Thibault Moulin

Le cyber espionnage en droit international

Editions A. PEDONE

SOMMAIRE

INTRODUCTION

PREMIÈRE PARTIE
LES RÈGLES CONNECTÉES À L'INTÉGRITÉ TERRITORIALE

TITRE I.
LE DROIT DE LA COEXISTENCE PACIFIQUE

Chapitre 1. Le droit interdisant les atteintes à la souveraineté territoriale
Chapitre 2. Le droit de la sécurité collective

TITRE II.
LE DROIT RÉGISSANT LA CONDUITE DES HOSTILITÉS

Chapitre 1. Le droit applicable entre États belligérants
Chapitre 2. Le droit applicable entre États belligérants et États neutres

DEUXIÈME PARTIE
LES RÈGLES DÉCONNECTÉES DE L'INTÉGRITÉ TERRITORIALE

TITRE I.
LE DROIT DE LA COOPÉRATION

Chapitre 1. Le droit des relations diplomatiques
Chapitre 2. Le droit international économique

TITRE II.
LE DROIT DU RENSEIGNEMENT

Chapitre 1. Le droit national en matière d'espionnage
Chapitre 2. Un droit international coutumier spécifique à l'espionnage ?

CONCLUSION GÉNÉRALE

I.S.B.N. 978-2-233-00989-0

1. « *Oui, j'ai entendu parler de vous* », avoua Nikita Khrouchtchev à Allen Dulles, le directeur de la CIA, lors d'une rencontre organisée en septembre 1959[1] – « *je lis vos rapports* »[2]. Si pour les citoyens, l'espionnage peut apparaître comme une activité drapée de mystère, cette confession du Premier Secrétaire du Parti Communiste dévoile une toute autre réalité : au sommet de l'Etat, la possibilité d'être visé par des services de renseignement étrangers n'est un secret pour personne. D'ailleurs, et c'est là que réside tout le paradoxe de l'espionnage, la législation d'un Etat lui permet bien souvent d'acquérir des renseignements étrangers, mais aussi de punir quiconque viserait ses propres secrets. La devise de l'*Australian Signals Directorate* illustre à merveille cette inhérente contradiction : « *Révéler leurs Secrets – Protéger les Nôtres* »[3].

2. L'espionnage est loin d'être un phénomène récent, et a même été surnommé « la seconde plus ancienne profession au monde »[4]. Plus de 500 ans avant notre ère, le stratège chinois Sun Tzu recommandait déjà le recours à des espions[5], et Jules César mit sur pied une mission de reconnaissance avant d'envahir la Grande-Bretagne[6]. L'Angleterre, la France et la Russie se dotèrent d'organisations de renseignement dès la Renaissance[7], et certains espions ont marqué l'Histoire : Mata Hari, Richard Sorge, les époux Rosenberg, Kim Philby, Jonathan Pollard etc. Le recours à des espions apparaît même dans la Bible et l'Iliade ! Toutefois, le visage du renseignement a connu des changements significatifs depuis l'émergence d'internet, et cette « dématérialisation » présente de nombreux avantages pour les Etats. Le cyber-espionnage ne nécessite ainsi ni l'envoi ou le recrutement d'un agent en territoire étranger, ni le recours à un important dispositif matériel. Cela permet en premier lieu de réduire les risques, tant pour l'agent que pour l'Etat

[1] LATHROP (C.), *The Literary Spy,* New Haven, Yale University Press, p. 50 [nous traduisons].
[2] *Ibid*.
[3] Soit, dans la version originale : « *Reveal Their Secrets – Protect Our Own* ».
[4] KNIGHTLEY (P.), *The Second Oldest Profession: Spies and Spying in the Twentieth Century,* New York, Norton, 1980, 468 p.
[5] GILES (L.), *Sun Tzu on the Art of War,* Leicester, Allandale Online Publishing, 2000, p. 62.
[6] RICHMOND (I.), « Spies in Ancient Greece », *Greece & Rome*, Vol. 45, 1998, n°1, pp. 4-5.
[7] MCELREATH (D.) et al., *Introduction to Homeland Security,* Boca Raton, CRC Press, seconde édition, 2013, p. 297.

I.S.B.N. 978-2-233-00989-0

qui l'envoie. Encore de nos jours, il est fréquent qu'un espion déployé « sur le terrain » soit exécuté[8], ou devienne une monnaie d'échange suite à sa capture[9]. Il n'y a rien de tel avec l'espionnage numérique. Même si un « cyber-espion » est identifié et qu'un mandat d'arrêt est émis à son encontre, l'Etat responsable se contente bien souvent de nier son implication, et n'extrade pas son agent. Les chances que ce dernier soit emprisonné sont donc minces. Cela permet en second lieu de réduire le temps nécessaire à la préparation des opérations, ainsi que leur coût. Le déploiement d'un agent en territoire étranger requiert bien souvent l'apprentissage de langues étrangères, la construction de fausses identités, et la mise en place de moyens de communication spéciaux[10]. Mettre sur écoute des lignes de communications peut coûter plusieurs millions de dollars[11], et un programme de reconnaissance satellitaire, plusieurs milliards[12]. A l'inverse – et à l'exception de quelques techniques spécifiques, comme l'exploration de données [ou « *data mining* »] de masse – le cyber-espionnage est relativement peu onéreux[13]. Fondamentalement, il ne nécessite que quelques experts en informatique, des ordinateurs, et un accès à internet. En

[8] Ainsi, « *des dernières semaines de 2010 jusqu'à la fin de 2012, selon d'anciens officiels américains, les Chinois tuèrent au moins une douzaine de sources de la CIA* [*Central Intelligence Agency*] ». Le métier a même ses « subtilités » : « *selon trois de ces officiels, l'un fut tué devant ses collègues dans la cour d'un bâtiment gouvernemental – un message* [envoyé] *à tous ceux qui auraient pu travailler pour la CIA* » . Voir : MAZZETTI (M.) et al., « Killing C.I.A. Informants, China Crippled U.S. Spying Operations », *The New York Times*, 20 mai 2017 [disponible sur le lien suivant : https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html] Consulté le 24 avril 2019 [nous traduisons].

[9] « Spy swap in the offing? Exchange for Whelan to be considered after sentence, says lawyer », *TASS*, 15 juin 2020 [disponible sur le lien suivant : https://tass.com/society/1167735] Consulté le 7 août 2020 ; « Spy swap: Five freed in Russia-Lithuania-Norway exchange », *BBC*, 15 novembre 2019 [disponible sur le lien suivant : https://www.bbc.com/news/world-europe-50431713] Consulté le 7 août 2020 ; CROWLEY (M.), « In Prisoner Swap, Iran Frees American Held Since 2016 », *The New York Times*, 7 décembre 2019 [disponible sur le lien suivant : https://www.nytimes.com/2019/12/07/us/politics/iran-prisoner-swap-xiyue-wang.html?auth=login-email&login=email] Consulté le 7 août 2020.

[10] GALEOTTI (M.), « Size Doesn't Matter for Spies Anymore », *Foreign Policy*, 31 mars 2018 [disponible sur le lien suivant : https://foreignpolicy.com/2018/01/31/size-doesnt-matter-for-spies-anymore] Consulté le 14 avril 2019.

[11] Par exemple, l'opération *CKELBOW* consistait à mettre sur écoute les « *lignes de transmission de données sensibles reliant les installations d'armes nucléaire à Troitsk et le Ministère de la Défense à Moscou* », et « *coûta aux Etats-Unis la somme de 20 millions de dollars* ». Voir : HOFFMAN (D.), *The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal,* New York, Anchor Books, 2017, Chapter 14 [nous traduisons].

[12] SCHWARTZ (S.), *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940,* Washington, Brookings Institution Press, 1998, pp. 238-239.

[13] GALEOTTI (M.), « Size Doesn't Matter for Spies Anymore », *op. cit.* De plus, construire des « *cyber-armes* » devient de moins en moins cher, grâce à « *quatre procédés* ». Premièrement, « *la main d'œuvre devient plus efficace, les fouineurs gagnent en habilité* […] *ils passent moins de temps à apprendre, à expérimenter et à faire des erreurs en écrivant du code* ». Deuxièmement, « *[c]ertaines parties des cyber-armes sont devenues de plus en plus standardisées* », à l'instar des « *outils pour exploiter les vulnérabilités* ». Troisièmement, « *réutiliser des logiciels malveillants et construire à partir de ces derniers permet aux pirates d'apprendre à produire des cyber-armes de façon plus efficace* ». Quatrièmement, les leçons résultants du développement de certains logiciels malveillants sont transmises grâce à un certain « *partage d'expérience* ». Voir : SMEETS (M.), « How Much Does a Cyber Weapon Cost? Nobody Knows », *CFR*, 21 novembre 2016 [disponible sur le lien suivant : www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows] Consulté le 16 avril 2019 [nous traduisons].

I.S.B.N. 978-2-233-00989-0

troisième lieu, la quantité d'informations potentiellement accessibles est bien plus importante avec une opération de cyber-espionnage que de renseignement humain. La première opération de ce type attribuée à un Etat fut appelée *Moonlight Maze,* et se déroula en 1999. A l'époque, l'enquête concluait déjà « *que le nombre total de fichiers volés, si imprimés et empilés, serait plus haut que le Washington Monument* »[14]. Une fameuse déclaration du Général Keith Alexander était que les activités de cyber-espionnage économique menées contre les entreprises américaines constituaient « *le plus grand transfert de richesse de l'Histoire* »[15].

3. La question de la régulation du cyber-espionnage, qui est au cœur de cette étude, soulève quant à elle deux défis majeurs. Le premier, c'est le fait que l'espionnage n'ait été appréhendé que de manière incomplète par le droit international, et ne constitue pas un fait internationalement illicite en soi. Seul le droit des conflits armés a défini le régime juridique applicable aux espions, et il est admis que l'espionnage entre belligérants n'est pas contraire aux lois de la guerre. En dehors de ce cadre, et notamment en temps de paix, c'est la règle de souveraineté territoriale qui a longtemps permis une régulation indirecte de l'espionnage. En effet, et quelle que soit l'activité menée, l'envoi d'un agent sur le territoire d'un Etat constitue nécessairement – en l'absence de consentement de ce dernier – une violation de souveraineté. Une autre forme de régulation indirecte est également identifiable dans la Convention de Vienne sur les Relations Diplomatiques, et protège tant l'Etat accréditant que l'Etat accréditaire. D'un côté, il est interdit aux agents de l'Etat accréditaire de pénétrer dans les locaux d'une ambassade, tandis que les archives, documents et correspondances officielles de la mission sont réputés inviolables. D'un autre côté, le personnel diplomatique est tenu de respecter la législation locale, qui prohibe systématiquement l'espionnage. Il n'existe donc aucun instrument contraignant qui interdise (ou autorise) ouvertement l'espionnage, et encore moins le cyber-espionnage. Le second défi se trouve dans la transposition éventuelle de ces règles à un environnement et à une activité numériques. Bien que les Etats aient reconnu que le droit international s'applique dans le cyber-espace – le « cinquième domaine » – leurs divergences sur ses modalités d'application sont en fait trop nombreuses pour permettre une simple analogie entre le régime juridique applicable à l'espionnage et celui du cyber-espionnage.

4. Afin de poser les bases de cette étude, il s'agira tout d'abord d'en définir les notions principales (**I**), puis son cadre conceptuel (**II**). Cette introduction mettra enfin en lumière ses enjeux (**III**).

[14] ROBINSON (M.), *Why Democrats lost the presidential election and how they can win next time,* Scotts Valley, CreateSpace, 2017, p. 107 [nous traduisons].
[15] ROGIN (J.), « NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history" », *Foreign Policy,* 9 juillet 2012 [disponible sur : https://foreignpolicy.com/2012/07/09/ nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/] Consulté le 12 avril 2019 [nous traduisons].

I.S.B.N. 978-2-233-00989-0

I. NOTIONS DE L'ÉTUDE

5. C'est à l'écrivain américain William Gibson que l'on doit l'invention du terme « cyber-espace », dont la définition par le roman *Neuromancien* ne saurait que difficilement satisfaire le juriste : « *[l]e cyber-espace. Une hallucination consensuelle, vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays* […] *Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain* »[16]. La formule est en fait la contraction des mots « espace » et « cybernétique », étant entendu que le préfixe « cyber » viendrait viendrait du grec « κυβερνάω » – « *kubernân* », c'est-à-dire « gouverner » – et a depuis servi à former un certain nombre de termes ayant trait à Internet. Bien que le mot fasse désormais partie du langage courant, et soit notamment utilisé par les juristes, il n'existe en fait pas de définition universellement admise du terme « cyber-espace ». Cette étude ambitionne donc d'expliquer ce qu'est le cyber-espace (**Section 2**).

6. Mais avant cela, c'est le concept de « cyber-espionnage » – c'est-à-dire l'objet central de cette étude – qui sera étudié. Bien que la conception délivrée par Alvin Toffler soit visionnaire, elle ne saurait non plus contenter le juriste : en 1990, ce dernier avait déjà anticipé l'intérêt que les ordinateurs pouvaient révêtir pour mener des activités d'espionnage. Selon lui, « *l'espion du futur* » ne ressemblerait probablement pas « *à James Bond* » mais à « *l'ingénieur qui vit tranquillement au coin de la rue et ne fait jamais rien de plus violent que de tourner la page d'une notice ou de presser une touche du clavier de son micro-ordinateur* »[17]. Cette étude vise donc, en premier lieu, à proposer une définition plus consensuelle du cyber-espionnage (**Section 1**).

SECTION 1. LA NOTION DE « CYBER-ESPIONNAGE »

7. Afin de définir le terme de « cyber-espionnage », cette étude procèdera en deux temps. Elle identifiera d'abord les éléments constitutifs de cette activité (§ **1**), avant de la distinguer d'autres notions (§ **2**).

§ 1. Les éléments constitutifs du cyber-espionnage

8. S'il n'existe pas de définition universellement admise du « cyber-espionnage », une activité aussi désignée par les Etats-Unis, le Royaume-Uni et l'Organisation du traité de l'Atlantique nord (OTAN) sous le terme d'« exploitation de réseau informatique », la pratique étatique permet d'identifier plusieurs éléments de convergence lorsqu'il s'agit d'identifier cette notion. Le premier, c'est l'objectif visé par le cyber-espionnage ; le second, c'est le caractère non-consensuel de cette activité. Ainsi, le cyber-

[16] GIBSON (W.), *Neuromancien*, Paris, La Découverte, 1984, p. 64.
[17] LATHROP (C.), *The Literary Spy*, *op. cit.*, p. 129 [nous traduisons].

I.S.B.N. 978-2-233-00989-0

espionnage correspondrait au « *vol* », à l' « *accès* » ou à la « *collecte* » de « *secrets* », d'informations « *classifiées* » ou « *confidentielles* » et ce, « *sans la permission* » de leurs propriétaires, de manière « *non autorisée* », « *irrégulière* » ou « *illicite* »[18].

[18] Selon l'Australie, le cyber-espionnage est « *le vol d'information à des fins de renseignement* » : Department of the Prime Minister and Cabinet (Australie), *Australia's Cyber Security Strategy*, Canberra, Commonwealth of Australia 2016, p. 15 [nous traduisons]. Selon le Nigéria, c'est « *l'acte ou la pratique d'obtenir des secrets sans la permission du propriétaire de l'information* » : Bureau du Conseiller à la Sécurité nationale (Nigéria), « National Cybersecurity Strategy », 2017, appendix 2 [disponible sur le lien suivant : https://tekedia.com/wp-content/uploads/2017/04/ncss-STRATEGY.pdf] Consulté le 28 octobre 2017 [nous traduisons]. Selon l'Afrique du Sud, c'est « [une cyber menace] *impliquant entre autres, la collecte secrète d'informations classifiées sans la permission de leur propriétaire* » : South African Defence, « Defence Review 2015 », 2014, para. 75 [disponible sur le lien suivant : www.dod.mil.za/documents/defencereview/defence%20 review%202015.pdf] Consulté le 18 mai 2017 [nous traduisons]. Selon le Monténégro, c'est « *le recours à un agent afin d'obtenir des informations sur les intentions ou les activités d'un pays étranger ou d'une entreprise concurrente* » : Gouvernement (Monténégro), « National Cyber Security Strategy for Montenegro 2013-2017 », 2013, p. 7 [disponible sur : www.unodc.org/res/cld/lessons-learned/national-cyber-security-strategy-for-montenegro-2013-2017_html/National_Cyber_Security_Strategy_for_ Montenegro_2013-2017.pdf] Consulté le 3 octobre 2016 [nous traduisons]. L'Italie semble ajouter une distinction supplémentaire, puisque les termes « *exploitation de réseau informatique* » et « *cyber-espionnage* » trouvent des définitions différentes. La première serait constituée « *des opérations menées dans le cyberspace afin d'extraire des informations de réseaux TIC ou de systèmes informatiques. Ce sont des activités de collecte de renseignements, ou des actes préparatoires* [menés] *en vue d'exécuter une cyber-attaque* » : Présidence du Conseil des Ministres (Italie), « Italian National Strategic Framework for Cyberspace Security », 2013, p. 41 [disponible sur le lien suivant : www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf] Consulté le 24 septembre 2016 [nous traduisons]. Le second, quant à lui, serait « *l'acquisition irrégulière de données confidentielles ou classifiées, pas systématiquement de nature économique ou commerciale* » : *ibid.,* p. 13 [nous traduisons]. Selon l'Autriche, « *les cyber-attaques dirigées contre la confidentialité d'un système TI sont appelées "cyber espionnage", c'est-à-dire l'espionnage numérique* » : Chancellerie fédérale (Autriche), « Austrian Cyber Security Strategy », 2013, p. 20 [disponible: www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21] Consulté le 2 octobre 2016 [nous traduisons]. L'Allemagne adopte une position similaire, mais souligne qu'elles « *sont lancées ou conduites par des services de renseignement étrangers* » : Ministère fédéral de l'intérieur (Allemagne), « Cyber Security Strategy for Germany », 2011, pp. 14-15 [disponible sur : www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_ download.pdf?__blob=publicationFile] Consulté le 24 septembre 2019 [nous traduisons]. Selon la Macédoine, le cyber-espionnage est « *une cyber-attaque dirigée contre la confidentialité des systèmes de TIC* » : République de Macédoine, « National Cyber Security Strategy 2018-2022 », 2018, p. 36 [disponible sur : https://www.mioa.gov.mk/sites/default/files/pbl_files/ documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf] Consulté le 30 septembre 2020. Selon la Suisse, le cyber-espionnage est une « « *[a]ctivité visant à accéder de manière non autorisée à des informations à des fins politiques, militaires ou économiques dans le cyberespace* » : Conseil fédéral (Suisse), *Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022*, Berne, Unité de pilotage informatique de la Confédération UPIC, 2018, p. 31. Le Chili définit l' « espionnage » et les « activités de surveillance comme des « *conduites qui affectent la confidentialité des informations en raison de leur vol pour des raisons politiques ou stratégiques* » : Gouvernement (Chili), « National Cybersecurity Policy », 2017, p. 35. [disponible sur le lien suivant : http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf] Consulté le 3 octobre 2020.

I.S.B.N. 978-2-233-00989-0

TABLE DES MATIÈRES

Remerciements 5
Sommaire 7
Sigles et abréviations 9

INTRODUCTION

I. Notions de l'étude 16
Section 1. La notion de « cyber-espionnage » 16
§ 1. Les éléments constitutifs du cyber-espionnage 16
§ 2. Les éléments de distinction entre le cyber-espionnage et d'autres activités .. 20
A. La distinction entre le cyber-espionnage et les cyber-attaques 20
B. La distinction entre le cyber-espionnage et d'autres formes de renseignement. 25
Section 2. La notion de « cyber-espace » 29
§ 1. Les éléments caractéristiques du cyber-espace 29
§ 2. La régulation du cyber-espace 36
II. Cadre conceptuel de l'étude 43
Section 1. La détermination du droit 45
§ 1. L'approche de l'interprétation des traités 45
§ 2. L'approche des sources 50
A. L'approche du droit international coutumier 51
B. L'approche des principes généraux du droit et des Manuels de Tallinn 57
Section 2. Le concept d'évitement normatif 59
§ 1. La possibilité d'une absence d'interdiction ou de permission 60
§ 2. L'absence d'interdiction ou de permission comme résultat de la volonté étatique 65
III. Enjeux de l'étude 67
Section 1. Délimitation du champ de l'étude 68
Section 2. Argument principal de l'étude 71

I.S.B.N. 978-2-233-00989-0

PREMIÈRE PARTIE
LES RÈGLES CONNECTÉES À L'INTÉGRITÉ TERRITORIALE

TITRE I. LE DROIT DE LA COEXISTENCE PACIFIQUE

Chapitre 1. Le droit interdisant les atteintes à la souveraineté territoriale 79
Section 1. L'impossibile assimilation de l'intrusion numérique *per se* à une violation de souveraineté 80
§ 1. L'impossible assimilation de l'espionnage *per se* à un fait internationalement illicite 81
§ 2. L'impossible assimilation de l'intrusion numérique à une intrusion physique 86
Section 2. L'impossible assimilation de l'intrusion numérique causant un dommage à une violation de souveraineté 94
§ 1. L'indifférence du dommage dans la qualification de violation de souveraineté 94
§ 2. L'absence de contre-mesures en réponse à des opérations de cyber-espionnage 99
Chapitre 2. Le droit de la sécurité collective 103
Section 1. L'absence de règlementation du cyber-espionnage selon une lecture traditionnelle de la Charte 104
§ 1. La définition des termes des articles 2§4 et 51 de la Charte des Nations Unies 104
§ 2. L'application des articles 2§4 et 51 de la Charte des Nations Unies 107
Section 2. L'absence de règlementation du cyber-espionnage selon une lecture alternative de la Charte 114
§ 1. Le recours aux méta-règles d'interprétation 114
§ 2. Le recours à l'interprétation téléologique 122
Conclusion du titre I. 127

TITRE II. LE DROIT RÉGISSANT LA CONDUITE DES HOSTILITÉS

Chapitre 1. Le droit applicable entre états belligérants 131
Section 1. La vocation territoriale des règles relatives à l'espionnage entre belligérants 132
§ 1. Les catégories d'espions définies par les lois de la guerre 132
§ 2. La difficile transposition des règles relatives à l'espionnage dans un espace virtuel 136
Section 2. Le relatif désintérêt des Etats quant à la précision des règles applicables au cyber-espionnage 141
§ 1. L'absence du cyber-espionnage dans la définition de standards minimum de protection par les Etats 141
§ 2. Le rejet de l'application des règles existantes de droit international humanitaire aux cyber-opérations par certains Etats 145

I.S.B.N. 978-2-233-00989-0

Chapitre 2. Le droit applicable entre états belligérants et états neutres.... 149
Section 1. L'absence de règlementation du cyber-espionnage par les règles applicables aux opérations matérielles 150
§ 1. Les obligations pesant sur les belligérants 150
§ 2. Les obligations pesant sur l'Etat neutre..... 159
Section 2. Une restriction limitée du cyber-espionnage par les règles applicables à l'utilisation des moyens de télécommunication 162
§ 1. Les obligations pesant sur les belligérants 162
§ 2. Les obligations pesant sur l'Etat neutre..... 163
Conclusion du titre II. 167

CONCLUSION DE LA PREMIÈRE PARTIE 169

DEUXIÈME PARTIE
LES RÈGLES DÉCONNECTÉES DE L'INTÉGRITÉ TERRITORIALE

TITRE I. LE DROIT DE LA COOPÉRATION

Chapitre 1. Le droit des relations diplomatiques 177
Section 1. La règlementation indirecte de l'espionnage par les ambassades..... 178
§ 1. Les moyens de protection au stade de l'accréditation de la mission 178
§ 2. Les moyens de protection au stade de l'accomplissement de la mission..... 179
Section 2. La règlementation indirecte de l'espionnage sur les ambassades.. 186
§ 1. L'absence de règlementation du cyber-espionnage par les règles relatives à l'inviolabilité des locaux de la mission diplomatique 186
§ 2. La contrariété du cyber-espionnage avec les règles d'inviolabilité des archives et documents de la mission 191
Chapitre 2. Le droit international économique..... 197
Section 1. L'absence d'interdiction du cyber-espionnage économique..... 198
§ 1. L'absence d'interdiction par l'obligation de traitement national..... 198
§ 2. L'absence d'interdiction par l'obligation de protection des renseignements non-divulgués 202
Section 2. La préservation de certaines formes de cyber-espionnage politique..... 209
§ 1. La préservation de certaines formes de cyber-espionnage politique en temps de paix 209
§ 2. La préservation de certaines formes de cyber-espionnage politique en temps de conflit ou de fortes tensions 211
Conclusion du titre I. 215

I.S.B.N. 978-2-233-00989-0

TITRE II. LE DROIT DU RENSEIGNEMENT

Chapitre 1. Le droit national en matière d'espionnage 219
Section 1. Une interdiction unanime de l'espionnage en droit pénal national .. 220
§ 1. Une interdiction classique de l'espionnage en général 220
A. L'interdiction de l'espionnage dans les législations actuelles 220
B. L'interdiction de l'espionnage dans les législations plus anciennes 225
§ 2. Une interdiction progressive des intrusions et interceptions numériques 228
Section 2. Une autorisation majoritaire des activités de renseignement dirigées contre d'autres Etats en droit national 232
§ 1. Les dispositions prévoyant la collecte de renseignements 232
§ 2. Les motifs permettant la collecte de renseignements 240
Chapitre 2. Un droit international coutumier spécifique à l'espionnage ? 247
Section 1. La pratique 248
Section 2. L'*opinio juris* 251
§ 1. L'absence de droit à l'espionnage 251
§ 2. L'absence d'interdiction de l'espionnage 259
Conclusion du titre II. 265

CONCLUSION DE LA DEUXIÈME PARTIE 265

CONCLUSION GÉNÉRALE

Bibliographie 277
Documents officiels 313
Traités internationaux, actes institutionnels, réglementations et législations nationales 349
Jurisprudence 361

I.S.B.N. 978-2-233-00989-0

Bien que les États s'espionnent depuis des siècles, l'émergence d'internet a favorisé une intensification des activités de renseignement. Dans cet espace qui se joue des frontières – et où triomphent l'anonymat, une prise de risque décrue et un accès potentiel à de multiples informations – le fragile équilibre autrefois atteint par le droit international à l'égard des formes traditionnelles d'espionnage vole en éclat.

En effet, l'espionnage *per se* n'a jamais été expressément interdit ou autorisé par le *jus gentium*, et les États se sont longtemps contentés d'une régulation indirecte de cette activité, par le prisme de différentes règles : souveraineté territoriale, droit des relations diplomatiques, lois de la guerre. Leur essence et leur raison d'être reposaient, toutefois, sur la présence de l'espion en territoire étranger ou en zone ennemie, et la possibilité de l'appréhender. « Servir et périr » : bien souvent, c'est au risque de sa vie qu'un agent défendait les intérêts de son pays. En cas de capture d'un espion, ce dernier se devait d'assumer le poids de sa condamnation ou de sa déclaration *persona non grata* ; l'État d'envoi, d'en essuyer l'infamie.

Or, le cyber-espionnage bouleverse ce cadre, puisque l'agent peut désormais remplir sa mission à partir de sa propre juridiction. À l'exception du cyber-espionnage mené contre les documents diplomatiques, il s'avère désormais que cette activité échappe en grande partie au droit. En reposant sur un corpus inédit de pratique étatique – élément essentiel à l'interprétation de règles existantes et à l'identification de règles coutumières nouvelles – cet ouvrage démontre que le cyber-espionnage est sujet à un évitement normatif. Cette activité n'est pas interdite – car les États ne commettent aucun acte internationalement illicite lorsqu'ils s'y livrent – mais n'est pas pour autant « permise », « autorisé » ou constitutive d'un « droit », puisqu'ils sont libres également d'adopter des mesures pour prévenir et contrer les activités de cyber-espionnage menées par d'autres États. Or, cet état de la régulation n'a rien de fortuit : les États souhaitent en effet profiter de cette absence d'interdiction, sans pour autant que d'autres aient un droit à mener de telles activités, susceptibles de léser leurs propres intérêts.

ISBN 978-2-233-00989-0

9 782233 009890

CESICE

48 €

Photo : Pris(c)ille - Collection particulière

cyber espionnage