Conférence Internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone

Abidjan, du 8 au 10 février 2016

Les réponses juridiques, judiciaires et policières au cyberterrorisme

Bertrand Warusfel

Professeur des Universités,

Faculté de droit - Université Lille 2,

avocat au barreau de Paris

ORGANISATION INTERNATIONALE DE la francophonie

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

Qu’est-ce que le cyberterrorisme ?

- Le croisement du terrorisme et de la révolution numérique
- A la fois attaque contre les objectifs numériques et utilisation des réseaux pour l’apologie et le soutien au terrorisme ?
  - mais, cette extension de qualification peut poser des difficultés juridiques (notamment, en assimilant l’intention terroriste à l’acte terroriste lui-même)

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

Plus particulièrement, des attaques contre des infrastructures numériques

- *Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes : (…) 2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code* (art. 421-1 Cpen, FR)

Rule 36 – Terror attacks

Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population, are prohibited.

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

La prévention du cyber-terrorisme et la cybersécurité sont donc convergentes

- protection des infrastructures d'information étatiques

mais aussi

- protection des infrastructures d'information critiques

ou, plus encore

- celle de tous les opérateurs d'importance vitale (OIV), quel que soit leur secteur

voire

- celle de tous les grands prestataires de service en ligne (future directive de l'UE : NIS en 2016)

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

Comment renforcer la prévention des actes de cyberterrorisme ?

- Imposer des obligations de sécurité à tous les opérateurs (sectoriels ou non) concernés
- Les obliger à notifier les incidents et les attaques
- Installer des sondes de détection d'intrusion
- Échanger de l'information sur les attaques avec le privé

+ (si l'on recouvre la lutte contre la propagande en ligne) :

- Surveiller le web et imposer la fermeture (administrative ou judiciaire ?) des sites

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

Préparation de la réaction d'urgence

- Donner la compétence pour recueillir les informations techniques caractérisant les attaques
- Autoriser les équipes de l'autorité nationale de sécurité à intervenir
- Compétence pour mener des actions tendant à entraver les attaques

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

Compétence juridique pour mener des actions tendant à entraver les attaques

Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque.
(*Art. L. 2321-2. CDéf, FR)*

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

Des instruments de répression des actions cyberterroristes

- Application des dispositions de droit commun
- Application des dispositions spéciales réprimant la criminalité numérique
- Possibilités de renforcer les sanctions de droit commun lorsqu'il y a atteinte à des infrastructures critiques ou étatiques
- Faudrait-il des infractions cyber-terroristes spécifiques ?

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ

En conclusion

- La numérisation croissante ouvre de nouvelles perspectives aux agissements terroristes
- La sécurisation des systèmes d'information (en particulier, ceux des opérateurs d'importance vitale et des grands prestataires) contribue aussi à prévenir les actes cyber-terroristes
- La lutte contre la propagande en ligne en relève pas de la même logique et nécessiter un équilibre entre compétences administratives et judiciaires (afin de préserver les libertés d'expression et de communication)
- Lorsque la loi donne des compétences aux autorités de cyberdéfense, cela permet la riposte rapide en cas d'attaque cyber-terroriste
- Les infractions pénales préexistantes en matière de terrorisme ou de cybercriminalité (éventuellement adaptées) permettent de faire face au cyber-terrorisme

bertrand.warusfel@univ-lille2.fr

Université de Lille 2 DROIT ET SANTÉ