans ce cas, est ensuite menée par Caroline Brandao, représentante de la Croix-Rouge. Ainsi, la situation est bien celle d'un conflit armé, dans laquelle s'applique donc le droit international humanitaire. Or ce dernier a été violé sur les principes de distinction. Cependant, l'établissement des responsabilités est difficilement discernable.

Le président de la cour internationale de justice, le commissaire en chef Eric de Beauregard, rend enfin sa décision et considère que la Bordurie est bien responsable de la cyberattaque. De plus, la cour considère que cette attaque constitue un conflit armé, et que la légitime défense est en conséquence admise pour la contre-offensive menée par la Transyldavie. Enfin, le fait que des victimes civiles aient été tuées dans les deux pays entraine la cour à leur imposer de réparer les dommages causés.

***

Après ces exercices pratiques d'expertise juridique, la journée d'étude a été complétée par les interventions de la Réserve Citoyenne de Cyberdéfense pour expliquer la contribution de cet organisme aux questions de cyberdéfense, et de représentants des entreprises Sogeti et Thales afin qu'ils présentent les solutions industrielles pour la protection des Organismes d'Importance Vitale (OIV) et des entreprises.

Réserve Citoyenne de Cyberdéfense :

Représentée par Marie-Claire Plaud et Jean-Paul Defransure, la Réserve Citoyenne de Cyberdéfense a pour vocation de rassembler des citoyens de tous domaines en vue de d'étudier, de sensibiliser et de conseiller les entreprises sur la thématique de Cyberdéfense. Créée en 2012 et forte de 150 membres et de nombreux partenaires industriels, la Réserve Citoyenne de Cyberdéfense est présente sur tout le territoire français, au travers de pôles spécialisés relatifs aux divers enjeux que pose la cyberdéfense.

Sogeti et Thales :

Christian Guerrini et Thieyacine Fall, respectivement directeurs de mission au sein des groupes Sogeti et Thales, ont présenté les solutions industrielles face aux enjeux de la cyberdéfense. Après avoir rappelé l'omniprésence des systèmes industriels dans tous les secteurs de la société, ils ont expliqué l'importance des potentiels impacts d'une attaque contre ces systèmes industriels, qui y sont de plus en plus exposés. C'est la raison pour laquelle il existe une pression règlementaire et normative importante. De plus, l'anticipation, la protection, la dissuasion et la réaction en cas d'attaque sont les attitudes vitales à adopter pour une entreprise. Ensuite, les entreprises peuvent bénéficier d'un large panel de services de cybersécurité proposé par des groupes comme Sogeti et Thales. Enfin, des services de supervision de sécurité peuvent épauler les entreprises dans leurs systèmes de protection.

En conclusion, la qualité et l'expertise des intervenants qui se sont prêtés à ces exercices de jeu de rôle juridique ont été unanimement saluées. L'originalité de cette approche a ainsi permis de traiter d'une question de grande actualité, par anticipation de cas d'attaques Cyber de différentes ampleurs sur des cibles de grande importance pour notre Nation. En conséquence, la réussite de cette journée organisée par la chaire Cyberdéfense et Cybersécurité Saint-Cyr / Sogeti / Thales, nécessitera de réitérer l'exercice dans les années à venir.

Mathieu Houette, CREC Saint-Cyr,

Gérard de Boisboissel, CREC Saint-Cyr.

PS : L'ensemble des prestations ayant été filmé, un DVD sera disponible sur requête auprès madame Séverine Bonnardet, de la Fondation Saint-Cyr : severine.bonnardet@f-sc.org