La règle du boomerang

COnférence sur la Réponse aux Incidents et l'Investigation Numérique
Lille

Eve Matringe

Avocate
Barreau de Luxembourg
Etude Roy Nathan
Membre de l'Association Luxembourgeoise des Avocats Pénalistes

27 janvier 2016

La règle du boomerang

La règle du boomerang
CONférence sur la Réponse aux Incidents et l'Investigation Numérique
Lille

Eve Matringe

Avocate
Barreau de Luxembourg
Etude Roy Nathan
Membre de l'Association Luxembourgeoise des Avocats Pénalistes

27 janvier 2016

Eve Matringe, avocate au barreau de Luxembourg, mais je vais aujourd'hui me placer du point de vue du droit français.

Conditions d'utilisation

La Problématique

D'un point de vue juridique, lorsqu'une entreprise ou une institution est victime d'une attaque informatique :

* Est-il juridiquement possible de contre-attaquer ?
* Le cas échéant, quels sont les points à envisager ?

La règle du boomerang

La Problématique

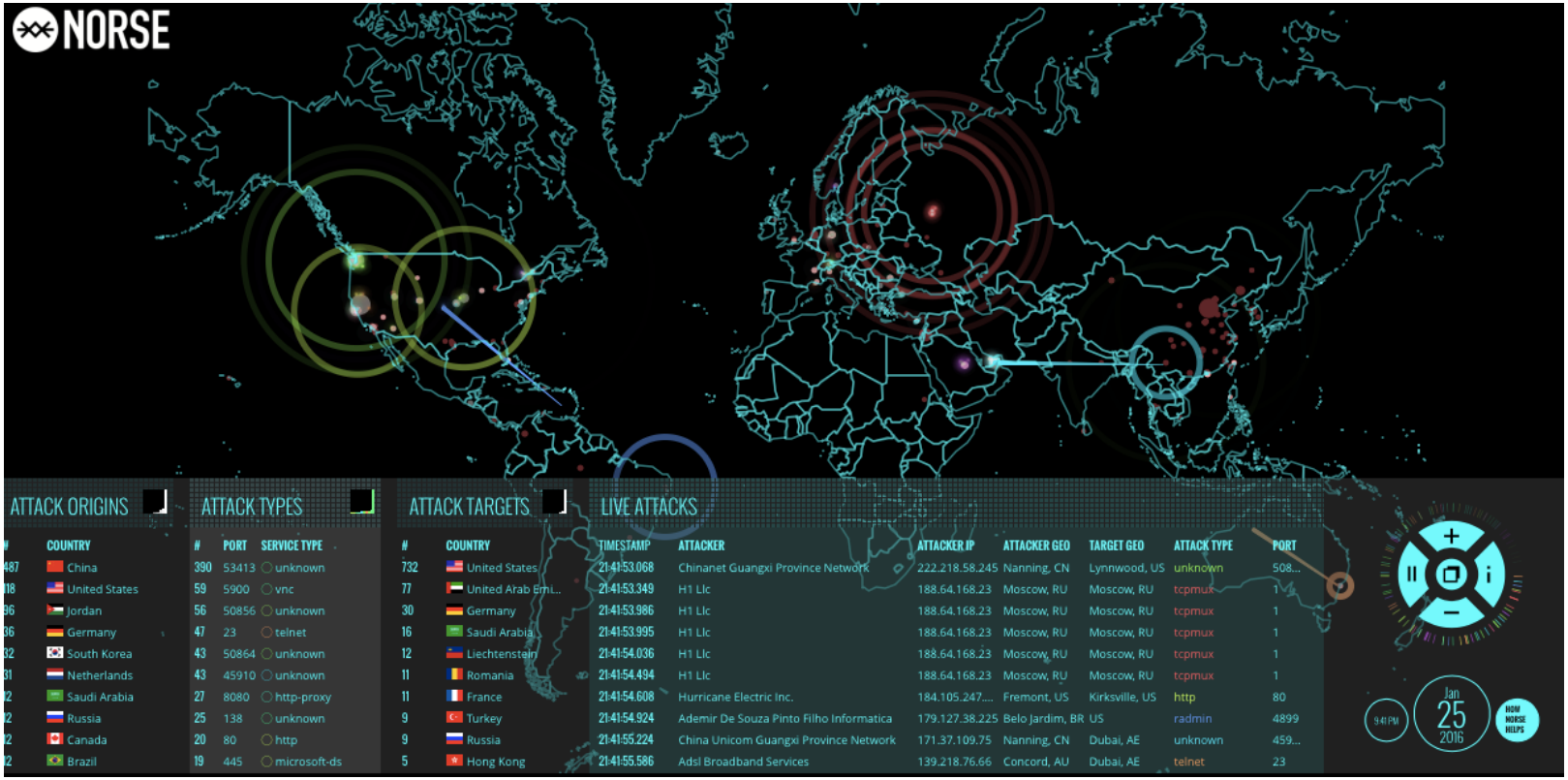
La Problématique

D'un point de vue juridique, lorsqu'une entreprise ou une institution est victime d'une attaque informatique :

* Est-il juridiquement possible de contre-attaquer ?
* Le cas échéant, quels sont les points à envisager ?

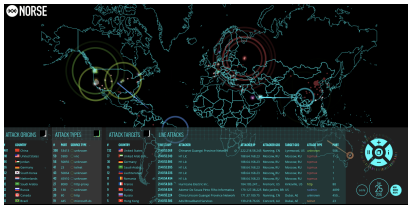
Il s'agit ici uniquement d'envisager l'aspect juridique de la réplique à une attaque informatique. Je suis avocat, pas spécialiste en investigation numérique. Les techniques utilisées ne relèvent donc pas de ma sphère de compétence.

Pourquoi l'analogie avec le Boomerang ? parce qu'il s'agit d'une arme présentant un aspect technique important, et que celui qui ne le maîtrise pas court des risques non négligeables du fait de son utilisation inappropriée. Donc la première règle, pratique, est que si on ne sait pas ce qu'on fait, mieux vaut s'abstenir de répliquer.



Source : http ://map.norsecorp.com/

La règle du boomerang



Source : http ://map.norsecorp.com/

ce site propose une infographie d'attaques en cours, sans que je sache bien si c'est juste une illustration aléatoire ou si cela correspond bien à des données en temps réel.
entreprise ou institution, c'est-à-dire personne publique, relevant du droit public. La réplique peut en effet relever du droit international, cela d'autant plus que la délinquance informatique par le moyen des réseaux est forcément internationale. Je vais donc vous présenter les deux aspects, du point de vue du droit français (avec un peu de droit de l'Union européenne).
Attaque informatique : je pense que vous voyiez mieux que moi ce dont il peut s'agir. En gros, tout ce est visé par les articles 323-1 et suivants du Code pénal français : intrusion, altération de données, entrave au système, destruction du système, en bande organisée éventuellement. A cela s'ajoutent les infractions en matière de données personnelles (art.226-16 et s.), et d'atteinte au secret des correspondance (art.226-15).

Réplique : il s'agit ici uniquement de la riposte informatique. Autrement dit, dans quelle mesure la "Légitime défense" peut justifier la réplique informatique de l'entité victime d'une attaque informatique.

Effectivité

Effectivité

Avoir un droit non effectif = ne pas en avoir

La règle du boomerang

Effectivité

Effectivité
Avoir un droit non effectif = ne pas en avoir

Pourquoi la question de la riposte à une attaque informatique doit être envisagée par le droit ? Le droit garantit un certain nombre de choses, dont la sécurité et l'égalité, tant aux individus qu'aux entités publiques comme privées (vie privé, droit de propriété, intellectuelle comme matérielle). S'il n'y a pas de sanction effective des atteintes portées à ces droits, alors le droit n'existe plus ou c'est tout comme.
Personne ne porte d'armure aujourd'hui, parce que ça ne protège plus contre les armes actuelles.
Or offrir peut-être une réparation a postériori n'est pas satisfaisant s'il est possible d'éviter le plus gros du préjudice. A l'inverse, il ne faut pas non plus permettre la commission d'infraction pénale sous prétexte d'être la victime d'une attaque.
La question de la riposte à une attaque poste aussi le problème de la réciprocité, notion de droit international. Ainsi, le droit français confère une immunité aux Services secrets qui commettraient des actes réprimés par les articles 323-1 et suivant du Code pénal, pour les motifs : (article 323-8) pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code, et notamment "Les intérêts économiques, industriels et scientifiques majeurs de la France". En d'autres termes, le droit français excuse l'attaque informatique à l'étranger aux fins d'espionnage économique.
Dans ce cas, comment invoquer la légitime défense pour justifier une riposte alors que nos propres agents ne se gênent pas pour réaliser ce type d'actes ? Plus largement, dans un monde où les États et les multinationales utilisent les réseaux pour se procurer illégalement (ou a-légalement, comme disent certains Bretons) des informations ?
=> principe de réciprocité qui existe en droit international [Virally, 1967][Lagarde,].

Je vais brièvement vous parler du droit international et des questions qu'il faudra résoudre dans ce domaine, pour vous présenter ensuite la position du droit privé français, pénal et civil.

Le droit international

Entre États

Les réseaux sont communs à plusieurs États.

Par traités internationaux

Les États sont liés par des règles de droit qu'ils ont acceptées.

Juridictions internationales

- Crées par Traité, pour sanctionner les violations du droit issu des traités. (par ex. la Cour pénale internationale)
- OU juge national, appliquant le droit international.

Certaines attaques passent par les réseaux, et concernent donc des situations internationales[Barat-Ginies, 2014], soit parce que attaquant et victime sont de nationalités différentes, ce qui impliquent leurs États respectifs, soit parce qu'un État est impliqué dans l'attaque. De façon très sommaire, disons que la particularité du droit international public est qu'il a pour sujet de droit les États, et que ces sujets de droit ne sont liés que par leur consentement, leur volonté, leur acceptation. Ce consentement prend le plus souvent la forme d'accords formels, les traités internationaux.
Ces traités sont parfois mis en ?uvre par des juridictions internationales, elles aussi créées par traité international. La compétence de ces juridictions est donc le résultat de leur acceptation par l'État. Certains États refusent la compétence de telle ou telle juridiction internationale, de sorte que celle-ci n'a pas le pouvoir de les juger.
L'exemple le plus parlant est la Cour pénale internationale, créée par le Traité de Rome (signé le 17 juillet 1998 par 120 pays, ratifié par 60) pour juger les crimes contre l'humanité. La Cour n'a compétence pour juger un individu que

- l'accusé est un ressortissant d'un État partie ou d'un État qui a autrement accepté la compétence de la Cour.
- Le crime a été commis sur le territoire d'un État partie ou d'un État qui a autrement accepté la compétence de la Cour ; ou
- Le Conseil de sécurité de l'ONU a déféré la situation au Procureur, quels que soient la nationalité de l'accusé ou le lieu où le crime a été commis.

Certains de ces traités confèrent des droits aux individus, notamment ceux qui garantissent les droits fondamentaux. Parmi ces droits figure celui de saisir la juridiction internationale d'un recours.

Le Manuel de Tallin

Légitime défense en droit international

Une opération cyber constitue un emploi de la force quand son niveau (degré/seuil d'intensité) et ses effets sont comparables à une opération traditionnelle (non cyber) qui aurait atteint le niveau de l'emploi de la force

Cas d'attaque informatique réelle

APT1 : Exposing One of China's Cyber Espionage Units (http ://intelreport.mandiant.com/)

Légitime défense en droit international

Une opération cyber constitue un emploi de la force quand son niveau (degré/seuil d'intensité) et ses effets sont comparables à une opération traditionnelle (non cyber) qui aurait atteint le niveau de l'emploi de la force

Cas d'attaque informatique réelle

APT1 : Exposing One of China's Cyber Espionage Units (http ://intelreport.mandiant.com/)

Publié en 2013 et rédigé par le centre de recherche de l'OTAN, ce document conclut à l'applicabilité du droit international de la guerre aux cyberattaques, en apportant quelques précisions[Libicki, 2014][Kempf, b][Kempf, a][Randretsa, 2014]. Mais l'applicabilité du droit aux réseaux est une évidence, tant en droit privé qu'en droit public. Le problème n'est pas d'avoir des règles, mais de les faire appliquer.
Il est plutôt évident que si une cyberattaque a les effets d'une attaque "classique", elle doit alors entraîner les mêmes conséquences, et notamment le droit pour les États de riposter. ça ne règle donc pas la question de la riposte à une collecte ou à la destruction d'informations.
Plus clairement dit, ça ne règle pas le problème des opérations de renseignement ou d'espionnage économique, menées par des États, et ciblant les entreprises et institutions d'autres États.

De façon plus générale, vu la propension des États-Unis à éluder au maximum les textes internationaux qui pourraient les gêner, voir l'OTAN, qui est largement sous leadership américain, prôner l'applicabilité du droit international, ça évoque un peu la Vierge Marie donnant un cours de kamasutra.

Les droits fondamentaux

Droits reconnus à l'individu, en général à l'encontre de l'État, visant à protéger la dignité de la personne humaine, son essence. Ici :

- Droit à la vie privée (+ données personnelles)
- Droit au recours

Droits reconnus à l'individu, en général à l'encontre de l'État, visant à protéger la dignité de la personne humaine, son essence. Ici :

- Droit à la vie privée (+ données personnelles)
- Droit au recours

Les droits fondamentaux sont garantis aux individus à l'encontre des États. Le problème est leur justiciabilité, tous les traités ne sont pas sanctionnés devant une juridiction internationale, tous ces droits ne sont pas directement applicables devant le juge national.

Les droits fondamentaux sont ici essentiellement le droit à la vie privée et à la protection des données personnelles

droit pénal

Dès que les 3 éléments d'une infraction pénale sont réunis (légal, matériel, intentionnel), le droit pénal joue. Indifférence du mobile. Sanction pénale. Poursuite pénale indépendamment d'une plainte de la victime.

droit civil

Droit des relations entre personnes privées. Responsabilité civile. Sanction civile (dommages-intérêts et/ou réparation en nature)

La règle du boomerang

Le droit privé

droit pénal

Dès que les 3 éléments d'une infraction pénale sont réunis (légal, matériel, intentionnel), le droit pénal joue. Indifférence du mobile. Sanction pénale. Poursuite pénale indépendamment d'une plainte de la victime.

droit civil

Droit des relations entre personnes privées. Responsabilité civile. Sanction civile (dommages-intérêts et/ou réparation en nature)

Si une entreprise réplique à une attaque informatique, il faut envisager le droit pénal et le droit civil pour déterminer la responsabilité éventuellement encourue.

Le droit pénal d'un État a vocation à s'appliquer, soit parce que l'auteur de l'infraction est l'un de ses ressortissants, soit parce que la victime de l'attaque est l'un de ses ressortissants, soit parce que le lieu d'origine de l'attaque ou sa cible se trouve sur son territoire. (Critères de la Drective 2013/40/UE du 12 aout 2013 relative aux attaques contre les systèmes d'information, entrée en vigueur le 4 septembre 2015[201,]).

Le droit pénal se caractérise notamment par le fait que les poursuites sont menées par l'État, indépendamment de la plainte d'une victime.

Droit pénal

Faits justificatifs

En présence d'une infraction pénale constituée, l'auteur est excusé, sa responsabilité pénale est amoindrie ou disparait totalement.

- Légitime défense
- État de nécessité

Faits justificatifs

En présence d'une infraction pénale constituée, l'auteur est excusé, sa responsabilité pénale est amoindrie ou disparait totalement.

- Légitime défense
- État de nécessité

Précisons que ces deux notions existent dans beaucoup de droit européens. Mais si un droit pénal de l'un des État membre de l'UE n'admet pas ces faits justificatifs, le fait que le droit français admette cette excuse ne rend pas cela opposable aux autorités de cet autre État membre, à qui sont droit pénal permettrait de poursuivre une infraction commise sur les réseaux.
La légitime défense se définit comme "l'état de celui qui, sous le coup de la nécessité de protéger sa personne ou celle d'autrui, ou même ses biens, contre une agression injuste (actuelle ou imminente) commet lui-même un acte interdit par la loi pénale, situation qui vaut pour lui fait justificatif, si du moins l'intensité de sa riposte est proportionnée à la gravité de l'atteinte" (CORNU, Vocabulaire Juridique)[Bernardini, 2014].
"Réaction justifiée à une agression injustifiée" (Lexique des termes juridiques)
Le problème qui se pose est de déterminer avec exactitude l'attaquant, la légitime défense ne peut pas jouer pour justifier une "erreur" de cible. Dans ce cas, la victime devient agresseur elle-même et engage sa responsabilité.
Or, si une intrusion de longue date peut laisser supposer qu'il sera facile d'identifier avec précision son auteur, il n'en va pas de même en cas d'attaque de type DoS par exemple ou d'un piratage unique.

Proportionnalité

Le juge apprécie la proportionnalité entre l'infraction commise et l'infraction subie (ou qui devait l'être).

Cass. Crim. 6 décembre 1995, nř95-80075

Dans un bar, une femme est attrapé par un ivrogne et se défend d'un coup de talon aiguille ; elle lui a causé une contusion crânienne ayant entraîné une lésion du nerf optique de l' ?il gauche. Les juges du fond et la Cour de cassation estiment que c'était disproportionné (d'autant que la dame était accompagnée de proches susceptibles d'intervenir).

Proportionnalité

Le juge apprécie la proportionnalité entre l'infraction commise et l'infraction subie (ou qui devait l'être).

Cass. Crim. 6 décembre 1995, nr95-80075

Dans un bar, une femme est attrapé par un ivrogne et se défend d'un coup de talon aiguille ; elle lui a causé une contusion crânienne ayant entraîné une lésion du nerf optique de l' ?il gauche. Les juges du fond et la Cour de cassation estiment que c'était disproportionné (d'autant que la dame était accompagnée de proches susceptibles d'intervenir).

En admettant qu'on ait correctement identifié l'attaquant, la grande difficulté va être de doser la riposte. Il faut déjà qu'il s'agisse d'une attaque particulièrement violente pour justifier une réplique. Une "simple" collecte d'informations ne suffira pas à justifier une riposte. Et dès que la riposte n'est plus proportionnée à l'attaque, il n'y a plus d'excuse de légitime défense.

L'état de nécessité

Le joker

"Situation dans laquelle se trouve une personne qui ne peut raisonnablement sauver un bien, un intérêt ou un droit que par la commission d'une acte qui, s'il était détaché des circonstances qui l'entourent, serait délictueux" FORIERS, thèse, Bruxelles, 1951, numéro 9.

Le joker

"Situation dans laquelle se trouve une personne qui ne peut raisonnablement sauver un bien, un intérêt ou un droit que par la commission d'une acte qui, s'il était détaché des circonstances qui l'entourent, serait délictueux" FORIERS, thèse, Bruxelles, 1951, numéro 9.

Ce fait justificatif figure à l'article 122-7 du Code pénal : "n'est pas pénalement responsable la personne qui, face à un danger actuel ou imminent qui menace elle-même, autrui ou un bien, accomplit un acte nécessaire à la sauvegarde de la personne ou du bien, sauf s'il y a disproportion entre les moyens employés et la gravité de la menace"[Danti-Juan, 2015]. Le problème va être de déterminer quels sont les droits ou biens dignes de protection contre une atteinte grave.
Par exemple, si le site internet d'une conférence de sécurité informatique comporte une faille évidente, dont l'exploitation permet d'accéder aux données personnelles de tous les participants enregistrés, la protection de ces informations justifie-t-elle de tester la sécurité du site en question ? (pour moi oui, parce que c'est le seul moyen d'en avoir le c ?ur net, sauf à accorder une aveugle aux prestataires informatiques). Mais il s'agit d'interprétation, et par ailleurs, la collecte sauvage de données personnelles est une infraction pénale, mais qui est finalement assez peu sanctionnée.
Peut-être que l'affirmation du droit à la vie privée, et son renforcement pour lutter contre les immixtion croissante de l'État conduira à admettre qu'une action dans le but de protéger ce droit est nécessaire. Par ailleurs, en admettant qu'un État veuille s'engager dans cette voie, cela ne règlera pas le problème des sanctions pénales encourues dans les pays où est localisé l'agresseur devenu victime. En effet, le droit pénal français ne s'applique qu'en France.

Le jeu de faits justificatifs peut aussi faire disparaitre l'obligation de réparer le dommage causé (légitime

défense).

L'enjeu : la protection des individus

La question de la riposte, de sa légalité, etc. ne devrait même pas se poser. Dès le moment où tous les États et un nombre toujours plus grand d'individus, personnes physiques comme entreprises, sont susceptibles de se livrer à des actes de piratage informatique à des fins de guerre économique notamment, l'avantage concurrentiel qui pouvait en découler disparait et il ne reste que le "léger" problème de l'atteinte à la vie privée des individus.

Le seul moyen de sortir de ce problème est sans doute celui qui s'est imposé en matière nucléaire, des traités internationaux, qui s'imposent à tous les États, et qui offrent aux individus des instances pour obtenir justice à l'encontre des États-voyous, y compris nos démocraties occidentales, dont les turpitudes ont été mises à jour par Edward Snowden.

Remerciements

- à Donald Knuth et Till Tantau
- à Raphael Vinot et Stéphane Emma
- aux organisateurs de cet événement.

Réalisé avec <3 et LaTeX

Questions

- légitime défense préventive ?
- fabrication d'outil d'attaque ?
- l'auditoire est essentiellement composé de forces de l'ordre qui enquêtent (i. e. qui ne sont pas en mesure de répliquer)

Si vous avez d'autres questions : eve.matringe@barreau.lu

Questions

- légitime défense préventive ?
- fabrication d'outil d'attaque ?
- l'auditoire est essentiellement composé de forces de l'ordre qui enquêtent (i. e. qui ne sont pas en mesure de répliquer)

Si vous avez d'autres questions : eve.matringe@barreau.lu

- La notion de légitime défense comme celle d'état de nécessité envisagent l'action a priori aux fins d'éviter un dommage imminent. Le problème sera toujours de parvenir à démontrer et à vérifier ensuite l'opportunité et la proportionnalité de la réaction.

- A l'heure actuelle, en ce qui concerne les États de l'Union, la directive 2013/40/UE vise en son article 7 « Outils utilisés pour commettre les infractions
  Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition intentionnelles d'un des outils suivants lorsque l'acte est commis sans droit et dans l'intention de l'utiliser pour commettre l'une des infractions visées aux articles 3 à 6, au moins lorsqu'il ne s'agit pas de cas mineurs :
  a) un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées aux articles 3 à 6 ; (...) ».

  S'agissant des autres États, ils peuvent avoir ratifié la Convention sur la cybercriminalité de Budapest du 23 novembre 2001[Bud,], dont l'article 6 vise le même problème. Toutefois, ce texte n'a pas été ratifié par la Russie et la Chine notamment [Maitra, 2015].

- La capacité de réponse et la légalité de la réponse sont deux questions différentes. Mon avis est que l'État a l'obligation positive de prendre les mesures nécessaires pour protéger le droit fondamental de ses ressortissants à la vie privée et à la protection des données personnelles. Qu'il ne l'ait pas encore fait expose l'État à de potentielles actions en responsabilité en raison de son inaction. Que certains individus aient choisi de répliquer montre que c'est possible. Il s'agit donc, à mon avis, d'une voie à explorer.

Pour aller plus loin I

(sans approbation des auteurs cités, il s'agit seulement de présenter quelques éléments de doctrine sur les questions évoquées dans cette présentation)


Convention sur la cybercriminalité de budapest du 23 novembre 2001.


Directive 2013/40/ue du 12 août 2013 relative aux attaques contre les systèmes d'information.


Barat-Ginies, O. (2014).
Existe-t-il un droit international du cyberespace ?
Hérodote, 1 :201–220.


Bernardini, R. (2014).
Légitime défense.
In Dalloz, editor, *Encyclopédie Dalloz de droit pénal*. Dalloz.


Danti-Juan, M. (2015).
Etat de nécessité.
In Dalloz, editor, *Encyclopédie Dalloz de droit pénal*. Dalloz.


Kempf, O.
Le manuel de tallin.

Pour aller plus loin II


Kempf, O.
L'otan et la cybersécurité.


Lagarde, P.
La réciprocité en droit international privé, volume 154, chapter La Réciprocité-Rétorsion, pages 124–175.
The Hague Academy of International Law, Leiden, Boston,.


Libicki, M. C. (2014).
De tallinn à las vegas, une cyberattaque d'importance justifie-t-elle une réponse cinétique ?
Hérodote, 1 :221–239.


Maitra, A. K. (2015).
Offensive cyber-weapons : technical, legal, and strategic aspects.
Environ Syst Decis, 35 :169–182.


Randretsa, T. (10/09/2014).
Légitime défense et cyberattaque à la lumière du manuel de tallinn.

Pour aller plus loin III

Virally, M. (1967).

Le principe de réciprocité dans le droit international contemporain, volume 122 of *Collected Courses of the Hague Academy of International Law*, chapter La réciprocité : principe général du droit international ?

The Hague Academy of International Law, Leiden, Boston.