diploweb.com La revue géopolitique
ISSN : 2111-4307

L’attribution publique des cyberattaques comme stratégie diplomatique défensive

mardi 29 avril 2025,par Pascal MARTIN

Citer cet article / To cite this version :
Pascal MARTIN, **L’attribution publique des cyberattaques comme stratégie diplomatique défensive**, *Diploweb.com : la revue géopolitique, 29 avril 2025.*

Les actions cyberoffensives, info-centrées et variées dans leur nature, peuvent être exploitées au profit d'une diplomatie coercitive selon deux approches distinctes, mais complémentaires : offensivement, à travers des opérations cyberclandestines mises en œuvre par les services de renseignement, leurs proxies ou des structures vassalisées mais démarquées ; ou défensivement, en procédant à l'attribution officielle d'une action cyberoffensive selon les enjeux politiques, conjoncturels ou non, en s'appuyant sur l'analyse techno-centrée réalisée avec l'appui des services de renseignement.

Initialement publié par Diploweb le 17 mars 2025, nous remettons cet article de grande qualité en Une dans un contexte exceptionnel. En effet, le 29 avril 2025, la France attribue pour la première fois officiellement des cyberattaques répétées à la Russie.
Deux bonus : vous trouverez en pied de page le communiqué du Ministère de l'Europe et des Affaires étrangères (Russie – Attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28) (29 avril 2025)) ; et le lien vers le Rapport menaces et incidents du CERT-FR.

L'ESPACE CYBERNETIQUE est devenu un milieu à part entière de conduite des relations internationales ou des conflits : l'emploi de capacités cyberoffensives par des acteurs étatiques pour parvenir à des avantages politico-stratégiques [1] est désormais une constante des relations internationales [2], conduisant à de nouvelles réflexions sur les questions liées à la sécurité collective. L'emploi d'un large spectre de modes opératoires info-centrés à des fins offensives, utilisant le cyberespace comme vecteur, nourrit une instabilité croissante. **Les États exploitent ces capacités asymétriques à des fins coercitives**, au profit d'enjeux géopolitiques, dans le cadre d'une stratégie d'usure pouvant aboutir à une fragilisation du tissu économique et social, de la légitimité des autorités politiques et des institutions, ainsi qu'à une polarisation des opinions dans le cadre d'une « guerre cognitive » [3].

Cette stratégie de « zone grise », s'affranchissant des normes internationales, cumulée aux caractéristiques du cyberespace et aux capacités d'actions cyberoffensives des services de renseignement, brouille les concepts de la conflictualité interétatique. Désormais, la pénétration des réseaux adverses a intégré le spectre des outils tactiques à la disposition de l'État [4]. L'intensification des attaques informatiques depuis le début du XXIème siècle tend donc à appréhender le cyber comme un nouveau moyen d'expression de la volonté des États : un nouvel outil au profit de leur diplomatie à travers un prisme coercitif. Cette évolution replace les services comme des acteurs à part entière des relations entre États [5] et rappelle, selon la conception de Michael Herman [6], que « *la diplomatie et le renseignement sont à la fois des concurrents et des collaborateurs* [7]. »

Pascal Martin

1. L’action cyberoffensive exploitée à des fins diplomatiques et politiques

En 1999, Qiao Liang et Wang Xiangsui considéraient que les actions offensives en informatique s’inscrivent dans la catégorie des attaques qui ont pour but d’obliger un autre État à satisfaire ses propres intérêts et exigences [8]. En effet, les potentialités du numérique inviteraient les autorités politiques à privilégier l’action cyberoffensive, plutôt qu’une solution purement politique [9]. Ce constat s’appuie sur les opportunités offertes par l’espace numérique, qui permettent d’éviter les contraintes et conséquences liées au recours à la force armée conventionnelle : consécutivement à l’attaque de l’Ukraine par la Russie, le président Joe Biden a ainsi publiquement menacé la Russie de subir des cyberattaques massives [10]. **Le cyber est devenu un substitut possible à une confrontation armée conventionnelle** dans les rapports de forces interétatiques et s’inscrit donc dans le cadre d’une stratégie de diplomatie coercitive. Les services de renseignement peuvent, à travers leurs actions cyberoffensives, pleinement œuvrer au profit de celle-ci. En effet, le renseignement « *concourt pleinement à l’exercice de la diplomatie* [11] », et tous les pays disposant de services de renseignement avec d’importantes capacités, y compris techniques, s’appuient sur eux pour **obtenir un avantage, que ce soit à l’approche de négociations internationales ou sur le champ de bataille** [12]. Cette porosité institutionnelle est soulignée par le Ministère des affaires étrangères en 2008 qui mentionne l’appui que peut utilement apporter le renseignement à la diplomatie [13].

La diversité des actions offensives possibles, renforcée par les difficultés d’attribution, accroît la marge de manœuvre des États en mettant en œuvre une stratégie d’usure des adversaires géopolitiques. En effet, les opérations peuvent avoir des conséquences économiques et politiques non-négligeables (comme l’arrêt d’une activité industrielle ou d’un service, ou l’atteinte à la réputation d’une organisation, tandis qu’une importante augmentation des cyberattaques contre les infrastructures critiques est constatée [14]), permettre le vol de

données à haute valeur ajoutée dans le domaine industriel, scientifique ou politique (pour exploitation ou diffusion massive dans le cadre de *leaks* [15]), et enfin, sont destinées à influencer le comportement des individus [16] (comme lors de processus électoraux). La combinaison de l'ensemble de ces capacités s'inscrit dans une stratégie globale décrite par les stratèges américains comme une « approche gouvernementale globale », dans laquelle tous les pouvoirs et capacités relevant d'une autorité étatique travaillent de manière coordonnée, en s'affranchissant des contraintes bureaucratiques, pour atteindre un objectif commun [17]. Cette stratégie serait notamment mise en œuvre par la Russie [18], dont les actions clandestines s'insèrent dans une stratégie globale d'usure, qui comprend donc un ensemble d'actions complémentaires, dont **l'infiltration des cercles de décision politique** [19].

Considérant les coûts et les risques d'escalade qui résulteraient d'un conflit ouvert avec d'autres États, le diplomate du département d'État américain George Kennan considérait que la conflictualité sera non conventionnelle selon sa conception du « *political warfare* ». Cette dernière prévoit l'emploi de moyens, dont le renseignement, les capacitaires militaires, diplomatiques et financières, pour atteindre des objectifs nationaux, y compris par l'emploi d'opérations secrètes. Dans ce cadre, George Kennan a encouragé les dirigeants américains à se débarrasser de la doctrine opérant une distinction fondamentale entre la paix et la guerre, afin d'intégrer la réalité des relations internationales, basée sur un rythme perpétuel de lutte (« *perpetual rhythm of struggle* ») [20]. Ces considérations sont d'autant plus pertinentes dans le cyberespace en raison de la désinhibition face à l'emploi de la force [21].

In fine, l'emploi offensif des capacités numériques est reconnu par les hautes sphères politiques comme une tactique géopolitique, tandis que **le cyberespace est désormais appréhendé comme une arme géopolitique** [22]. En effet, au niveau mondial la numérisation bouleverse les anciennes normes et traditions diplomatiques, notamment en raison du nombre croissant d'acteurs non-gouvernementaux opérant dans cet espace, y compris avec des moyens et des infrastructures limités, tandis que les États sont désormais conscients de leur propre vulnérabilité face aux cyberattaques et manipulations de l'information [23]. Si le gain potentiel de chaque opération cybernétique peut être indépendant, ces actions s'inscrivent bien souvent dans une stratégie globale permettant de contraindre un adversaire géopolitique et de modifier la marge de négociation entre les États [24]. Dans ce cadre, **le développement et l'emploi des cybercapacités des services de renseignement en ont fait des acteurs internationaux de premier plan**, où leur action s'appuie sur une tolérance tacite commune, mais ne pouvant faire l'objet d'une revendication officielle.

En effet, les divergences entre les pratiques réelles des services de renseignement et les positions officielles des gouvernements ne sont pas inhabituelles [25], mais trouvent un nouveau renforcement dans l'espace cybernétique.

Si les États peuvent employer les actions cyberoffensives, selon plusieurs *modus operandi* afin d'exercer une contrainte et une stratégie usure à l'encontre d'adversaires géopolitiques, l'attribution d'une attaque informatique peut également servir d'outil de rétorsion diplomatique dans le cadre d'une posture défensive [26].

2. L’attribution des opérations cyberoffensives comme outil de rétorsion diplomatique

Les cyberattaques se caractérisent par leur irrégularité [27], à l’accessibilité des armes numériques et à la difficulté d’identifier les assaillants [28]. Ces facteurs font de **l’attribution des attaques informatiques un enjeu majeur des doctrines de défense des États** depuis qu’elles ont atteint un degré d’intensité suffisamment important pour avoir des conséquences stratégiques ou, plus largement, nuire à leurs intérêts [29]. Dans ce cadre, l’attribution peut être considérée comme un outil contribuant à créer un cyberespace plus stable [30].

Les rapports parlementaires et études dans le domaine cyber s’accordent pour considérer que l’attribution d’une attaque informatique est « *particulièrement difficile* [31] », **mais pas impossible**. Outre les caractéristiques des réseaux et les techniques de dissimulation mises en œuvre par les attaquants, l’attribution est complexifiée en raison d’un environnement informationnel fortement contesté, conduisant certains auteurs à estimer qu’il faudrait que les acteurs civils, y compris universitaires, participent davantage au processus d’attribution dans une logique d’efficacité [32]. Si le cyberespace contraint fortement l’identification formelle de l’adversaire, l’anonymat n’y est pas absolu puisque le nombre de cas où une cyberattaque peut être attribuée avec une certitude absolue est quasiment nul, mais le nombre de cas où il est totalement impossible de déterminer qui est à l’origine de l’attaque est quasiment nul également [33]. En conséquence, **une cyberattaque peut être imputable d’un point de vue technique, sans être pour autant attribuable officiellement par un État**.

Le processus d’imputation d’une attaque informatique vise donc à préciser l’auteur d’une cyberattaque par des preuves ou un faisceau d’indices. Tandis que la décision d’attribution appartient aux plus hauts responsables politiques [34]. En effet, si le numérique permet à un État d’augmenter sa capacité à **nier de manière plausible** être à l’origine d’une action cyberoffensive, la difficulté d’attribution ne repose pas exclusivement sur des constantes techniques, mais relève également de plusieurs variables contextuelles [35]. Au-delà de cette approche techno-centrée de l’imputation, **la décision d’attribuer une cyberattaque relève d’une appréciation et donc d’une décision de nature politique** [36]. Il convient également d’analyser les motivations de l’attaquant. En effet, l’attribution ne repose que rarement sur des certitudes absolues et des preuves formelles : une telle décision s’appuie sur un niveau suffisamment bas d’incertitudes et sur un faisceau d’indices permettant à l’autorité politique, le cas échéant, de prendre la responsabilité d’attribuer un acte [37], car l’attribution revient à désigner officiellement l’agresseur sur la scène internationale. Dans ce cadre, elle peut être considérée comme réussie dès lors qu’elle permet d’atteindre les objectifs visés par un gouvernement [38].

Dmitri Alperovitch, cofondateur de l’entreprise de cybersécurité Crowdstrike, estime que l’identification technique des responsables des cyberattaques est un problème largement résolu. Cependant, **déterminer** ce qu’il convient de faire dans le cadre d’une attribution publique reste une question en suspens car chaque État appréhende les situations selon ses propres intérêts, ce qui suppose une doctrine flexible [39]. Ainsi, en fonction des enjeux politiques conjoncturels et des approches distinctes des autorités, des doctrines très disparates peuvent être observées. Aux États-Unis, par exemple, deux présidents successifs ont adopté des stratégies différentes : si Barack Obama avait fait preuve d’une relative retenue, Donald

Trump a multiplié durant son premier mandat les attributions, en permettant notamment la judiciarisation et l'inculpation en 2018 de douze officiers de renseignement russes et la mise en œuvre de sanctions économiques [40]. La France dispose-t-elle d'une doctrine dans le domaine de l'attribution des attaques informatiques ? Un mimétisme doctrinal peut-il être observé en la matière ?

La France évite les attributions officielles des actions cyberoffensives. La délégation parlementaire au renseignement (DPR) mentionne que cette conception repose sur la volonté de conserver un dialogue stratégique et opérationnel avec les homologues étrangers, y compris ceux susceptibles d'être à l'origine de cyberattaques visant la France [41]. Le but serait de conserver une liberté absolue d'appréciation dans le processus d'attribution [42], évitant donc qu'une doctrine prédéfinie en la matière ne vienne rigidifier et figer les processus d'analyse, ainsi qu'automatiser les schémas de réaction : **chaque situation est donc analysée isolément** en fonction du contexte stratégique et des enjeux conjoncturels [43]. Cependant, en 2018, Louis Gautier estimait qu'une doctrine officielle, mais demeurant confidentielle, devrait être établie, car l'attribution permet à l'État désignant officiellement l'attaquant de se trouver en posture de supériorité, y compris s'il agit à des fins purement politiques [44].

L'OTAN dispose ainsi d'un mécanisme d'attribution publique des cyberattaques où l'intérêt est de « pointer du doigt » et de considérer que le *name and shame*, ou le *name and blame*, vont permettre de stopper les attaques, malgré les potentielles limites en termes d'efficacité car certains attaquants vont nier et demander des preuves de leur responsabilité [45]. En outre, il convient de préciser qu'**apporter des éléments de preuve revient à dévoiler une partie des capacités techniques et savoir-faire des services en matière d'attribution**, tout comme les éventuels partenariats avec des services étrangers, et donc, à « *se fragiliser* [46]. » C'est donc l'ensemble de ces facteurs qui vient en partie structurer la décision politique et qui doit être pris en considération afin de prendre la décision adaptée à la préservation des intérêts nationaux sur la scène internationale.

In fine, plus que la dimension technique, **l'attribution d'une attaque informatique est un enjeu d'ordre politique** [47] qui s'insère dans les rivalités et rapports de force interétatiques. Elle autorise la poursuite de plusieurs objectifs, dont la légitimation, par l'État ciblé, de l'application de mesures de rétorsions, y compris des menaces ou l'imposition de sanctions économiques ou diplomatiques (comme l'expulsion de diplomates) : elle a donc une visée coercitive [48]. Cependant, l'attribution peut poursuivre d'autres objectifs [49] tels que :la clarification et l'application d'un ensemble de normes concernant le comportement des acteurs, étatiques ou non, dans le cyberespace ; contraindre l'adversaire à consacrer un temps et des ressources importants pour le développement de ses capacités afin de ne pas être identifié (même si l'attribution ne semble pas décourager un comportement similaire des attaquants à l'avenir [50]) ; permettre le renforcement de la prévention et de la défense par une diffusion d'informations portant sur les menaces potentielles, permettant ainsi d'apporter rapidement des correctifs aux réseaux ciblés et d'accroître leur résilience ;permettre la construction d'une communauté basée sur un partage d'information entre les différents acteurs concourant à l'attribution, dans le but d'**envoyer un signal politique** basé sur une vision partagée des menaces cyber, qui pourrait servir de point de départ pour construire une capacité plus importante d'attribution ; enfin, l'attribution peut servir à renforcer la légitimité et la crédibilité internes et internationales des acteurs participant au processus d'attribution, en démontrant leur savoir-faire et leurs capacités publiquement.

Dans le cadre de la politique interne, l'attribution permet d'aider la justification de l'allocation de budgets aux administrations chargées de cette mission [51]. En outre, l'aspect coercitif de l'attribution peut s'exercer à travers une posture de déception des intentions adverses : l'attaquant peut, par l'évaluation du rapport coût-bénéfice et l'adoption une approche rationnelle, modifier son comportement par la crainte d'une délégitimation sur la scène internationale [52].

*

In fine, les actions cyberoffensives, info-centrées et variées dans leur nature, peuvent être exploitées au profit d'une diplomatie coercitive selon deux approches distinctes, mais complémentaires : offensivement, à travers des opérations cyberclandestines mises en œuvre par les services de renseignement, leurs proxies ou des structures vassalisées mais démarquées ; ou défensivement, en procédant à l'attribution officielle d'une action cyberoffensive selon les enjeux politiques, conjoncturels ou non, en s'appuyant sur l'analyse techno-centrée réalisée avec l'appui des services de renseignement. Les États, qui adhèrent pleinement à ce *modus vivendi* [53],continueront à exploiter le cyber comme moyen d'expression de leur volonté, à travers du sabotage, de l'espionnage et des opérations de déstabilisation.

Ajout le 29 avril 2025

Source : Ministère de l'Europe et des Affaires étrangères :

Russie – Attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28) (29 avril 2025)

"La France condamne avec la plus grande fermeté le recours par le service de renseignement militaire russe (GRU) au mode opératoire d'attaque APT28, à l'origine de plusieurs cyber-attaques contre des intérêts français.

Depuis 2021, ce mode opératoire d'attaque (MOA) a été utilisé dans le ciblage ou la compromission d'une dizaine d'entités françaises. Ces entités sont des acteurs de la vie des Français : services publics, entreprises privées, ainsi qu'une organisation sportive liée à l'organisation des Jeux olympiques et paralympiques 2024. Par le passé, ce mode opératoire a également été utilisé par le GRU dans le sabotage de la chaîne de télévision TV5Monde en 2015, ainsi que dans la tentative de déstabilisation du processus électoral français en 2017.

APT28 est aussi employé pour exercer une pression constante sur les infrastructures ukrainiennes dans le contexte de la guerre d'agression menée par la Russie contre l'Ukraine, notamment lorsqu'il est opéré par l'unité 20728 du GRU. De nombreux partenaires européens ont également été visés par APT28 au cours des dernières années. À ce titre, l'UE a imposé des

sanctions aux personnes et entités responsables des attaques menées à l'aide de ce mode opératoire.

Ces activités déstabilisatrices sont inacceptables et indignes d'un membre permanent du Conseil de sécurité des Nations unies. Elles sont par ailleurs contraires aux normes des Nations unies en matière de comportement responsable des États dans le cyberespace, auxquelles la Russie a souscrit.

Aux côtés de ses partenaires, la France est résolue à employer l'ensemble des moyens à sa disposition pour anticiper les comportements malveillants de la Russie dans le cyberespace, les décourager et y réagir le cas échéant.

L'Agence nationale de sécurité des systèmes d'information publie ce jour un rapport alertant sur la menace liée à APT28 dans le but de prévenir de futures attaques : https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-006/ "

Télécharger le Rapport menaces et incidents du CERT-FR

L'ANSSI et ses partenaires du Centre de coordination des crises cyber (C4) ont observé entre 2021 et 2024 des attaques informatiques conduites par les opérateurs d'APT28, qui sont publiquement rattachés par différentes sources à la Russie. Le mode opératoire d'attaque APT28 a été utilisé contre de nombreuses entités en France, en Europe, en Ukraine et en Amérique du Nord, afin de collecter des renseignements. En 2024, la victimologie française des campagnes associées à APT28 comprend des entités des secteurs gouvernemental, diplomatique et de la recherche. Les investigations menées par l'ANSSI et ses partenaires du C4 ont permis d'identifier plusieurs chaîne d'infection, présentées dans le document. Ces attaques se poursuivent dans le contexte de la guerre d'agression déclenchée par la Russie contre l'Ukraine depuis le 24 février 2022.

URL du rapport : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-006.pdf

---

P.-S.

L'auteur s'exprime à titre personnel. Officier de la gendarmerie nationale, Pascal Martin est chef d'un département d'investigation au sein de l'unité cyber de la gendarmerie nationale (UNC). Il est diplômé de l'École des officiers de la gendarmerie nationale (2018), d'un master 2 de droit de l'université Paris Panthéon-Assas (2018), d'un diplôme universitaire en cybercriminalité de la Guardia Civil espagnole (2022) et d'un doctorat en histoire contemporaine de l'université de Bordeaux (2022). Sa thèse, primée par l'Association pour les études sur la guerre et la stratégie (AEGES) en 2023, porte sur le renseignement en France face au cyberespace et aux nouvelles technologies de l'information et de la communication (NTIC). Chercheur associé au Centre de recherche de la gendarmerie nationale (CRGN) et à l'Institut de recherche stratégique de l'École militaire (IRSEM) ses publications portent sur les problématiques cyber, le renseignement et les manipulations de l'information.

Notes

[1] BUCHANAN Ben, « The Hacker and the State. Cyber Attacks and the New Normal of

Geopolitics », *op. cit.* , 413 p.

[2] LACHAUD Bastien, VALETTA-ARDISSON Alexandra, Rapport d'information sur la cyberdéfense, 2018, *op. cit.,* p. 15

[3] PREBOT Baptiste, CLAVERIE Bernard, DU CLUZEL François, « Cognitive Warfare – La guerre cognitive », Innovation Hub NATO, Neuilly, 2020, 116 p.

[4] BUCHANAN Ben, « The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics », *op. cit.* , p. 306

[5] FORCADE Olivier, LAURENT Sébastien-Yves, « Secrets d'État – Pouvoirs et renseignement dans le monde contemporain », Paris, Armand et Colin, 2005, p. 149

[6] Anime depuis plusieurs années l'*Oxford Intelligence Group* de Nuffield College à l'Université d'Oxford et qui a exercé pendant plus de 30 ans au GCHQ ainsi que comme secrétaire du *Joint Intelligence Committee*

[7] COUSSERAN Jean-Claude, HAYEZ Philippe, « Nouvelles leçons sur le Renseignement », *op. cit.*, p. 292

[8] LIANG Qiao, XIANGSUI Wang, « La guerre hors limites », *op. cit.*, p.169

[9] SALTZMAN Ilai, « Cyber Posturing and the Offense-Defense Balance », *op. cit.,* p. 43

[10] DILANIAN Ken Dilanian, KUBE Courtney, « Biden has been presented with options for massive cyberattacks against Russia », *NBC News*, 24 février 2022 – Source : https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558?s=09

[11] COUSSERAN Jean-Claude, HAYEZ Philippe, « Nouvelles leçons sur le Renseignement », *op. cit.,* p. 298

[12] GIOE David V., « Cyber operations and useful fools : the approach of Russian hybrid intelligence », Intelligence and National Security, volume 33 – issue 7, 2018, p. 954-973

[13] Ministère des affaires étrangères, « Livre blanc sur la politique étrangère et européenne de la France 2008-2020 », 2008, p. 67

[14] RUDNER Martin, « Cyber-Threats to Critical National Infrastructure : An Intelligence Challenge », *op. cit.*, p. 453-481

[15] PECH Yannick, « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », Prospective et stratégie, n° 10, 2019, p. 85

[16] CHARILLON Frédéric, « *Guerres d'influence. Les États à la conquête des esprits* », Paris, éditions Odile Jacob, 2022, p. 75

[17] GIOE David V., « Cyber operations and useful fools : the approach of Russian hybrid intelligence », *op. cit.,* p. 954-973

[18] *Ibid.*

[19] RIEHLE Kevin, « Russia's intelligence illegals program : an enduring asset », Intelligence and National Security, volume 35 – issue 3, 2020, p. 389

[20] JONES Seth G., « The Return of Political Warfare », International Security Program, Center for Strategic & International Studies, 2018, p. 4

[21] BUCHANAN Ben, « The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics », *op. cit.*, p. 319

[22] FRIPP Will, « The hacked world order : how nations fight, trade, maneuver, and manipulate in the digital age », *Intelligence and National Security*, volume 33 – issue 4, 2018, p. 623-626

[23] *Ibid.*

[24] BRANTLY F. Aaron, « Cyber Actions by State Actors : Motivation and Utility », *op. cit.,* p. 465-484

[25] GEORGIVA Ilina, « The unexpected norm-setters : Intelligence agencies in cyberspace », Contemporary Security Policy, volume 41 – issue 1, 2020, p. 33-54

[26] EGLOFF Florian J., SMEETS Max, « Publicly attributing cyber attacks : a framework », Journal of Strategic Studies, vol 46 – no 3, 2023, p. 502-533

[27] Délégation parlementaire au renseignement, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020, 2020, p. 252

[28] MOTTE Martin (dir.), SOUTOU Georges-Henri, DE LESPINOIS Jérôme, et al., « La mesure de la force – Traité de stratégie de l'École de guerre », Paris, éditions Tallendier, 2ème édition revue et corrigée, 2019, p. 349

[29] DESFORGES Alix, « Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France », thèse de géographie mention géopolitique, Université Paris 8, Vincennes-St-Denis, thèse dirigée par Frédérick Douzet, Professeure à l'Université Paris 8, 2018, p. 239-247

[30] EGLOFF Florian J., SMEETS Max, « Publicly attributing cyber attacks : a framework », *op. cit.*, p.502-533

[31] Commission de la défense nationale et des forces armées, Examen, ouvert à la presse, du rapport d'information sur la cyberdéfense (M. Bastien LACHAUD et Mme Alenxandra VALETTA-ARDISSON, rapporteurs), session ordinaire 2017-2018, compte-rendu n°69,

mercredi 04 juillet 2018, séance de 11 heures 30

[32] EGLOFF Florian J., « Contested public attributions of cyber incidents and the role of academia », *Contemporary Security Policy*, volume 41 – issue 1, 2020, p. 55-81

[33] LACHAUD Bastien, VALETTA-ARDISSON Alexandra, Rapport d'information sur la cyberdéfense, 2018, *op. cit.,* p. 27

[34] Délégation parlementaire au renseignement, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020, *op. cit.*, p. 248

[35] BUCHANAN Ben, RID Thomas, « Attributing Cyber Attacks », Journal of Strategic Studies, vol.38, n°1-2, 2015, p.4-37

[36] EGLOFF Florian J., SMEETS Max, « Publicly attributing cyber attacks : a framework », *op. cit.*, p. 502-533

[37] LACHAUD Bastien, VALETTA-ARDISSON Alexandra, Rapport d'information sur la cyberdéfense, 2018, *op. cit.,* p. 27

[38] EGLOFF Florian J., SMEETS Max, « Publicly attributing cyber attacks : a framework », *op. cit.*, p.502-533

[39] *Ibid.*

[40] VINCENT Élise, « Cybertensions entre les États-Unis, la Russie et la Chine », Le Monde, édition du lundi 15 mars 2021

[41] Délégation parlementaire au renseignement, Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020, *op. cit.*, p. 260

[42] Citée par Élise Vincent, « Cybertensions entre les États-Unis, la Russie et…, *op. cit.*

[43] Audition de M. Louis GAUTIER, secrétaire général de la défense et de la sécurité nationale, mercredi 21 février 2018, *op. cit.*

[44] *Ibid*.

[45] Audition du général de division aérienne Didier TISSEYRE, général commandant la cyber défense, mercredi 4 mars 2020, *op. cit.*

[46] *Ibid*.

[47] DESFORGES Alix, Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France, thèse de géographie mention géopolitique, *op. cit.*, p. 247

[48] BRANTLY Aaron F., « Cyber Actions by State Actors : Motivation and Utility », *op. cit.*, p. 465-484

[49] EGLOFF Florian J., SMEETS Max, « Publicly attributing cyber attacks : a framework », *op. cit.*, p.502-533

[50] *Ibid.*

[51] *Ibid.*, p. 510

[52] *Ibid.* p. 508-510

[53] BUCHANAN Ben, « The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics », *op. cit.*, p. 319