

COLLOQUE PLURIDISCIPLINAIRE - UNIVERSITE DE DSCHANG
APPEL À COMMUNICATIONS

DU 06 AU 07 MAI 2021

CYBERCRIMINALITE & CYBERSECURITE AU CAMEROUN ET EN AFRIQUE

Représentations, Manifestations, Financements
& Traitements des menaces

CYBER-SÉCURITÉ



RÉSUMÉ

Avec une croissance exponentielle des phénomènes de cybercriminalité, le développement des investissements massifs dans le numérique, l'adoption d'une loi sur la cybersécurité et la cybercriminalité et une politique nationale de la cybersécurité, le Cameroun est devenu le nouveau centre de gravité et de référence de la cybersécurité en Afrique Centrale ; même si les connaissances sur le phénomène restent encore fragmentaires. En prélude à l'ouverture d'un Master Professionnel de l'Université de Dschang sur la cybersécurité et la gouvernance sécuritaire, ce colloque met en perspective une réflexion sur la complexité et les enjeux de la cybersécurité. Il offre un regard croisé et complémentaire sur des questions d'intérêt commun relatives aux problématiques de la cybersécurité. Il réunira de nombreux chercheurs, professionnels, experts, spécialistes nationaux et internationaux intéressés par l'objet cybersécurité, tout en cherchant à combler une double lacune : d'une part celle des informaticiens spécialisés en sécurité informatique mais ne disposant pas de connaissances suffisantes sur l'environnement juridique, politique, économique, national et international de la Cyber sécurité ; et d'autre part celle des spécialistes de la sécurité qui n'ont pas de connaissances suffisantes en informatique alors que l'essentiel de l'insécurité se déroule actuellement sur le cyberspace.

ABSTRACT

Due to the exponential increase in the cybercriminality phenomena, the development of huge investments in digitalization, the adoption of a law on cyber security and cybercriminality, as well as a national policy of cyber security, Cameroon has become a new center of gravity and reference of cyber security in Central Africa ; even if knowledge on the phenomenon is still fragmentary. Prior to the opening of a Professional Master on cyber security and security governance at the University of Dschang, this colloquium is geared towards reflecting on the complexity and the stakes of cyber security. It enables a complementary cross-view of issues of mutual interest with regards to the question of cyber security. It will bring together a good number of researchers, professionals, experts, and specialists from the national territory and from abroad who are interested in the matter of cyber security, while seeking to amend a double deficiency : on the one hand, that of computer-scientists specialized in computer security but without enough knowledge surrounding cyber security at the juridical, political, economic, national and international levels ; on the other hand, that of security specialists not having enough knowledge in computer science meanwhile insecurity at the moment is essentially occurring on the cyber space.

01

ARGUMENTAIRE

Les expériences internationales en matière de cyber-stratégie, cyberattaque, de cyberdéfense, de cybercriminalité (Quéméner, 2018), de cyberguerre (Cattaruzza, 2019) ou de cybermenace annonçaient la couleur d'une nouvelle structuration des rapports de force à la fois à l'échelle mondiale et locale (Arpagian, 2017). En reconnaissant la parenté de ce contexte avec celui du Cameroun, on ouvre à la réflexion sur la cybersécurité, un champ nouveau d'analyse utile par ailleurs tant pour les décideurs publics, que pour les investisseurs privés.

Le constat ci-dessus posé fait apparaître beaucoup de gloses, par exemple que le réseau internet par son ampleur et ses répercussions stratégiques importantes sur le champ national, est l'enjeu de nombreuses rivalités qui donnent lieu à des stratégies de domination de la part des acteurs politiques (Cukierman, Rouach, 2018). Ces répercussions qui déplacent le cadre national de la cybersécurité vers le cadre international (Boulangier, 2014), résument tout le caractère hautement stratégique du phénomène pour la sécurité des Etats (Cattaruzza, 2018) et surtout son instrumentalisation comme moyen de puissance (David, 2017) et de pouvoir entre formes d'organisations politiques, forces politiques, religieuses, économiques et bien d'autres (Taillat, Cattaruzza, Danet, 2018).

Au Cameroun, le Ministre des Postes et Télécommunications a coutume de souligner combien les réseaux sociaux sont devenus de véritables outils de désinformation, d'intimidation, d'appel à la haine, aux meurtres, à la violence. Cette désinformation

émane généralement des individus dont le but est de nuire justement à la réputation des personnalités ou des institutions de la République. Le cycle politique ouvert depuis les élections présidentielles de 2018 a particulièrement été significatif s'agissant du recours à l'usage des réseaux sociaux par les citoyens. La période s'avère aussi propice à toutes sortes de manipulations, notamment la diffusion d'éléments à la véracité incertaine et contestable. L'on assiste à l'amplification d'un discours de haine et d'exclusion, parfois selon un vocabulaire appelant à la division des Camerounais, sur des bases communautaires, ethniques ou tribales. Dans le même temps, l'on note la montée en puissance de l'intolérance et des extrémismes de tout bord.

Selon l'Agence nationale des techniques de l'information et de la communication (ANTIC), entre 2015 et 2017, sept (07) sites web d'administrations publiques camerounaises ont subi une attaque de type web defacement, en 2017 trente-quatre (34) sites gouvernementaux ont été attaqués par des programmes malveillants, plusieurs centaines de cas d'usurpations d'identités sur les réseaux sociaux dont cent quatre-vingt-deux (182) contre des membres du Gouvernement, environ quatre (04) milliards de FCFA de pertes économiques liées au scamming dans les principaux foyers que sont les zones universitaires des villes de Bamenda, Buéa, Yaoundé et Douala. En 2017 toujours, les pertes dues à la fraude à la carte bancaire s'évaluaient à environ 3,7 milliards de Francs CFA, et la fraude à la SIMBOX à plusieurs milliards de FCFA.

Au début des années 2000 pourtant, le numérique portait les promesses de développement, de pacification, de surveillance généralisée des territoires (Henrotin, 2018), et de progrès économique de l'Etat par les opportunités de marchandisation, d'échanges et de valeurs qu'il diffusait (Moreau Defarges, 2018). Avec une croissance exponentielle de 22% d'utilisateurs d'internet en 2017, en passant de 5,01 millions à 6,13 millions, le Cameroun était devenu le centre de gravité du cybernétique en Afrique Centrale. L'émergence d'un cyberspace né de l'interconnexion des réseaux va révolutionner les modes de vie (Haddad, 2018), bouleverser les pratiques politiques (Nocetti, 2018), les pratiques sécuritaires, les pratiques économiques, les pratiques culturelles, les pratiques pédagogiques, démultiplier les moyens de communication et ouvrir de nouveaux horizons aux acteurs étatiques et interétatiques (Delesse, 2016). Mais, internet va également engendrer des défis proportionnels aux promesses (Taillat, 2018) : des crispations territoriales (Moreau Defarges, 2017), les bouleversements des liens sociaux et stratégiques (Taillat, 2017) et alimenter une prolifération de conflits et d'antagonismes entre acteurs (Ducruet, 2017). Ces défis en raison de leurs caractères dystopiques (Massit-Folléa, 2018) se cristallisent en nouvelles formes de menaces (Cassuto, 2018) aussi bien dans le champ politique, sécuritaire, économique, diplomatique (Nocetti, 2017) et culturel. En 2020 encore, parmi les 10 premières menaces mondiales relevées par le Global Risks Report, se trouve en bonne place les fraudes ou vols informatiques (Data fraud or theft) et les cyberattaques.

A l'heure du *in data* et du *out data*, les débats se multiplient autour d'une question d'intérêt commun, celle de la maîtrise des enjeux de la cybersécurité. En effet, la cyber

sécurité en raison du développement considérable d'internet, de son omniprésence et de son usage non contrôlé dans toutes les dimensions de la société, soulève des problématiques d'intérêt multiples (Aby, 2020). L'Etat, le gouvernement, les militaires, les entreprises, les populations ont besoin de cerner toute la complexité de la cybersécurité (Haddad, 2017) et la matérialité de ses enjeux au Cameroun, pour mieux valoriser et veiller à la préservation de leurs intérêts.

La cybersécurité est un défi politique, économique, social et épistémique de premier ordre tant pour les États que pour les organismes privés et la société toute entière et se présente comme une source de connaissances et de mise en relation des acteurs (Sudres, 2017). Ce que l'on constate, c'est l'ampleur et la rapidité de la transformation et de la réappropriation du concept sur le continent africain. Malgré cela, il reste un objet d'étude aux contours flous, qui n'a pas encore réussi à asseoir sa conceptualisation (Danet, Desforges, 2020). Ce phénomène interpelle les chercheurs à diversifier leurs approches épistémologiques de la cybersécurité (D'Elia Danilo, 2015) afin de cerner les contours variés de sa conceptualisation (Kempf, 2017) qui tiennent compte de l'espace et du sens de son opérationnalisation comme le montre si bien le cas des pays africains. Sa survenue au Cameroun renforce déjà la portée de son cadre particulariste en raison des phénomènes observés. La cybersécurité au Cameroun continue d'être dominé par le regard normativiste et institutionnel (Delerue, Géry, 2018), alors qu'elle interpelle fondamentalement la rationalité scientifique et méthodologique de toutes les disciplines. Les questions liées aux phénomènes de cyberspace (Douzet, 2020), de cybercriminalité (Cattaruzza, Buisson 2018), de cyberdéfense, de cyberattaques, etc. n'interpellent pas seulement les compétences politico-institutionnelles, mais aussi celles des autres disciplines. Dans cette perspective, il s'agit de valoriser l'intersectionnalité afin de cerner la conception globale du phénomène au Cameroun. Comment ?

D'une part, en œuvrant pour connaître et faire connaître le phénomène autant dans sa dimension pratique, pluri et interdisciplinaire; et d'autre part, en valorisant les ressorts empiriques et plus actuels de la cybersécurité au Cameroun à partir non plus seulement des modèles internationaux mais suivant une vision centrée sur les paradigmes de la recherche locale. Le but du colloque est de convoquer l'approche pluridisciplinaire pour analyser le phénomène de cybersécurité en contexte camerounais. Ce sera l'occasion de fédérer à l'approche non seulement des professionnels de la cybersécurité (Weber, Commandant, 2018), les approches scientifiques, de science politique, de sociologie, de psychologie, de droit, de géographie, d'histoire, d'économie, d'informatique, et bien d'autres. Il servira de plateforme pour des échanges enrichissants, des débats d'idées et des critiques constructives pour contribuer tout autant à l'enracinement qu'à l'avancement de la maîtrise du phénomène de la cybersécurité en Afrique et au Cameroun.

L'un des dilemmes de la recherche en matière de cybersécurité (Lavoix, 2019) provient du cloisonnement spatial persistant de la plupart des études africaines qui traitent séparément la sécurité et les questions de cyberspace. Plus spécifiquement, les études africaines en matière de cybersécurité peinent à sortir de leur forme d'homogénéisation conceptuelle et de leurs tendances comparatives sur le développement (Bogui, 2010) et la gouvernance des données (Longuet, Fenet, Hirsch et al. 2017). Or, lorsque l'Afrique est étudiée dans une tendance comparative, elle ne l'est pas pour elle-même mais au prisme des clichés qui empêchent sa réductibilité, c'est-à-dire sa capacité à mettre en relation la problématique de la cybersécurité et la multiplicité des contextes en raison de leurs particularités spatiales, sécuritaires, socio-anthropologiques, économiques, politiques et diplomatiques (Walsh, Kalika, Dominguez-Péry, 2018).

L'objectif principal de ce colloque est d'une part favoriser un creuset d'échanges et d'analyses scientifiques entre les différents acteurs intervenant dans le champ de la cybersécurité au Cameroun et d'autre part de comprendre la cybersécurité sous le prisme du terrain camerounais marqué tour à tour par les études sur l'épistémologie du phénomène (Tepi, 2020), et ses enjeux normatifs et stratégiques (Yogo, 2015) qui attestent de l'émergence d'une jeune tradition d'analyse sur la cybersécurité. A la faveur de ces débats sur le champ politique camerounais riche en participation et en contestation, il est clair qu'on assiste à un renouveau des études sur la cybersécurité.

Cette tradition d'analyse centrée sur le local a le mérite de tracer les sillons d'une réflexion plus approfondie sur la cybersécurité dans le cyberspace camerounais. Elle n'insistera plus sur les cadres d'interprétations centrés sur la vision occidentale de la cybersécurité (Douzet, 2020) mais mettra un accent à la fois sur les cadres de conceptualisation mais aussi d'opérationnalisation internes et externes de la cybersécurité au Cameroun. Cette approche a le mérite d'amener à se focaliser sur la manière avec laquelle les acteurs intervenants dans le champ de la cybersécurité (acteurs politiques, acteurs économiques, acteurs sécuritaires, groupes sociaux, acteurs culturels et acteurs internationaux) mobilisent des relations de pouvoir, des comportements politiques, stratégiques, les discours politiques, et arriment solidement la cybersécurité à la structuration de leurs enjeux dans le cyberspace camerounais.

Dans le prolongement de cette réflexion engagée sur les cadres d'interprétation internes et externes de la cybersécurité au Cameroun, nous encouragerons les chercheurs à faire des propositions qui sont conformes aux axes et sous-thèmes suivants:

01

CONNAISSANCES DE LA SÉCURITÉ ET DE LA CYBER SÉCURITÉ Entre regard ancien et perspectives nouvelles sur la sécurité

SOUS-THÈMES

- 1) Histoire de la cybercriminalité et de la cybersécurité
- 2) Concepts, théories et pratiques de la cybersécurité
- 3) Grands enjeux contemporains de la sécurité et de la cybersécurité
- 4) Géopolitique de la cybercriminalité au Cameroun

02

ENVIRONNEMENT SOCIO-PSYCHOLOGIQUE, ÉCONOMIQUE DE LA CYBERSÉCURITÉ

SOUS-THÈMES

- 1) Psychologie des cyber criminels au Cameroun
- 2) Sociologie du cyber espace et de la cyber criminalité
- 3) Espionnage économique à l'ère du numérique
- 4) Évaluation économique et financière de la cybercriminalité et cybersécurité dans les organismes publics et les entreprises privées.

03

ENVIRONNEMENT JURIDIQUE ET POLITIQUE DE LA CYBERSÉCURITÉ

SOUS-THÈMES

- 1) Droit du numérique au Cameroun
- 2) Droit pénal de l'informatique et de la cybercriminalité
- 3) Politiques et actions publiques de cybersécurité au Cameroun
- 4) Normes internationales/ Coopérations internationale et africaine en matière de cybersécurité
- 5) Etudes stratégiques et cybersécurité au Cameroun : quelle convergence ?
- 6) Le cyber renseignement : approches et méthodes
- 7) Veille sécuritaire à l'ère du numérique
- 8) Mutations de la sécurité à l'ère du numérique

04

ENVIRONNEMENT TECHNIQUE DE LA CYBERSÉCURITÉ

SOUS-THÈMES

- 1) Langues et techniques d'expression dans le cyberspace
- 2) Techniques des systèmes d'exploitation, réseaux informatiques, bases de données, conception et sécurité, etc.
- 3) Sécurité Web
- 4) Réseaux, systèmes et programmation web au service de la cybersécurité
- 5) Sécurité des réseaux et des systèmes d'information
- 6) Cryptographie
- 7) Forensics
- 8) L'algorithmique et la programmation à l'épreuve de la cybercriminalité
- 9) Reverse Engineering
- 10) Reconnaissance
- 11) Audit de cybersécurité

Toute personne intéressée peut soumettre une proposition de communication sur l'un des sous-thèmes du Colloque. Les propositions de communications doivent être envoyées simultanément aux adresses : guymvellecybersec2021@gmail.com ; comitecybersec2021@gmail.com; au plus tard le **28 février 2021 à 12 heures GMT**.

Chaque **proposition de communication** devra comprendre :

- Les noms, prénoms, grade et institution de rattachement de l'auteur ;
- L'axe thématique et sous-thème choisis ;
- Le titre de la communication ;
- Un résumé d'environ 250 mots ;
- Un exposé de quelques lignes précisant les hypothèses de travail, la problématique, la méthodologie d'investigation, l'approche théorique préconisée et les résultats escomptés.

Dès notification de l'acceptation de la proposition de communication, l'auteur rédigera et enverra le texte intégral au plus tard le **30 mars 2021 à 12 heures GMT** simultanément aux adresses : guymvellecybersec2021@gmail.com ; comitecybersec2021@gmail.com

Le texte de la communication ne doit pas dépasser 25 pages (Garamond 12, interligne 1,5, références et commentaires en notes de bas de pages). Le texte suivra la structure dialectique avec une introduction générale, un corps de devoir bipartite et une conclusion générale. Il comportera également un résumé d'environ 250 mots, des mots clés et une bibliographie indicative.

Chaque communicateur transmettra au plus tard le **30 mai 2021** le texte finalisé de sa communication ayant tenu compte des débats et éventuelles observations du Comité scientifique si toutefois, il souhaite sa publication. Après avis du Comité scientifique, les textes des communications présélectionnées feront l'objet d'une publication sous la forme d'un ouvrage collectif.

DATE	ACTIVITE
10 janvier 2021	Lancement de l'appel à communications
28 février 2021	Date limite d'envoi des propositions de communication
15 mars 2021	Sélection des propositions et notification aux auteurs
30 mars 2021	Date limite d'envoi des communications
01 au 15 avril 2021	Inscription au Colloque
06 au 07 mai 2021	Tenue du colloque

05

LANGUES DU COLLOQUE

FRA

Français



Anglais

ENG

06

PROFIL DES CONTRIBUTEURS



Les contributeurs pourront être des enseignants-chercheurs et/ou des chercheurs ayant au moins le grade de docteur ; soit des professionnels s'intéressant à la cybersécurité. Pourront aussi contribuer des auditeurs ou des doctorants.

07

PROFIL DES PARTICIPANTS



Il s'agit des universitaires, des chercheurs, des professionnels, des étudiants, des décideurs publics, les chefs d'entreprises : autorités locales, préfectorales et centrales ; des acteurs de la société civile, des leaders de partis politiques et autres.

08

LIEUX DU COLLOQUE

Université de Dschang
à Yaoundé



Université de Dschang à
Dschang

09

SUPERVISEUR GENERAL



ROGER PEPIN TSAFACK NANFOSSO

Professeur, Recteur de l'Université de Dschang

SUPERVISEURS GENERAUX-ADJOINTS

HENRI DESIRE MODI KOKO BEBEY

Professeur, Doyen, FSJP, UDs

THOMAS TAMO TATSIETE

Professeur, Directeur de l'IUT-FV de Bandjoun

DIRECTION SCIENTIFIQUE

GUY MVELLE

*Professeur, Département de Science Politique,
Secrétaire général de l'Université de Dschang,
Directeur*

CLEMENTIN TAYOU DJAMENYI

*Chef de Département de génie informatique,
IUT-FV, Directeur Adjoint*

MEMBRES DU COMITE SCIENTIFIQUE



JEAN NJOYA

Professeur, Vice-Recteur EPTIC, Université de Dschang



ALEXIS NGATCHOU

Professeur, CT, Université de Dschang



SERGE HILAIRE DE PRINCE POKAM

Professeur, Chef de Département de science politique, Université de Dschang



JOSEPH KEUTCHEU

Maître de Conférences, Vice-Doyen FSJP, Université de Dschang



ANDRE TCHOUIPIE

Professeur, Université de Dschang



YVETTE RACHEL KALIEU ELONGO

Professeur, Vice-Doyen, FSJP-UDs



ALAWADI ZELAO

Chargé de Cours, Vice-Doyen, FSJP



RENÉ NJEUFACK TEMGWA

Maître de Conférences, Chef de Département de droit privé fondamental, FSJP-UDs



LÉOPOLD ISIDORE MIENDJEM

Professeur, Chef de Département, FSJP-UDs



PHILIPPE KEUBOU

Maître de Conférences, Chef de département de Droit pénal et sciences criminelles



EDOUARD GNIMPIEBA TONNANG

Professeur, Chef de Département, FSJP-UDs



MARCELLIN NKENLINFACK

Maître de Conférences, FS-UDs



THIERRY NOULAMO

Chargé de Cours, IUT-FV-UDs



BERNARD FOTSING TALLA

Chargé de Cours, IUT-FV-UDs



ERIC FOTSING

Chargé de Cours, IUT-FV-UD

MEMBRES DU COMITE D'ORGANISATION



Eric Bertrand LEKINI

Assistant, Département de Science politique, Université de Dschang



Carine KAMNO

Assistant, Département de Science politique, Université de Dschang

MEMBRES DU COMITE D'ORGANISATION



Georges Macaire EYENGA

Assistant, Département de Science politique, Université de Dschang



Max Synclair MBIDA ONAMBELE

Chargé de Cours, Département Sciences politiques, Université de Dschang



Gaetan OMBGA MIMBOE

Chargé de Cours, Département Sciences politiques, Université de Dschang



Jean Pierre LIENOU

Chargé de Cours, IUT-FV-UDs



Narcisse TALLA TANKAM

Chargé de Cours, IUT-FV-UDs



Guilène MPAME

Chargée de Cours, IUT-FV-UDs



Miguel Landry FOKO SINDJOUNG

Chargé de Cours, IUT-FV-UDs



Maurice TCHOUPE

Chargé de Cours, IUT-FV-UDs



Vianney KENGNE

Chargé de Cours, FS-UDs

10

BIBLIOGRAPHIE

ABY, Romain (2020), « Cybersécurité et contrôle de la région », in BADIE, Bertrand (dir), *Le Moyen-Orient et le monde. L'état du monde 2021*. La Découverte, 2020, pp. 239-245.

ARPAGIAN, Nicolas (2017), « Cyberguerre : longtemps annoncée, désormais réalité ? Une nouvelle forme de la guerre moderne », in DE MONTBRIAL, Thierry (dir), *La guerre de l'information aura-t-elle lieu ? Ramses 2018*. Institut français des relations internationales, pp. 156-161.

ARPAGIAN, Nicolas (2018), *La cybersécurité*. Presses Universitaires de France

BOGUI, Jean-Jacques (2010), « La cybercriminalité, menace pour le développement. Les escroqueries Internet en Côte d'Ivoire », *Afrique contemporaine*, vol. 234, no. 2, pp. 155-170.

BOULANGER, Philippe (2014), « Le cyberespace, nouvel espace de rivalités », *Géopolitique des médias. Acteurs, rivalités et conflits*, Armand Colin, pp. 263-294.

- CASSUTO, Thomas (2018), « Nouvelles perspectives dans la lutte contre la cybercriminalité », *Sécurité globale*, vol. 15, no. 3, pp. 29-35.
- CATTARUZZA, Amaël (2018), « La construction politique de l'espace numérique. Penser l'espace numérique comme un espace stratégique », in TAILLAT, Stéphane (dir) éd., *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, pp. 19-25.
- CATTARUZZA, Amaël (2019), « De la guerre à la cyberguerre ? », *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data*, Le Cavalier Bleu, pp. 115-125.
- CATTARUZZA, Amaël, et BUISSON, Jérémy(2018), « La dimension sociale du combat cybernétique. La dimension sociotechnique du cyberspace », in TAILLAT Stéphane éd., *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, pp. 35-43.
- CUKIERMAN, Edouard, et ROUACH, Daniel (2018), « Le futur des technologies en Israël », *Israël Valley. Le bouclier technologique de l'innovation*, EMS Editions, 2018, pp. 157-175.
- D'ELIA, Danilo (2015), « La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine », *Sécurité et stratégie*, vol. 19, no. 2, pp. 72-80.
- DANET, Didier, et DESFORGES Alix (2020), « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, vol. 177-178, no. 2-3, pp. 179-195.
- DAVID, Dominique (2017), « Un nouveau jeu de puissance ? Vieux et neuf à la fois », DE MONTBRIAL Thierry éd., *La guerre de l'information aura-t-elle lieu ? Ramses 2018*. Institut français des relations internationales, pp. 48-53.
- DELERUE, François, et AUDE, Géry (2018). « Les aspects juridique et stratégique de la cyberdéfense. Le droit international et la cyberdéfense », in TAILLAT Stéphane (dir), *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, pp. 61-70.
- DELESSE, Claude (2016), NSA National Security Agency. *L'histoire de la plus secrète des agences de renseignement*, Tallandier.
- DOUZET, Frédéric (2020), « Éditorial. Du cyberspace à la datasphère. Enjeux stratégiques de la révolution numérique », *Hérodote*, vol. 177-178, no. 2-3, pp. 3-15.
- DOUZET, Frédéric, et GERY Aude (2020), « Le cyberspace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberspace », *Hérodote*, vol. 177-178, no. 2-3, pp. 329-350.
- DUCRUET, César (2017), « Le système technicoéconomico-planétaire peut-il résister au choc ? Un réseau concentré, complexe et vulnérable », in DE MONTBRIAL, Thierry (dir), *La guerre de l'information aura-t-elle lieu ? Ramses 2018*. Institut français des relations internationales, pp. 84-89.

- HADDAD, Saïd (2017), « Une grammaire de la cybersécurité française ou la construction d'une stratégie nationale de cyberdéfense (2008-2017) », *Stratégique*, vol. 117, no. 4, pp. 119-135.
- HADDAD, Saïd (2018), « Le cyberspace ou la construction d'un « champ de confrontation à part entière » », in TAILLAT, Stéphane (dir), *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, pp. 44-51.
- HENROTIN, Joseph (2018), « Cyberdéfense : une généalogie », in TAILLAT Stéphane (dir), *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, pp. 71-77.
- KEMPE, Olivier (2017), « Des différences entre la cybersécurité et la transformation digitale », *Stratégique*, vol. 117, no. 4, pp. 59-64.
- LAVOIX, Hélène (2019), « Revisiter l'idée de cybersécurité pour le monde digital du 21e siècle », *Sécurité globale*, vol. 19, no. 3, pp. 27-32.
- MASSIT-FOLLEA, Françoise (2017), « De l'utopie internet aux défis d'un monde numérisé. Information et connaissance, liberté individuelle et vivre ensemble », in DE MONTBRIAL, Thierry (dir), *La guerre de l'information aura-t-elle lieu ?* Ramses 2018. Institut français des relations internationales, pp. 144-149.
- MOREAU DEFARGES, Philippe (2017), « Démocraties, États, peuples en crises ? La démocratie change d'échelle », in DE MONTBRIAL, Thierry (dir), *La guerre de l'information aura-t-elle lieu ?* Ramses 2018. Institut français des relations internationales, pp. 80-83.
- MOREAU DEFARGES, Philippe (2017), « Un changement de temps. La scène internationale peut-elle se déconstruire ? », DE MONTBRIAL Thierry (dir), *La guerre de l'information aura-t-elle lieu ?* Ramses 2018. Institut français des relations internationales, pp. 42-47.
- NOCETTI, Julien (2017), « Comment l'information recompose les relations internationales. La faute à Internet ? », in DE MONTBRIAL, Thierry (dir), *La guerre de l'information aura-t-elle lieu ?* Ramses 2018. Institut français des relations internationales, pp. 138-143.
- NOCETTI, Julien (2017), « La diplomatie à l'heure du numérique. De la diplomatie numérique à la diplomatie du numérique », in DE MONTBRIAL, Thierry (dir), *La guerre de l'information aura-t-elle lieu ?* Ramses 2018. Institut français des relations internationales, pp. 150-155.
- QUEMENER, Myriam (2018), « Pour une lutte plus efficace contre la cybercriminalité », *Sécurité globale*, vol. 15, no. 3, pp. 5-16.
- SUDRES, Arnaud (2017), « Cyberspace et dimension stratégique de la force informatique », *Stratégique*, vol. 117, no. 4, pp. 65-82.

- TAILLAT, Stéphane (2017), « L'impact du numérique sur les relations stratégiques internationales », *Stratégie*, vol. 117, no. 4, pp. 137-153.
- TAILLAT, Stéphane (2018), « Le cyberspace et la conflictualité internationale », *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, pp. 26-33.
- TAILLAT, Stéphane, CATTARUZZA, Amaël, et DANET, Didier (2018), *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin.
- TEPI, Samuel (2020), *la cybercriminalité au Cameroun : enjeux d'une législation en quête d'efficacité*, harmattan, paris.
- VENTRE, Daniel (2015), « Cyberstratégie », Stéphane Taillat éd., *Guerre et stratégie*. Presses Universitaires de France, pp. 333-348.
- WALSH, Isabelle, KALIKA, Michel, et DOMINGUEZ-PERY (2018), Carine, *Les Grands Auteurs en Systèmes d'information*. EMS Editions, 2018
- WEBER, Claude, et COMMANDANT, Jean-Philippe (2018), « De l'importance du facteur humain », in TAILLAT Stéphane (dir.), *La Cyberdéfense. Politique de l'espace numérique*. Armand Colin, pp. 52-59.
- YOGO, Edouard, Épiphanie (2015), *la cybersécurité et la cyberdéfense au Cameroun : problèmes juridiques, politique et stratégiques*, Acte du colloque, Yaoundé, CAESS, Afrédit,

