Council for the Development of Social Science Research in Africa
Conseil pour le développement de la recherche en sciences sociales en Afrique
Conselho para o Desenvolvimento da Pesquisa em Ciências Sociais em África
مجلس تنمية البحوث الإجتماعية في أفريقيا

CODESRIA

SERIES DES BIBLIOGRAPHIES DU CODICE

CODICE BIBLIOGRAPHIES SERIES

2016

Training, Grants and Fellowships Programme
Programme Formation, bourses et subventions

GOVERNANCE INSTITUTE / INSTITUT SUR LA GOUVERNANCE

BIBLIOGRAPHY / BIBLIOGRAPHIE

On / sur:

THE AFRICAN STATE AND PUBLIC CYBER-SECURITY SERVICE

L'ETAT AFRICAIN ET LE SERVICE PUBLIC DE LA CYBERSECURITE

Dakar, Sénégal / Senegal, 21/11 - 02/12, 2016

CODESRIA,
BP 3304, CP 18524, Dakar, Sénégal.
Tel.: +221-33 825 98.22/23 - 221 33 864 12 63 - Fax: +221-33 824 12.89
E-mail: codesria@codesria.sn
Site Web: http://www.codesria.org/
Facebook: http://www.facebook.com/pages/CODESRIA/181817969495Twitter:
http://twitter.com/codesria

Table of Contents / Table des matières

INTRODUCTION

The CODESRIA Democratic Governance Institute, which was launched in 1992, is an annual interdisciplinary forum which brings together about ten researchers from various regions of the continent and the diaspora as well as a few non-African researchers conducting innovative research on topics related to the general topic of governance.

The 2016 Democratic Governance Institute topic is : "The African State and public cyber-security service "

"The 2015 Democratic Governance Institute session's topic was "Cyber-Security, Sovereignty and Democratic Governance in Africa". Among its recommendations was the need to deepen understanding on the theme of cyber-security by holding a second session. Thus the topic of the 2016 Institute is: "The African State and Public Cyber-Security Service".
In an environment marked by growing insecurity, a widening digital gap at the expense of Africa, which, just like poverty, is becoming commonplace, the continent has not yet benefitted from all the advantages of the digital era but rather, undergoes more than anywhere else in the world its adverse effects. The collective work of the 2015 session researchers has enabled the study of cases that illustrate that democratic cyber-governance is at work; cyber-citizenship is under construction; Africa is starting to develop responses to cyber-threats and is aware of the need for building a prospective vision of cyber-security governance".

In this framework, the CODESRIA Documentation, Information and Communication Centre (CODICE) has compiled this bibliography. Various sources of bibliographic data have been used among which the CODESRIA data bases.

The bibliography is in two sections; the first section lists the documents in hard copy and the second, the documents in electronic format. Classified alphabetically by author, the selected references are either in French or in English.

The Call for application for the Democratic Governance Institute is in the annex of this bibliography.

We hope that this bibliography will be useful, and suggestions for its improvement are welcome.
Have a fruitful Institute.

L'Institut sur la gouvernance démocratique lancé en 1992 par le CODESRIA est un forum interdisciplinaire qui réunit chaque année une dizaine de chercheurs provenant des diverses régions du continent et de la diaspora, ainsi que quelques chercheurs non africains qui entreprennent des recherches innovantes sur des sujets liés au thème général de la gouvernance.

L'Institut sur la Gouvernance 2016 porte sur : « L'Etat africain et le service public de la cybersécurité »

« La session 2015 de l'Institut sur la gouvernance démocratique a été consacrée au thème « Cybersécurité, souveraineté et gouvernance démocratique en Afrique ». Elle a formulé, entre autres recommandations, la nécessité d'approfondir la thématique de la cybersécurité à travers notamment l'organisation d'une seconde session de l'Institut sur le thème : « l'Etat africain et le service public de la cybersécurité ».
Dans un environnement marqué par une insécurité grandissante, la fracture numérique se creuse au détriment de l'Afrique en se banalisant, à l'instar de la pauvreté. Le continent ne profite pas encore de tous les avantages du numérique mais en subit, plus que tous, les travers. La réflexion collective des chercheurs de la session 2015 a permis d'étudier des cas qui illustrent que la cybergouvernance démocratique est en marche, que la cybercitoyenneté est en construction, que l'Afrique commence à ébaucher des réponses face aux cybermenaces et qu'elle est consciente de la nécessité de construire une vision prospective de la gouvernance de la cybersécurité ».

Dans cette perspective, le centre de documentation, d'information et de communication du CODESRIA (CODICE) a élaboré cette bibliographie. Á cet effet, différentes sources d'information bibliographique ont été utilisées parmi lesquelles les bases de données du CODESRIA.

Cette bibliographie est divisée en deux parties, une première partie regroupant les documents en format papier et une deuxième réunissant les documents en format électronique. Les références sélectionnées sont classées alphabétiquement par auteur et sont soit en anglais soit en français.

L'appel à contributions lancé pour les besoins de l'institut sur la gouvernance démocratique est annexé à la présente bibliographie.

Nous espérons que cette bibliographie vous sera utile et le CODICE est à l'écoute de toutes suggestions permettant son éventuel enrichissement.
Bon institut.

CODESRIA Documentation, Information and Communication Centre
Centre de documentation, d'information et de communication du CODESRIA (CODICE)

PART I / 1ère PARTIE

DOCUMENTS IN HARD COPY

DOCUMENTS PAPIERS

I – Documents in Hard Copy / Documents papiers

1. **AGOSTINELLI, Serge; AUGEY, Dominique; LAURIE, Frédéric**

Entre communautés et mobilité: une approche interdisciplinaire des médias
Paris : Presses des Mines, 2011. - 202 p.
(Collection Économie et gestion, ISSN 2101-3241)
ISBN : 978-2-911256-43-1
(New acquisition)

2. **ANCEL, Marie-Elodie ; BEKERMAN, Gérard ; BERTRAND, André René, et al.**

Droit et technique : études à la mémoire du professeur Xavier Linant de Bellefonds
Paris: LexisNexis : Litec, 2007. - XVIII-474 p.
ISBN : 978-2-7110-0641-0
(New acquisition)

3. **ARPAGIAN, Nicolas**

L'État, la peur et le citoyen: du sentiment d'insécurité à la marchandisation des risques
Paris : INHESJ : Vuibert, 2010. - 213 p.
ISBN : 978-2-7117-6883-7
(New acquisition)

4. **ARPAGIAN, Nicolas, Dir.**

Liberté, égalité... sécurité
Paris : Dalloz, 2007. - 252 p.
ISBN : 978-2-247-07268-2
(New acquisition)

5. **ARPAGIAN, Nicolas ; DELBECQUE, Éric**

Pour une stratégie globale de sécurité nationale
Paris: Dalloz, 2008. - 306 p.
ISBN : 978-2-247-07699-4
(New acquisition)

6. **AUZON, Olivier d'**

Les droits des internautes à l'ère de l'économie numérique
Héricy: Éditions du Puits Fleuri, 2009. - 391 p.
(Le Conseiller juridique pour tous, ISSN 0414-6492 ; 257)
ISBN : 978-2-86739-398-3
(New acquisition)

7. **BA, Abdoul**

Internet, cyberespace et usages en Afrique
Paris: L'Harmattan , . – 281 p., 22 cm
ISBN : 2747544117

Subject(s) : *Internet -- Liberté d'expression --Commerce --Démocratie --Mondialisation --Infrastructure des communications --Développement économique et social – Cyberespace --TIC --Commerce électronique --Liberté de la presse -- Afrique*
Call N°: 08.16.01/BAA/13017

8. BAKARY, Tessy; DE, Maïmouna
Cyber politique@Sunugal.net: Internet comme espace de production du politique et de décision électorale au Sénégal
Colloque sur des élections présidentielles du 27 février 2000 au Sénégal -- Dakar -- SN -- 19-21 juillet
Dakar: CODESRIA, 2000. – 39 p. 30cm

Subject(s) : *Démocratisation --Politique --Enquêtes --Chefs d'Etat – Elections- - Transitions politiques --Changement politique --Nouvelles technologies de l'information -- Sénégal*
Call N°: CD-12192

9. BART, François; LENOBLE-BART, Annie, Ed.
Afrique des réseaux et mondialisation
Paris: Karthala, 2003.- 204 p.
ISBN: 2-84586-390-X

Subjects : *Réseaux--Mondialisation -- Relations internationales -- Organisations féminines -- Minorités ethniques— Tourisme -- Réseaux informatiques --Afrique -- Réseaux ethno-culturels -- Réseaux sociaux -- Réseaux transnationaux -- Réseaux électroniques*
Call N°: 08.16.01/BAR/14110

10. BENSOUSSAN, Alain
Informatique, télécoms, Internet: réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques
5e édition.
Levallois : F. Lefebvre, 2012. - 1103 p.
ISBN 978-2-85115-954-0
(New acquisition)

11. BOLLE, Pierre-Henri ; CASORLA, Francis ; LAMY, Bertrand de, et al.
Le droit pénal à l'aube du troisième millénaire: mélanges offerts à Jean Pradel
Paris : Éditions Cujas, 2006. - 1159 p.
ISBN : 2-254-06411-8
(New acquisition)

12. BOYER, Bertrand
Cyberstratégie, l'art de la guerre numérique
Paris : Nuvis, 2012. – 238 p.
(Collection La pensée stratégique)
ISBN: 978-2-36367-013-7 / ISBN 2-36367-013-2
(New acquisition)

13. BRYDEN, Alan; FLURI, Philipp, Ed.
Security Sector Reform: Institutions, Society and Good Governance
Baden-Baden Nomos Verlagsgesellschaft , . – 327 p.
ISBN: 383 2 903801

Subject(s): *Defence --Society --Governance --Terrorism --Crime --Democracy --Parliament --Police --Military Personnel-- Security Reform --Good Governance --Cybercrime*
Call N°: 01.02.06/BRY/14678

14. BRZEZINSKI, Zbigniew
Between Two Ages: America's Role in the Technetronic Era

New York: Viking Press, 1970. – xvii-334 p.
ISBN 0670160415 / ISBN 9780670160419
ISBN 0140043144 / ISBN 9780140043143
(New acquisition)

15. CALDERAN, Lisette ; HIDOINE, Bernard ; MILLET, Jacques, Dir.
L'usager numérique
Paris : ADBS éditions, 2010. - 203 p.
Séminaire INRIA, 27 septembre-1er octobre 2010, Anglet ; organisé par l'Institut national de recherche en informatique et en automatique
(Sciences et techniques de l'information, ISSN 1762-8288)
ISBN : 978-2-84365-126-7
(New acquisition)

16. CAPRIOLI, Éric A.
Droit international de l'économie numérique: les problèmes juridiques liés à l'internationalisation de l'économie numérique
2e édition
Paris : Litec, 2007. - xiv-369 p. (Pratique professionnelle, procédure)
ISBN : 978-2-7110-0774-5
(New acquisition)

17. CASTELLS, Manuel
L'ère de l'information. La société en réseaux
Paris: Fayard, 2001. - 671 p.
Trad. de: The Rise of the Network Society
ISBN : 978-2-213-60845-7 / ISBN : 2-213-60845-8
(New acquisition)

18. CASTETS-RENARD, Céline
Droit de l'Internet: droit français et européen 2e édition,
Paris : Montchrétien Montchrestien-Lextenso éditions, 2012. - viii-490 p. (Collection Cours, ISSN 1954-0450)
ISBN : 978-2-7076-1817-7
(New acquisition)

19. CHATELAIN, Yannick; ROCHE, Loïck
Marketing et cybercriminalité
Paris : Hèrmes Science, 2000. - 155 p.
ISBN: 2-7462-0174-7
(New acquisition)

20. CLOUGH, Jonathan
Principles of cybercrime
Cambridge: Cambridge University Press, 2010. - liii-449 p.
ISBN: 978-0-521-89925-3 / ISBN: 0-521-89925-7
(New acquisition)

21. CONSEIL D'ETAT, France
Étude annuelle 2014: le numérique et les droits fondamentaux : rapport adopté par l'assemblée générale du Conseil d'État le 17 juillet 2014
Paris : la Documentation française, 2014. - 441 p.

(Etudes et documents - Conseil d'Etat, ISSN 0182-788X ; 65) N° de : "Les Rapports du Conseil d'État", 2014, n°65
ISBN : 978-2-11-009765-1
(New acquisition)

22. DELBECQUE, Eric
La métamorphose du pouvoir: la chance des civilisations
Paris : Vuibert, 2009. - 329 p.
ISBN : 978-2-7117-6892-9
(New acquisition)

23. EBO, Bosah
Cyberimperialism? : Global Relations in the New Electronic Frontier
London: Praeger , . - X-260p.
ISBN: 0275965627

Subject(s): *Information Technology --Development Countries --Developing Countries --Theory --Sustainable Development --Cultural Identity – Africa*
Call N°: 08.16.01/EBO/13477

24. FAUCHOUX, Vincent ; DEPREZ, Pierre
Le droit de l'Internet. Lois, contrats et usages
2e édition
Paris : LexisNexis, 2013. - XIII-445 p.
ISBN : 978-2-7110-1713-3
(New acquisition)

25. FERAL-SCHUHL, Cristiane Cyberdroit
Le droit à l'épreuve de l'Internet
6e édition
Paris : Dalloz, 2010. - XXII-1100 p. (Praxis Dalloz)
ISBN : 978-2-247-10120-7
(New acquisition)

26. FEVRIER, Rémy
Les collectivités territoriales face à la cybercriminalité : les responsabilités des élus locaux, l impact sur les citoyens, les méthodes pour protéger son système d'information
Paris: Eska, 2014. – 312 p.
ISBN: 9782747222952 / ISBN: 2747222950
(New acquisition)

27. FORTIN, Francis, Dir.
Cybercriminalité: entre inconduite et crime organisé
Québec : Presses internationales polytechnique, 2013. - XVII-366 p.
ISBN : 978-2-553-01647-9
(New acquisition)

28. FRANCHIN, Franck ; MONNET, Rodolphe
Le business de la cybercriminalité
Paris : Hermès science : Lavoisier, 2005. – iii-205 p
ISBN : 2-7462-1054-1
(New acquisition)

29. FREYSSINET, Eric
La cybercriminalité en mouvement
Paris: Hermès Science ; Cachan : Lavoisier, 2012. - 226 p.
ISBN: 978-2-7462-3288-4
(New acquisition)

30. GEORGE, Eric; GRANJON, Fabien, Dir.
Critiques de la société de l'information
Paris : L'Harmattan, 2008. - 264 p.
ISBN : 978-2-296-07031-8
(New acquisition)

31. GIROT, Jean-Luc
Le harcèlement numérique
Paris: Dalloz, 2005. - 271 p.
ISBN: 2-247-06195-8
(New acquisition)

32. GRAGIDO, Will; PIRC, John
Cybercrime and Espionage: An Analysis of Subversive Multivector Threats Rockland (Mass.): Syngress, 2011. - xv-254 p.
ISBN: 978-1-59749-613-1
(New acquisition)

33. GRYNBAUM, Luc; LE GOFFIC, Caroline; MORLET, Lydia
Droit des activités numériques Paris : Dalloz, 2014. - xi-1040 p.
ISBN : 978-2-247-07607-9
(New acquisition)

34. GUISNEL, J.
La guerre dans le cyberespace
Paris : La Découverte, 1999
(New acquisition)

35. HAAS, Gérard; COHEN-HADRIA, Yaël, Dir.
Guide juridique informatique et libertés: collecte, traitement et sécurité des données dans l'univers numérique : ce que vous devez savoir
St-Herblain: Éditions ENI, 2012. - 230 p.
(New acquisition)

36. HOLLANDE, Alain ; LINANT DE BELLEFONDS, Xavier
Pratique du droit de l'informatique : logiciels, systèmes, Internet
6e édition
Paris : Delmas, 2008. - 480 p.
ISBN : 978-2-247-06642-1
(New acquisition)

37. HUET, Jérôme ; DREYER, Emmanuel
Droit de la communication numérique
Paris : LGDJ : Lextenso éd., 2011. - 376 p.
ISBN : 978-2-275-03490-4
(New acquisition)

38. Internet sans danger: le guide du bon sens numérique
Montrouge: Bayard, 2013. - 143 p.
ISBN: 978-2-227-48633-1
(New acquisition)

39. JABER, Abbas
Les infractions commises sur Internet
Paris : L'Harmattan, 2009.- 314 p.
Thèse de doctorat, Droit privé, Dijon, 2007
ISBN: 978-2-296-09618-9
(New acquisition)

40. JAGODZINSKI, Jan
Youth Fantasies: the Perverse Landscape of the Media
New York: Palgrave Macmillan, 2004.- ix-281 p.
ISBN: 1-4039-6165-4

Subject (s): *Youth – Media – Games -- Video Game -- Cyberspace*
Call N° : 14.02.02/JAG/13388

41. JAKOBSSON, Markus ; RAMZAN, Zulfikar
Crimeware: Understanding New Attacks and Defenses Upper Saddle River,
NJ: Addison-Wesley, 2008. - xxi-582 p.
ISBN : 978-0-321-50195-0 / ISBN : 0-321-50195-0
(New acquisition)

42. JAUREGUIBERRY, Francis; PROUX, Serge, Ed.
Internet, nouvel espace citoyen ?
Paris : L'Harmattan , 2003. - 249 p.
ISBN274753443X

Subject(s) : *Moyens de communication --Mondialisation --Démocratie --Socialisation – Cyberespace --Démocratie électronique --Fracture numérique --Site web*
Call N°: 08.16.01/JAU/13870

43. JENKINS, Henry; THORBURN, David, Ed.
Democracy and New Media
Cambridge: The MIT Presse, . - X-385 p.
ISBN: 0262101017

Subject(s) : *Media --Information Technology --Internet --Elections --Voting --Journalism --Access to Information -- Democracy --Engineering Communications --Political Aspects --Information Society – - Cyberspace --Citizenship -- Cyber-democracy --Digitalization --Political culture - - Africa*
Call N°: 04/JEN/13013)

44. JORDAN, Tim
Hacking: Digital Media and Technological Determinism
Cambridge : Polity Press, 2008. - vi-160 p.
ISBN: 978-0-7456-3972-7
(New acquisition)

45. KHOURI, Nicole
La Politique antiterroriste de l'Etat Egyptien à la télévision en 1994
Revue Tiers-Monde, T. XXXVII, N°146, 1996, p. 263-283

Subject(s) : *Terrorisme --Paix -- Influence sociale --Télévision --Stabilité politique --Propagande --Etat - Egypte*

46. KOOPS, Bert-Jaap; BRENNER, Susan W., Ed.
Cybercrime and Jurisdiction: A Global Survey
The Hague: TMC Asser Press, 2006. - xvii-355 p.
ISBN : 978-90-6704-221-5 / ISBN : 90-6704-221-8
(New acquisition)

47. KOUTOUMA NSONA, Raïssa Edwige Macha
Les Internautes et les Cybercafés à Brazzaville
Brazzaville: Université Marien Ngouabi , 2005. – 76 p. 30 cm
Mémoire Maîtrise ès Lettres Université Marien Ngouabi, Faculté des Lettres et des Sciences Humaines, Département des Sciences et Techniques de la Communication.

Subject(s): *Implications sociales --Organisations internationales --Société civile – internautes --Cybercafes -- Utilisation de l'Internet - - Congo - - Brazzaville*
Call N°: 08.16.01/KOU/12961

48. LESSIG, Lawrence
L'avenir des idées: le sort des biens communs à l'heure des réseaux numériques
Lyon : Presses universitaires de Lyon, 2005. - XVII-414 p.
ISBN : 2-7297-0772-7
(New acquisition)

49. LEVY, Alain
Sur les traces de Big brother: la vie privée à l'ère numérique : document
Paris : l'Éditeur, 2010. - 262 p.
ISBN : 978-2-36201-017-0
(New acquisition)

50. LEVY, Pierre
Qu'est-ce que le virtuel ?
Paris : La Découverte, 1998. - 153 p.
ISBN : 2-7071-2835-X
(New acquisition)

51. LIANG, Qiao; XIANGSUI, Wang
La Guerre hors limites
Paris : Payot & Rivages, 2014. - 309 p.
ISBN: 2-7436-1517-6 / ISBN: 978-2-7481-1517-8
(New acquisition)

52. LIBICKI, Martin C.
Conquest in Cyberspace: National Security and Information Warfare
Cambridge, Cambridge University Press, 2007. - XII-323 p.
ISBN: 978-0-521-87160-0
(New acquisition)

53. LIBICKI, Martin C.
Cyberdeterrence and Cyberwar
Santa Monica (CA): Rand Corporation, 2009. - xxiv-214 p.
ISBN: 978-0-8330-4734-2 / ISBN: 0-8330-4734-5
(New acquisition)

54. LUCIANI-BOYER, Pascale
L'élu(e) face au numérique : de la puissance publique à la puissance citoyenne, un défi majeur des territoires
Paris: Berger-Levrault, 2015. - 284 p.
ISBN: 978-2-7013-1837-0
(New acquisition)

55. LVI-FAUR, David, Ed
Handbook on the Politics of Regulation
Cheltenham: Edward Elgar, 2011.- xvii-695 p.
ISBN: 978-1-84844-005-0

Subject (s): *Regulations – Politics – Governance – State – Law – Media – Advertising – Internet – Risk-- Environment – Manuals -- Regulation Theory -- Civil Regulation -- Global Regulation*
Call N°: 04.01.01/LEV/15766

56. MAKINDA, Samuel M.; OKUMU, F. Wafula
The African Union: Challenges of Globalization, Security, and Governance
London: Routledge, 2008. - XVII-209 p.

Subject(s) : *OAU --Peaceful Coexistence --Science and Technology --Globalization --Governance --Democracy -- Corruption -- African Union --Security -- Africa*
Call N°: 01.03.03/MAK/14640

57. MALABAT, Valérie ; DE LAMY, Bertrand ; GIACOPELLI, Muriel, Dir.
La réforme du Code pénal et du code de procédure pénale. Opinio doctorum
Paris, Dalloz, 2009. - xii-409 p.
ISBN : 978-2-247-08587-3
(New acquisition)

58. MALLET, Jean-Claude, Dir.
Défense et sécurité nationale : le livre blanc
Paris : La Documentation française, 2008. - 350 p.
ISBN : 978-2-7381-2185-1
(New acquisition)

59. MAUSHART, Susan
Pause: comment trois ados hyperconnectés et leur mère (qui dormait avec son smartphone) ont survécu à six mois sans le moindre média électronique
Paris: Marabout, 2014. - 441 p.
ISBN : 978-2-501-09057-5
(New acquisition)

60. MCQUADE III, Samuel C.
Encyclopedia of Cybercrime
Westport: Greenwood Press, 2009. - XXIII-210 p.
(New acquisition)

61. MISURACA, Gianluca C.
E-governance in Africa, from Theory to Action: a Handbook on ICTs for Local Governance
Ottawa: IDRC, 2007.- xix-313 p.
ISBN: 1-59221-579-3

Subject (s): *Internet – Public Administration – Governance – Information Technology - - Communication Engineering – Decentralization -- Local Government – Africa -- E- Governance -- E-Government -- Good Governance*
Call N°: 18.16.01/MIS/14266

62. NORODOM, Anne-Thida ; GODON, Alain
Internet et le droit international.
Paris: A. Pedone, 2014. 497 p.
ISBN: 9782233007209 / ISBN: 2233007204
(New acquisition)

63. PAILLARD, Laurent
La gratuité intellectuelle: pour une véritable révolution numérique
Lyon : Parangon : la Vie est à nous, 2013. - 163 p.
ISBN : 978-2-8419-0227-9
(New acquisition)

64. PEDROT, Philippe, Dir.
Traçabilité et responsabilité
Paris: Economica, 2003. - X-323 p.
ISBN: 2-7178-4597-6 / ISBN: 978-2-7178-4597-6
(New acquisition)

65. PERRIAULT, Jacques; VAGUER, Céline, Dir.
La norme numérique: savoir en ligne et Internet
Paris : CNRS éd., 2010. - 264 p.
ISBN: 978-2-271-07101-9
(New acquisition)

66. PEUGEOT, Valérie; AMBROSI, Alain; KOLE, Ellen; LOHENTO, Ken; DUMOLIN, Benoît; PIMIENTA, Daniel, Ed.
Réseaux humains, réseaux électroniques : de nouveaux espaces pour l'action collective
Paris: Editions Charles Léopold Mayer, 2001.- 262 p.
ISBN: 2-84377-054-8

Subject (s) : *Internet - - Réseaux - - Technologie de l'information - - Technologie des communications - - Politique - - Afrique - - Amérique du Nord - - Europe - -Réseaux Humains - - Réseaux Electroniques - - TIC*
Call N° : 08.16.01/PEU/14123

67. POLLET, Delphine, Dir.
Circuler dans la société numérique: droits et limites
Paris: L'Harmattan, 2013. - 165 p.
ISBN 978-2-343-01438-8
(New acquisition)

68. PRZYSWA, Éric
Cybercriminalité et contrefaçon
Paris: Éditions Fyp, 2010. - 199 p.
ISBN 978-2-916571-47-8 / ISBN 2-916571-47-7
(New acquisition)

69. QUEMENER, Myriam
Cybermenaces, entreprises et internautes
Paris: Economica, 2008. - X-264 p.
ISBN: 978-2-7178-5642-2
(New acquisition)

70. QUEMENER, Myriam; FERRY, Joël
Cybercriminalité: défi mondial
2e édition.
Paris : Economica, 2009. - VIII-308 p.
ISBN: 978-2-7178-5700-9
(New acquisition)

71. QUEMENER, Myriam ; CHARPENEL, Yves
Cybercriminalité : droit pénal appliqué
Paris: Economica, 2010. - 273 p.
(Collection Pratique du droit ; ISSN 1621-4242)
ISBN : 978-2-7178-5902-7
(New acquisition)

72. QUEMENER, Myriam ; PINTE, Jean-Paul
Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques
Paris : Hermès science : Lavoisier, 2013. - 239 p.
ISBN : 978-2-7462-3915-9
(New acquisition)

73. RAUFER, Xavier
Cyber-criminologie
Paris : CNRS éd., 2015. - 239 p.
ISBN : 978-2-271-08556-6
(New acquisition)

74. RIGAUX, François
Ordonnancements juridiques et conversion numérique
Bruxelles: Larcier, 2014.- 406 p.
ISBN: 978-2-8044-6946-7
(New acquisition)

75. RIMBAUD, Alexis
Le juge pénal et l'expertise numérique: révolutions au Palais
Paris : Dalloz, 2007. - 200 p.
ISBN: 978-2-247-07533-1
(New acquisition)

76. ROBERSON, Cliff; BIRZER, Michael L.
Introduction to Private Security: Theory meets Practice
Columbus: Prentice Hall, 2010.- XI-348 p.

Subjects (s): *Crime Prevention - - Police - - Privatization - - Terrorism - - Natural Disasters - - Computer Crime -- Civil Liability – Courts – Recruitment -- Drugs of Abuse – Alcohol – Ethics -- Private Security - - Criminal Justice - - Security Management*
Call N°: 02.04.03/ROB/14675

77. ROBINS, Melinda B.; HILLIARD, Robert L. – Ed.
Beyond Boundaries: Cyberspace in Africa
Portsmouth: Heinemann, 2001. - IX-188 p.
ISBN: 0325001847

Subject(s): *Information Technology --Social Aspects – cyberspace -- Africa*
Call N°: 08.16.01/ROB/14046

78. ROBINSON, Robert R., Ed.
Issues in Security Management: Thinking Critically about Security
Boston: Butterworth-Heinemann, 1999.- XIII-194 p.
ISBN: 978-0-7506-7078-4

Subject (s): *Crime Prevention - - Safety - - Safety Devices - - Industrial Espionage - - Universities - - Fire Control - - Computer Crime -- Security Management - - Private Security - - Gangs*
Call N°: 02.04.03/ROB/14642

79. ROCHFELD, Judith, Dir.
Les nouveaux défis du commerce électronique
Paris : LGDJ : Lextenso éd., 2010. - VIII-206 p.
ISBN : 978-2-275-03591-8
(New acquisition)

80. ROQUES-BONNET, Marie-Charlotte
Le droit peut-il ignorer la révolution numérique ?
Paris : Michalon, 2010. - 606 p.
ISBN : 978-2-84186-553-6
(New acquisition)

81. ROSIER, Karen, Dir.
Le droit du travail à l'ère numérique
Limal: Anthemis, 2011. - 512 p.
ISBN : 978-2-87455-173-4
(New acquisition)

82. ROY, Olivier
L'islam mondialisé
Paris : Editions du Seuil, 2002. - 210 p.
ISBN : 2020538342

Subject(s) : *Mondialisation --Jeunesse --Intégrisme --Terrorisme --Nationalisme --Parlement --Musulmans -- Islamisme --Réislamisation --Sécularisation --Occidentalisation*
Call N°: 05.04.03/ROY/15336

83. ROY, Olivier
Globalized Islam: the Search for a New Ummah
London: Hurst and Company, 2002. - XI-349 p.
ISBN: 1850655987

Subject(s) : *Islam --Youth --Fundamentalism --Internet --Terrorism --Globalization --Nationalism --Parliament -- Muslims -- Culture --Society --Islamism --Re-Islamization --Secularization -- Occidentalization --Jihad*
Call N°: 05.04.03/ROY/15373

84. SARDAR, Ziauddin
Liberating Cyberspace: Civil Liberties, Human Rights and the Internet
Publisher London Pluto Press, 1999. - X-290 p.
ISBN: 0745312942

Subject(s): *Civil Rights --Censorhip --Copyright --Democracy --Political Participation --Privacy --Women --Human Rights --Freedom of Speech --Freedom of Information – Internet – Cryptography -- Cyberspace*
Call N°: 08.16.01/LIB/12613

85. SUMMERS, Sarah J.; SCHWARZENEGGER, Christian; EGE, Gian; YOUNG, Finlay
The Emergence of EU Criminal Law: Cybercrime and the Regulation of the Information Society
Oxford; Portland: Hart Publishing, 2014. - XVII-335 p.
ISBN : 978-1-84113-727-8
(New acquisition)

86. TEYSSIE, Bernard, Dir.
La communication numérique, un droit, des droits
Paris : Ed. Panthéon-Assas, 2013. - 626 p.
(New acquisition)

87. TODD, Paul; BLOCH, Jonathan
Global Intelligence: the World's Secret Services Today
London: Zed Books, 2003. - XI-240 p.
ISBN: 1842771132

Subject(s): *Terrorism --Social Control – Secret Services --Security Services --Technology of Surveillance --Intelligence Agencies*
Call N°: 01.02.07/TOD/14846

88. TOURE, Papa Assane
Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal
Paris : L'Harmattan, 2014. - 616 p.
ISBN 978-2-336-30473-1
(New acquisition)

89. TOWNSEND, John
Cybercrimes: comment des indices cachés dévoilent la vérité Saint-Constant,
Québec : Broquet, 2015. - 32 p.
ISBN : 978-2-89654-451-6 / ISBN : 2-89654-451-8
(New acquisition)

90. TÜRK, Alex
La vie privée en péril. Des citoyens sous contrôle
Paris : O. Jacob, 2011. - 269 p.
ISBN 978-2-7381-2279-7
(New acquisition)

91. UNESCO. Paris
Les droits de l'homme dans le cyberespace
Paris : Economica : Unesco, 2005. – 151 p.
ISBN: 92-3-203979-6
(New acquisition)

92. VAN GRASDORFF, Eric
African Renaissance and Discourse Ownership in the Information Age: the Internet as a Factor of Domination and Liberation
Berlin: LIT Verlag, 2005.- 127 p.
ISBN: 3-8258-8247-0

Subject (s) : *Internet - - Information Technology – Africa - - African Renaissance - - Domination - - Liberation - - Information Age - - Information Revolution*
Call N°: 08.16.01/VAN/13962

93. VENTRE, Daniel, Dir.
Cyberguerre et guerre de l'information: stratégies, règles, enjeux
Paris : Hermès science publications : Lavoisier, 2010. - 319 p.
ISBN : 978-2-7462-3004-0 / ISBN : 2-7462-3004-6
(New acquisition)

94. VENTRE, Daniel
Cyberespace et acteurs du cyberconflit
Paris : Hermès science : Lavoisier, 2011. - 283 p.
ISBN : 978-2-7462-3123-8
(New acquisition)

95. VENTRE, Daniel
Cyberattaque et cyberdéfense
Paris : Hermès science publications : Lavoisier, 2011. - 312 p.
ISBN: 978-2-7462-3204-4
(New acquisition)

96. WALL, David S.
Cybercrime: The Transformation of Crime in the information age
Cambridge; Malden (Mass.): Polity, 2007. - XII-276 p.
ISBN: 978-0-7456-2735-9 /ISBN: 978-0-7456-2736-6 / ISBN: 0-7456-2736-6
(New acquisition)

97. WILD, Charles ; WEINSTEIN, Stuart ; MACEWAN, Neil; GEACH, Neal
Electronic and mobile commerce law: an analysis of trade, finance, media and cybercrime in the digital age
Hatfield: University of Hertfordshire Press, 2011. – XXVII-579 p.
ISBN: 978-1-907396-01-4 / ISBN: 1-907396-01-2
(New acquisition)

98. WILSON, Ernest J.; WONG, Kelvin R., Ed.
Negotiating the Net in Africa: the Politics of Internet Diffusion
Boulder: Lynne Rienner Publishers, 2007.- XII-237p.

Subject (s): *Internet - - Information Technology - - Communication Engineering - - Economic Aspects - - Social Aspects - - Africa - - Ghana - - Guinea-Bissau - - Kenya - - Rwanda - - South Africa - - Tanzania -- ICT*
Call N°: 08.16.01/WIL/13873

PART II / 2ème PARTIE

ELECTRONIC DOCUMENTS

DOCUMENTS ÉLECTRONIQUES

II – Electronic Documents–Documents électroniques

1. ADELAJA, Oluwabukola

Catching up with the rest of the world: the legal framework of cybercrime in Africa

Introduction: In recent times, there has been a rapid growth in ICT especially the internet in Africa. This has caused a growing concern among relevant stakeholders on the increase on cybercrime in Africa. This poses a risk of cyber attack exposure to critical economic and government sectors within Africa. Compared to other developed countries, only an average 15% of the African population uses the internet. Even though this is low in relative terms, Africa is fast becoming a hot spot for the perpetration of cybercrime. This is largely due to the expansion of broadband internet and the absence of regulatory measures to crack down on cyber criminals. The main challenge that is emerging is that the continent seems generally ill equipped to address the issue of cybercrime. The US and the UK are among the leading countries with a high rate of cybercrime. However, they are able to balance this out through implementing regulatory and technologically advanced measures to curb cybercrime.
This paper will argue for the need to implement anti cybercrime legislation in Africa. It will start off by looking at the current legislative efforts in the continent. This will be achieved by a selective case study of key countries in regions on Africa, namely the northern, western, eastern and southern parts of Africa.
Legislative effort is only part of the whole process. This paper will also argue for the need and importance of collaborative alliances within the regions through regional bodies such as the South African Development Co- operation (SADC), East Africa Community (EAC) and Economic Co-operation of West African States (ECOWAS). This should also extend outside the region and through the involvement and developments of experts in the field. This will be achieved by looking at current collaborative efforts in other parts of the world. This will be done bearing in mind the workability of such collaborations or technological implementations in Africa. Is the technological terrain in Africa ripe for such a move? Are there other social, political or economic constrains that exist to make this move difficult? Are there any current anti cybercrime efforts in place?
Source: http://afsaap.org.au/assets/Adelaja.pdf
File: ADELAJA_Oluwabukola_ Catching up with the rest of the world.pdf

2. AFRICAN CENTER for CYBERLAW and CYBERCRIME PREVENTION (ACCP)

Workshop report on cybercrime legislation in West Africa 11th April 2014
Workshop on the harmonization of cyber legislation in ECOWAS Accra (Ghana), 18 - 21 March 2014

Executive summary: Cybercrime has continued to compromise the growth potentials of the Africa region. It is a relatively new trend of crime, highly volatile and massive in dysfunctional impact. The scourge of online criminality has followed the growing use and application of information /communication technologies which have recorded an unprecedented level, invariably overwhelming traditional means of crime control.
The purpose of the workshop was to support countries of the ECOWAS region in their collective effort aimed at discussing the challenges cybercrime poses to their development. Governments and institutions are showing greater resolve to commit resources in the search for empirical and action - oriented remedial interventions to address the problem of cybercrime. Assurances of support from the Government of Ghana as a focal point to galvanise all authorities in the region to fight cybercrime were given by the Minister for Communications in his statement to the participants at the opening ceremony. As expected, the visible challenges brought by cybercrime operations overwhelm the individual capacities of African countries to make any meaningful intervention on their own.
Source:http://cybercrime-fr.org/index.pl/accp
https://tftcal.unctad.org/pluginfile.php/12929/mod_resource/content/2/Workshop%20Report%20by%20ACCP%20Ghana%2018%20-%2021%20March%202014.pdf
File: African Center for Cyberlaw_Workshop report on cybercrime.pdf

3. AGENCE DE L'INFORMATIQUE DE L'ETAT (ADIE), Dakar

Loi sur la cybercriminalité : LOI n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité.

Source : http://www.osiris.sn/IMG/pdf/loi_sur_la_cybercriminalite.pdf
http://www.adie.sn/index.php/documentation/publications/category/5-loistic?download=11:loi- cybercriminalite
File : AGENCE_INFORMATIQUE_ETAT_ Loi sur la cybercriminalité.pdf

4. AKUTA, Eric Agwe-Mbarika; ONG'OA, Isaac Monari ; JONES, Chanika Renee

Combating Cyber Crime in Sub-Sahara Africa; a Discourse on Law, Policy and Practice *Journal of Peace, Gender and Development Studies*, Vol. 1, N° 4, May 2011, p.129-137

Abstract: Prior to the arrival of ICTs in Sub Sahara Africa (SSA), Africa was seen as the Dark Continent. The development of ICTs was therefore expected to connect Africa to the rest of the world, and establish it as part of the Global community. This endeavor exposed Africa to the unintended consequences of the Internet (cybercrime). The manifestations of cybercrime, it's far reaching and potentially devastating capacity for harm caught most governments off guard because the existing laws, legislations and institutions were unable to keep up with the alarming rate at which cybercrime has diffused. Most governments have struggled to put in place safeguards that can help combat this malaise. While efforts are under way, they have been largely ineffective at repealing cyber crime.
This statement begs the question, what support can be rendered to strengthen the position of stakeholders in their fight against cybercrime in SSA. This study sought to address that question by examining three principal issues: First, it identified the various stakeholders involved in the fight against cybercrime in SSA. Second, it examined the existing laws, policies and practices employed by stakeholders to combat this malaise. Third, it discussed the impediments that these stakeholder structures and institutions face in countering cybercrime. A sound knowledge of these principal issues will provide policy makers and stakeholders with an in-depth understanding of the various structures and their existing efforts to combat cybercrime.
Source:http://www.interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al.pdf
http://www.interesjournals.org/full-articles/-combating-cyber-crime-in-sub-sahara-africa-a-discourse-on-law- policy-and-practice.pdf?view=inline
File: AKUTA_Eric Agwe-Mbarika_Combating Cyber Crime.pdf

5. ANING, Kwesi

Organized Crime in West Africa: Options for EU Engagement

Abstract: Worldwide, organized crime is considered a major threat to human security. Organized crime impedes social, economic, cultural and democratic developments globally, with disproportionate effects on developing and fragile states. The threat and challenges of organized crime in Africa in general and West Africa in particular is enormous because of the high presence of fragile states serving as potential breeding grounds for such activities (Commission of the European Communities 2007: 5). In Africa, as in the rest of the world, organized criminal activities take the form of drug trafficking, advanced fee and Internet fraud, human trafficking, diamond smuggling, forgery, cigarette smuggling, illegal manufacture of firearms, trafficking in firearms, armed robbery and the theft and smuggling of oil (Aning, 2008). For West African states, one of the most serious challenges to state survival is the influx of narcotics and their impact on public, private sector and community institutions. The emerging culture of quick and easy acquisition of money threatens democracy – drug cartels have bought friends in high places in West Africa. The scale of the problem is so massive that the United Nations Office for Drugs and Crime (UNODC) states: The crisis of drug trafficking in West Africa is gaining attention...Alarm bells are ringing about the volume of cocaine transiting the region (roughly 50 tons a year). West Africa...has become a hub for cocaine trafficking ... worth almost $2 billion a year. This is more than a drugs problem. It is a serious security threat (UNODC 2008: 1).
Organized transnational criminal groups pose threats to West Africa's fragile states and to democratic governance processes and institutions. The established link between drug trafficking in West Africa and Europe highlights the need for the European Union (EU) to engage its West African counterparts in fighting the negative impacts of organized crime in West Africa, including its corrosive effects on democratic institutions – parliaments, the judiciary, political parties and the executive arm of government. The EU can build democracy in the sub-region in a significant manner only if the threats posed by transnational organized crime (TOC) are addressed concurrently.
Source : http://www.idea.int/resources/analysis/loader.cfm?csmodule=security/getfile&pageid=37849
File: ANING_Kwesi_Organized Crime in West Africa.pdf

6. ATTA-ASAMOAH, Andrews

Understanding the West African cyber crime process

Introduction: Since the late 1980s, and particularly during the last decade, few mail addresses across the world have been spared the onslaught of unsolicited mail from the West Coast of Africa. In the early days many received such letters by post, later by fax and telex, and in recent times by e-mail. The content of the letters range from business proposals, inheritance reclamation, job offers, announcement of lottery wins, marriage proposals, immigration offers, admission to overseas academic institutions to money transfers and property sales, among others.

This form of crime originated in Nigeria and therefore became known as the 'Nigerian letter', but the phenomenon has in recent times assumed remarkable criminal dimensions through which thousands of young people operating from cybercafés in West Africa…
Source: https://issafrica.s3.amazonaws.com/site/uploads/18N4ATTAASAMOAH.PDF
File: ATTA-ASAMOAH_Andrews_Understanding the West African cybercrime process.pdf

7. BASSET, Laurence

Compte-rendu : Cyberattaque et cyberdéfense, Daniel VENTRE, 2011, Paris, Lavoisier, 312p.
Études internationales, Vol. 43, N° 3, 2012, p. 476-478
Source : http://www.erudit.org/revue/ei/2012/v43/n3/1012824ar.pdf http://id.erudit.org/iderudit/1012824ar
File: BASSET_Laurence_Compte-rendu : Cyberattaque et cyberdéfense.pdf

8. BAUD, Michel

La cyberguerre n'aura pas lieu, mais il faut s'y préparer
Politique étrangère, Vol. 77, N° 2, Été 2012, p. 305-316

Introduction : En octobre 2011, Thomas Rid, enseignant au King's College de Londres, publie « Cyber War Will Not Take Place1 », un article largement commenté dont la thèse centrale est qu'aucune cyberguerre ne s'est produite jusqu'à présent et qu'il est fort peu probable qu'il en aille différemment dans le futur. Pour lui, une cyberaction ne peut être que la continuation de modes d'action traditionnels à l'aide de moyens modernes. Il est vrai qu'aucune cyberguerre n'a encore fait de victimes - au sens où on l'entend dans la définition classique de la guerre2. Peut-on pour autant s'en désintéresser et laisser à d'autres le soin de préparer une guerre improbable ? Une forme de cyberguerre, au travers de cyberactions, d'attaques informatiques, existe pourtant. Tous les conflits récents ont vu l'utilisation de cyberarmes (Afghanistan, Géorgie, Libye, etc.). Le terme de cyberguerre renvoie donc à une réalité concrète, qu'il semble naturel d'aborder sous un angle militaire. En France, le sujet est largement débattu dans les armées. Fin 2011 a été inaugurée à Paris la chaire Castex de cyberstratégie…
Source: http://www.jstor.org/stable/42714580
File: BAUD_Michel _La cyberguerre naura pas lieu.pdf

9. BRENNER, Susan W

"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare
The Journal of Criminal Law and Criminology, Vol. 97, No. 2, Winter 2007, p. 379-475

Abstract: This Article explains why and how computer technology complicates the related processes of identifying internal (crime and terrorism) and external (war) threats to social order of responding to those threats. First, it divides the process - attribution - into two categories: what-attribution (what kind of attack is this?) and who-attribution (who is responsible for this attack?). Then, it analyzes, in detail, how and why our adversaries' use of computer technology blurs the distinctions between what is now cybercrime, cyberterrorism, and cyberwarfare. The Article goes on to analyze how and why computer technology and the blurring of these distinctions erode our ability to mount an effective response to threats of either type. Finally, it explores ways in which we can modify how we currently divide responsibility for identifying and responding to the three threat categories among law enforcement and the military, respectively. The goal here is to identify techniques we can use to improve attribution and response processes for emerging cyberthreats.
Source: http://www.jstor.org/stable/40042831
File : BRENNER_Susan W_ At Light Speed.pdf

10. BRETON, Thierry

Chantier sur la lutte contre la cybercriminalité : rapport remis à Monsieur le Ministre de l'Intérieur, de la Sécurité intérieure et des Libertés Locales le 25 février 2005, suite à une lettre de mission en date du 29 juin 2004

Introduction : Le développement des nouvelles technologies de l'information ouvre un nouvel espace. L'espace "informationnel" vient désormais s'ajouter aux espaces terrestre, maritime et aérien, dont la protection et la sécurité entrent naturellement dans le champ des compétences régaliennes de l'Etat. Espace virtuel, par sa structure et la nature même des informations qu'il véhicule, le cyberespace a des incidences concrètes sur la vie quotidienne, notamment en ce qui concerne l'accès à la connaissance, les communications entre les personnes, le commerce, l'exercice de la citoyenneté (vote électronique), l'administration ou le travail en ligne.

Toute activité, toute invention humaine porteuse de progrès, peut être aussi génératrice de comportements illicites. La cybercriminalité est l'une des nouvelles formes de criminalité et de délinquance, dont les conséquences peuvent être particulièrement graves pour notre sécurité collective, pour notre économie et, bien sûr, pour les citoyens qui peuvent être personnellement atteints, dans leur personne, dans leur dignité et dans leur patrimoine. Le caractère virtuel des échanges qui débutent sur Internet favorise le franchissement des barrières de l'illégalité, les internautes ayant le sentiment que les bornes morales ou légales de la vie réelle ne s'appliquent pas au cyberespace, ce dernier leur paraissant totalement "désincarné".
Source : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/054000263.pdf
File : BRETON_Thierry_Chantier sur la lutte contre la cybercriminalite.pdf

11. BUTLER, Bob; LACHOW, Irving

Multilateral Approaches for Improving Global Security in Cyberspace
Georgetown Journal of International Affairs, 2012, p. 5-14

Introduction: Effective cyber security requires that national private companies, and non -governmental work together to understand threats in share information and capabilities for threats. This is necessary because cyberspace interconnected environment that provides tremendous nations, organizations and individuals. Unfortunately, environment is also a haven for criminals, terrorists, and other actors whose intentions could undermine the value of the cyberspace commons for the majority of its users. If like- minded actors fail to understand and mitigate these risks, they are placing national and economic security in jeopardy. Global security in cyberspace is predicated on nations coming together with like-minded will, intent, and capabilities to defend against common threats. This article will explore how multilateral approaches can be applied to the cyber security challenge.1 It begins by describing the importance of principles and norms for building a common understanding of goals, terms and concepts. The article then identifies the key players that must participate in a multilateral framework. Although nation states are the principal actors in our proposed approach, businesses…
Source: http://www.jstor.org/stable/pdf/43134333.pdf
File: BUTLER_Bob_Multilateral Approaches for Improving Global Security.pdf

12. BORIES, Clémentines

Appréhender la cyberguerre en droit international : quelques réflexions et mises au point
La Revue des droits de l'homme, N° 6, 2014

Introduction : « Une clef USB défaillante peut faire plus de dégâts qu'une bombe de 250 kg ». A en croire le général Eric Bonnemaison, Directeur adjoint des Affaires stratégiques au Ministère de la Défense, la menace informatique, non contente de bouleverser le visage des conflits armés classiques, constituerait un risque fondamental pour les Etats ainsi que les civils. La « cyberguerre » est un phénomène relativement neuf, dont l'apparition se justifie par notre dépendance à l'outil informatique mais aussi par le faible coût qu'il y a à faire d'un instrument de communication et de travail une arme immatérielle dotée d'un fort potentiel offensif.
Phénomène devenu d'ampleur dans les relations internationales et impliquant au premier chef les Etats Unis d'Amérique, la Chine et la Russie, la « cyberguerre » constitue à la fois une déclinaison nouvelle des tensions internationales et un enjeu pour le droit. Ce n'est que depuis peu qu'elle préoccupe les juristes1, et ce surtout en dehors de nos frontières. Les analyses se concentrent alors avant tout sur les modifications du jus in bello et du jus ad bellum qui pourraient s'avérer nécessaires. La question de l'opportunité d'un traité international régissant
les conflits informatiques est notamment discutée, mais ne paraît pas susceptible de donner lieu à une réalisation véritable dans un délai raisonnable.
Il apparaît dès lors opportun d'interroger le droit positif afin de cerner comment les règles en vigueur peuvent permettre d'envisager les actions informatiques offensives. La présente étude se concentrera non sur les actes de piraterie informatique qui sont le fait d'individus isolés mais sur celles des actions informatiques offensives qui impliquent des Etats, en qualité de commanditaire ou bien de cible, ou encore parce que leurs ressortissants sont les victimes. Apparaît alors une première difficulté, d'ordre non seulement sémantique mais aussi conceptuel : ladite « cyberguerre », multifacettes, doit être définie afin que l'objet de l'analyse puisse être véritablement déterminé (I). Suit une seconde difficulté, celle de l'identification de règles de droit international permettant de répondre aux enjeux de telles attaques en protégeant les victimes civiles, tout en désignant les éventuels Etats commanditaires et/ou victimes de tels agissements (II)…
Source : https://revdh.revues.org/984?lang=fr
File : BORIES_Clementines_ Apprehender la cyberguerre en droit international.pdf

13. CASSIM, Fawzia

Addressing the Growing Spectre of Cybercrime in Africa: Evaluating Measures Adopted by South Africa and other Regional Role Players
The Comparative and International Law Journal of Southern Africa, Vol. 44, No.1, March 2011, p.123-138

Abstract: Cybercrime is thriving on the African continent. The increase in broadband access has resulted in an increase in internet users. Thus, Africa has become a 'safe haven' for online fraudsters. African countries are pre- occupied with pressing issues such as poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes, such as murder, rape, and theft. As a result, the fight against cybercrime is lagging behind. The lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels have compounded the problem. However, attempts are being made by some African countries to address cybercrime. The South African government has taken the lead in introducing cyber legislation to address cybercrime. The ineffectiveness of the South African common law to combat cybercrime, led to the promulgation of the Electronic Communications and Transactions Act 25 of2002 (ECT). Although South Africa has adopted the Council of Europe's Convention on Cyber Crime CETS NO 185 (CECC) it has not ratified the treaty. Other African countries such as Botswana, Kenya, Uganda and Cameroon have also taken steps to introduce cyber legislation and build regional partnerships to combat cybercrime. This is commendable. However, it is recommended that all African countries should adopt and ratify the CECCC to avoid becoming an easy target for international cybercrime.
Source: http://www.jstor.org/stable/23253117
File: CASSIM_Fawzia_Addressing the growing spectre of cybercrime in Africa.pdf

14. CASSIM, Fawzia

Addressing the spectre of cyber terrorism: a comparative perspective
Potchefstroom Electronic Law Journal, Vol.15, N° 2, 2012

Abstract: This article looks at the definition of cyber terrorism and terrorist use of the Internet. The article evaluates cyber terrorist threats facing countries such as the United States of America, the United Kingdom, India and South Africa. The article also examines measures introduced by the respective governments in these countries to counteract cyber terrorist threats. Finally, the article will propose a way forward to counteract such possible threats in the future. The face of terrorism is changing. The convergence of the physical and virtual worlds has resulted in the creation of a ―new threat‖ called cyber terrorism. Cyber terrorism is one of the recognised cybercrimes. The absence of suitable legal frameworks to address cyber terrorism at national and regional levels, the lack of adequate safeguards, the lack of cyber security strategies and the pre-occupation of countries with internal factors have all contributed to the creation of an environment that can be easily infiltrated by cyber terrorists. The horrific events of 9/11 provided the impetus for many countries to introduce antiterrorist legislation. The United States of America, United Kingdom, India and South Africa have introduced legislation to address the threat of cyber terrorism.
Source: http://dx.doi.org/10.4314/pelj.v15i2.14
File: CASSIM_Fawzia_ Addressing the spectre.pdf

15. CEA. Addis Abéba

Relever les défis de la cybersécurité en Afrique Note d‘orientation, NTIS/002/2014

Introduction : Le Rapport économique sur l‘Afrique (2013), publication conjointe de la Commission économique pour l‘Afrique (CEA) et de la Commission de l‘Union africaine (CUA), indique qu‘« apr s deux décennies de quasi-stagnation, la croissance de l‘Afrique s‘est sensiblement améliorée depuis le début du XXIe siècle1. » Depuis 2000, le continent africain connaît une envolée prolongée des cours des produits de base et une croissance soutenue. Le rapport indique en outre que « compte tenu d‘une prévision de 4,8 % en 2013 et de 5,1
% en 2014, par exemple, les perspectives de croissance à long terme de l‘Afrique demeurent fermes. » Il convient également de noter que des publications aussi prestigieuses que The Economist et l‘International Business Times et des organisations comme la Banque africaine de développement (BAD) ont affirmé que l‘Afrique abrite certaines des économies à la croissance la plus rapide au monde.
Source : http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1_fr.pdf
File : CEA_ Relever les defis de la cybersecurite.pdf

16. CEYHAN, Ayse

Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitudes.
Cultures et Conflits, N° 64, Hiver 2006, p.11-32

Résumé : Contrairement aux approches déterministes et essentialistes, cet article se propose d'analyser les relations technologie/sécurité en termes de contextes et dynamiques. Après avoir posé le cadre définitionnel où la technologie est envisagée au sens de « dispositif » qui produit un environnement et façonne les comportements individuels et sociaux, l'auteur examine les éléments de contexte qui conditionnent la technologisation fulgurante de la sécurité. Le contexte est caractérisé par plusieurs phénomènes qui ont pour point commun de générer des incertitudes. Le recours aux technologies émergentes de sécurité se produit dans un cadre de gouvernance libérale où l'Etat coopère avec les entreprises, les organismes internationaux, l'Union européenne, etc. Pour tous ces acteurs la technologie apparaît comme la solution la plus scientifique pour anticiper les dangers et menaces futurs. Cela soulève des problèmes éthiques, juridiques, philosophiques, sociologiques et politiques cruciaux qu'il convient d'examiner à la lumière de la transformation des rapports humains par la technologie.
Source: http://www.jstor.org/stable/23703876
File : CEYHAN_Ayse_Technologie et securite.pdf

17. CHAMBET, Patrick

Le cyber-terrorisme

Introduction : Depuis le 11 septembre 2001, les pays largement informatisés ont commencé à prendre sérieusement en compte les risques de cyber-terrorisme contre leurs entreprises et leur société en général. Mais il ne faut pas oublier que le cyber-terrorisme, même s'il semble actuellement entrer dans une nouvelle phase d'expansion, n'est pas un phénomène nouveau.
Avec une culture de la connectivité ancrée de plus en plus profondément dans les sociétés dites "modernes", il est promis à un bel avenir. Aujourd'hui, on ne saurait plus vivre sans certains services dont l'épine dorsale est constituée par des réseaux informatiques qui pourraient être réduits à néant par quelques attaques bien réelles, judicieusement menées dans le monde virtue.
Nous allons définir dans cet article les notions de cyber-terrorisme et de cyber-terroristes, puis envisager différents scénarios possibles, examiner les armes dont disposent les cyber-terroristes, et enfin aborder les mesures à prendre pour construire une défense efficace, car la menace de cyber-terrorisme doit maintenant être intégrée dans toute étude de sécurité.
Source : https://repo.zenk-security.com/Others/Le%20cyber-terrorisme.pdf
File : CHAMBET_Patrick _Le cyber-terrorisme.pdf

18. CHAWKI, Mohamed

Le vol d'informations : quel cadre juridique aujourd'hui ? *Droit-Tic*, juill. 2006

Résumé : Ce travail vise à examiner les délits traditionnels, qui sont de nature à qualifier des délits informatiques, au cours desquels est obtenu un accès illicite à des informations contenues dans les systèmes informatiques. À cet égard, il faut préalablement nous intéresser au vol d'information. Ce fait est désigné par quelques termes juridiques tels que soustraction, appropriation, ..., qui sont utilisés afin de caractériser le fait d'accéder à une information ou d'en prendre connaissance indûment. Si la jurisprudence et la doctrine tendent à affirmer que la définition du vol s'étend à une chose immatérielle, une objection souvent entendue, affirme que cette jurisprudence violerait le principe de la légalité des délits et des peines en se livrant à une interprétation analogique et téléologique du droit pénal. Quant à ce dernier, son article 311-1 énonce que « le vol est la soustraction frauduleuse de la chose d'autrui ». Si le législateur français dans le nouveau Code pénal aggrave les peines pour un vol simple, et la démarche utilisée pour le définir n'est pas la même, les éléments constitutifs de cette infraction sont uniques. Dans le langage courant, on vole les idées des autres en les plagiant. Une fois de plus, il n'est pas suffisant de déclarer que les termes employés dans le champ juridique de notre étude le sont sans qu'un sens technique leur soit conféré. Effectivement, le sens du terme « appréhension » aurait été plus élégant, dans la mesure où ce terme est défini comme « le fait de saisir par l'esprit, l'opération par laquelle l'esprit atteint immédiatement (par la perception, l'imagination, la mémoire) un objet de pensée simple ». Cependant, parler en ces termes reviendrait à réduire le champ des comportements visés, puisque le fait d'accéder à une information et surtout à une donnée, peut se faire sans son appréhension intellectuelle. Dans ce schéma, il conviendra donc de parler d'accès à l'information et non d'appréhension. Dans ce travail, nous examinons les modalités des actes illicites relatifs à l'accès aux informations. Il s'agit d'étudier l'élément matériel et l'élément moral du vol d'information.
Source : http://www.droit-tic.com/pdf/vol_information.pdf
File: CHAWKI_Mohamed_Le vol d'informations.pdf

19. CHAWKI, Mohamed

Nigeria Tackles Advance Free Fraud
Journal of Information, Law & Technology (JILT), 2009, N° 1

Abstract: Nigerian 419 scam is a major concern for the global community. The introduction, growth and utilization of information and telecommunication technologies (ICTs) have been accompanied by an increase in illegal activities. With respect to cyberspace, anonymous servers, hijacked emails and fake websites are being used as a tool and medium for fraud by cyber scammers. Nigerian advance fee fraud on the Internet is an obvious form of cybercrime that has been affected by the global revolution in ICTs. This form of crimes is not exclusive to advance sums of money to participate into business proposals but also covers romance, lottery and charity scams. Estimates of the total losses due to this scam vary widely. In the United Kingdom, a report conducted by a research group concluded that Internet scams in which criminals use information they trick from gullible victims and commonly strip their bank accounts cost the United Kingdom economy £150 million per year, with the average victim losing .Thus, there is a need for international cooperation to stamp out such illicit activities and protect Internet users. Although new techniques are constantly being implemented and regulations being adopted to combat and eradicate diverse forms of advance fee fraud, yet cyberspace is also providing new means and tools that facilitate committing these scams. Accordingly, this paper seeks to address and analyse some issues related to the use of cyberspace for fraud by cyber scammers especially in Advance Fee Fraud and the techniques used. It will also provide an analysis of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border crime taking Nigeria as a case study. Finally, the paper will conclude by discussing some measures to fight the use of Internet in illegal activities, especially with respect to AFF.
Source: http://go.warwick.ac.uk/jilt/2009_1/chawki
File: CHAWKI_Nigeria Tackles Advance Free Fraud.pdf

20. CHAWKI, Mohamed

Essai sur la notion de cybercriminalité, *IEHEI*, juillet 2006

Introduction: Les nouvelles technologies, en particulier l'informatique et la télématique, ont une place importante dans la vie économique, et la quantité de transactions et échanges menés par l'intermédiaire d'Internet est en spectaculaire progression. Si ces nouvelles technologies participent de manière positive au développement de la vie économique, elles présentent aussi de nouveaux moyens de commettre des infractions d'affaires, ce qui fait apparaître des dangers non négligeables, vue l'importance qu'elles ont désormais acquise. De même, les infractions informatiques ont le plus souvent un caractère international, alors que les informations en elles-mêmes sont des données régies par le droit national. Dans cette optique, les flux d'informations parcourant librement les autorités chargées de l'enquête sont, elles, strictement liées par leur compétence territoriale nationale et par le principe de souveraineté. Chaque législateur essaie soit de se protéger sur son territoire, soit d'abdiquer sa compétence législative face à ces actes illicites, soit d'observer et de légiférer aussi peu que possible, ce qui constituer une solution efficace. Cependant, cette situation est insatisfaisante, car elle plonge les internautes dans un réseau de normes multiples, source d'insécurité juridique.
Ainsi, organiser la lutte contre la cybercriminalité, c'est tenir compte de l'ensemble de ces paradoxes. Il est nécessaire de considérer les intérêts de chacun afin de parvenir à un équilibre. Les pays qui, pour lutter contre la cybercriminalité, tentent de restreindre l'usage d'Internet comme moyen pour commettre des infractions, s'opposent aux Internautes qui brandissent l'étendard de la liberté de circulation de l'information au niveau mondial.
Source : http://www.ie-ei.eu/IE-EI/Ressources/file/biblio/cybercrime.pdf
File : CHAWKI_Mohamed_Essai sur la notion de cybercriminalite.pdf

21. CHAWKI, Mohamed; ABDEL WAHAB, Mohamed S.

Identity Theft in Cyberspace: Issues and Solutions
Lex Electronica, Vol.11, N°1, Spring 2006

Introduction: Identity theft occurs when someone uses or exploits the personal identifying information of another person such as: name, social security number, mother's maiden name, ID number, etc…to commit fraud or engage in other unlawful activities. Whilst numerous variations of this crime exist, an identity thief can fraudulently use personal identifying information for any of the following purposes: (a) opening new credit card accounts; (b) taking over existing credit card account(s) ; (c) applying for loans; (d) renting apartments; (e) contracting with utility companies; (f) issuing fraudulent checks using another person's name and account number; (g) stealing and transfering money from existing bank accounts; (h) instituting bankruptcy proceedings; and/or (i) obtaining employment using a victim's name and details. On such account, identity theft is a serious crime that merits due consideration and adequate prevention and combating. Identity theft may be committed in whole or in part by the use of information and communication technologies (ICTs), which dispenses with face- to- face physical contact and al lows for distant encounters.

Historically, fraud involved face-to-face communication since physical contact was primarily the norm.10 Even when remote communication—i.e., snail mail—could be used to set up a fraudulent transaction, it was often still necessary for the parties to meet and consummate the crime with a physical transfer of the tangible property obtained by deceit.
Source: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf
File: CHAWKI_Mohamed_Identity Theft.pdf

22. CISSÉ Abdoullah

Gouvernance internationale d'Internet : normes et institutions
Diplomacy and Cyberspace Seminar, Rome, vendredi 4 juillet 2003

Introduction : Initialisé vers 1982 avec « l'interconnexion des réseaux à paquets » (les 2 protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol)), le développement de la communication par le biais des ordinateurs grâce aux navigateurs (l'hypertexte) connaît un essor à partir de 1989 avec Le World Wide Web (WEB). Aujourd'hui, l'Internet multimédia, depuis les années 90 offre la possibilité d'accès en temps réel, sur simple demande, à toutes sortes de documents (textes, paroles, images, son).
L'arrivée et l'implantation d'Internet en tant que média illustrent une réalité historique qui caractérise l'évolution des technologies de communication en général. Par conséquent, La gouvernance d'Internet s'insère dans la problématique plus large de la gouvernance des communications. Ainsi, Chaque innovation technique majeure s'accompagne des transformations fondamentales des régimes de gouvernance des communications.
Source: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan012178.pdf
File : CISSE_Abdoullah_Gouvernance internationale d_Internet.pdf

23. CISSÉ, Abdoullah

Exploration sur la cybercriminalité et la sécurité en Afrique : état des lieux et priorités de recherche. Synthèse des rapports nationaux
Ottawa: CRDI, Janvier 2011. –77 p.

Avant-propos : Le développement contemporain des Technologies de l'Information et de la Communication (TIC) constitue un enjeu majeur pour le développement économique en Afrique. Cependant, il a été à l'origine de l'apparition du phénomène de la cybercriminalité dont les caractéristiques particulières ont entraîné l'inadaptation des systèmes répressifs de la plupart des États africains, dont les réponses traditionnelles conçues pour un environnement matérialisé et national, se sont révélées inappropriées pour saisir ce nouveau phénomène criminel, immatériel et mondial de l'ère numérique.
Face à l'actualité de la cybercriminalité qui constitue une véritable menace pour la sécurité des réseaux informatiques, la sécurité des cybercitoyens et cyberconsommateurs dont la protection reste très précaire ainsi que pour le développement de la société de l'information et de l'économie du savoir en Afrique, il est nécessaire de fixer les grandes orientations de la stratégie de prévention et de répression de la cybercriminalité en Afrique en se basant sur les résultats de la recherche scientifique. Il faudra penser à des stratégies innovantes de politique criminelle combinant les réponses étatiques, sociétales et techniques et qui tiennent compte des capacités et des ressources des Etats africains tout en s'inspirant des bonnes pratiques recensées à l'échelle internationale et des lignes directrices de l'Union Internationale des Télécommunications sur la cybersécurité pour les pays en développement…
Source: https://idl-bnc.idrc.ca/dspace/bitstream/10625/47118/1/133493.pdf
File : CISSE_Abdoullah_Exploration sur la cybercriminalite.pdf

24. CISSÉ, Abdoullah

The Way Forward
Expert Meeting on Cyberlaws and Regulations for Enhancing E-Commerce: Including case studies and lessons learned, 25-27 March 2015

Source: http://unctad.org/meetings/en/Presentation/CII_EM5_P_ACisse_fr.pdf
File : CISSE_Abdoullah_The Way Forward.pdf

25. CISSE, Lamine

Réflexions sur la préoccupation de la protection des données personnelles : exemple du Sénégal
Communication à la 23e conférence internationale des commissaires à la protection des données, Session "la démocratie électronique"

Source: http://www.cnil.fr/conference2001/fr/Contribution/Cisse_html
File : CISSE_Lamine_Réflexions sur la préoccupation de la protection des données.pdf

26. CLEMENTE, Dave

International Security: Cyber Security As A Wicked Problem
The World Today, Vol. 67, N° 10, October 2011, p. 15-17

Introduction: Cyber security is a continuing problem for governments, the private sector and individuals around the world. It is now unusual for more than a month to pass without news of a large and often significant cyber-attack. For some victims these attacks are an annoyance while for others they are costly and result in compromised secrets, stolen proprietary designs or reputational damage. The May 2011 attacks against Sony's online PlayStation gaming networks were estimated to have cost 171 million dollars in damage and lost revenue. In the same month, American defence contractor Lockheed Martin suffered a serious breach that was facilitated by electronic identity tokens stolen in an earlier attack against security company RSA.
The litany of breaches, thefts and damage continues with ominous regularity, but why is cyber security such a difficult arena in which to make progress? Is it something that can be solved or must we learn to accept a measure of insecurity? In part, this is a problem made more acute by increasing social and technological complexity. Software, supply chains, social networks and more: the underpinning structures of our daily lives are increasingly interconnected and are interacting at greater speed, and a reliable cyberspace is an essential component of ail of these. It is too expensive and disruptive to start with a clean slate every time a major overhaul is needed. We merely upgrade and add layers to the original mode] - whether it is the internet, a computer operating system or an electrical grid…
Source: http://www.jstor.org/stable/pdf/41962585.pdf
File : CLEMENTE_Dave_International Security Cyber Security.pdf

27. COMMISSION EUROPEENNE(Bruxelles)

Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

Introduction : Au cours des vingt dernières années, Internet et, plus généralement, le cyberespace ont bouleversé l'ensemble de la société. Notre quotidien, nos droits fondamentaux, notre vie sociale et notre économie dépendent désormais de technologies de l'information et des communications (TIC) fonctionnant sans discontinuité. L'émergence d'un cyberespace libre et ouvert a favorisé l'intégration politique et sociale à l'échelle planétaire. Ce cyberespace a fait tomber les barrières entre les pays, les communautés et les individus et a permis l'interaction et le partage des informations et des idées à travers le monde. Il a constitué un forum pour la liberté d'expression et l'exercice des droits fondamentaux et a donné aux peuples les moyens de lutter pour des sociétés démocratiques et plus justes – comme le Printemps arabe l'a montré de façon frappante.
Pour que le cyberespace reste libre et ouvert, les normes, principes et valeurs que l'UE défend hors ligne doivent aussi s'appliquer en ligne. Les droits fondamentaux, la démocratie et l'État de droit doivent donc être protégés dans le cyberespace. Notre liberté et notre prospérité dépendent de plus en plus d'un Internet solide et novateur, qui continuera à se développer si l'innovation du secteur privé et la société civile favorisent sa croissance, mais la liberté en ligne exige aussi sécurité et sûreté. Le cyberespace doit être protégé contre les incidents, actes de malveillance et abus, et les pouvoirs publics ont un rôle important à jouer pour ce qui est de garantir un cyberespace libre et sûr. Plusieurs tâches leur incombent: sauvegarder l'accès et l'ouverture, respecter et protéger les droits fondamentaux en ligne et préserver la fiabilité et l'interopérabilité d'Internet. Cependant, le secteur privé détient et exploite des parties importantes du cyberespace et, pour qu'une initiative soit couronnée de succès dans ce domaine, elle doit tenir compte du rôle moteur des entreprises.
Source : http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_fr.pdf
File : COMMISSION EUROPEENNE_Strategie de cybersecurite de lUnion europeenne.pdf

28. DALZON, Jean-Pierre ; HAUET, Jean-Pierre

La cyber-sécurité dans les systèmes d'automatisme et de contrôle de procédé = Cyber-security of automation and process control systems.

Introduction : Depuis plus une décennie, le monde du contrôle de procédé a intégré les technologies de l'informatique. Stations opérateur et stations de configuration et de maintenance sont supportées par des matériels et logiciels du commerce. Ethernet et Internet sont devenus incontournables. Aujourd'hui, les radiocommunications : Wi-Fi, ZigBee, Bluetooth etc. prennent position dans les systèmes de contrôle. Le coût des systèmes diminue, leurs fonctionnalités s'enrichissent et leur intégration avec le monde de la gestion de production se fait plus étroite. Mais cette évolution rapproche les systèmes de contrôle du monde extérieur et les rend plus vulnérables à des intrusions et à des attaques de toutes natures.
Les risques qui en résultent, pour la production, pour la sécurité des biens et des personnes, sont fortement ressentis aux USA depuis les évènements du 11 septembre. En Europe, la prise de conscience est moindre mais les faits sont là…
Le présent article a pour objectif de sensibiliser les lecteurs à la problématique de la cybersécurité et de présenter les organisations à mettre en place pour se protéger. Il s'appuie sur les travaux de normalisation du comité ISA SP99 visant à permettre la conception et l'implémentation d'une politique optimale de protection des systèmes de contrôle contre les cyber-attaques.

Introduction: Over more than a decade, industrial controls have widely capitalized on the world of information systems. HMI stations and engineering tools are widely using off the shelf hardware and software while Ethernet and Internet have become a must. Moreover, control systems are starting to integrate radio-communications (Wi-Fi, ZigBee, Bluetooth, etc.).
Systems cost has substantially decreased, wider functionality is available and integration with production is tighter. But their protection against the external world has simultaneously decreased making them more vulnerable vis à vis intrusions and other attacks.
Source : http://www.kbintelligence.com/fileadmin/pdf/reecybersecurite.pdf
File : **DALZON_Jean-Pierre_** La cyber-securite dans les systemes dautomatisme et de controle.pdf

29. DANQUAH, P.; LONGE, O. B.

An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond.
African Journal of Computing &ICTs, Vol. 4, N° 2, 2011, p.37-48.

Abstract: The Space Transition Theory (Jaishankar 2008) presupposes that people behave differently in the cyber world from the physical world amongst other postulates that seek to explain cyber-criminal behavioural patterns. (Wall 2001) categorized cybercrime into the four main types of cyber trespass, cyber deception and theft, cyber pornography and cyber violence. This research sought test the postulates of the theory to determine if they form a viable and reliable basis for predicting or determining the occurrence of cybercrime. This was done by identifying the causal relationships between the first six postulates of the Space Transition Theory and the various categories of cybercrime.
Primary data from Ghana was used together with secondary data from other parts of the world to test the theory. Findings from the research showed some limitations in the variety of cybercrimes perpetrated and experienced in Ghana. Our research also established that fact that the Space Transition theory's postulates are not absolutely applicable to all categories of cybercrime. These outcomes serve as a significant reference point for both researchers, policy makers and anti-cybercrime researchers.
Source: http://www.ajocict.net/uploads/V4N1P6-2011_AJOCICT_-_An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality_-_The_Case_of_Ghana_and_Beyond.pdf
File: DANQUAH_P_An Empirical Test of the Space Transition.pdf

30. DESVIGNES, Jean-Louis

Un aperçu de l'histoire de la sécurité des systèmes d'information
Actes du Septième Colloque sur l'Histoire de l'Informatique et des Transmissions

Introduction : D'éminents spécialistes et historiens se sont déjà penchés sur l'histoire de la cryp-tographie, du chiffre, bref de tout ce que l'on qualifie communément de codes secrets et qui contribue à la préservation de la confidentialité d'informations que l'on ne souhaite pas partager. Les références ne manquent pas d'ailleurs, qui montrent l'importance de la maîtrise de ces techniques dont la force ou les faiblesses ont été jusqu'à changer le cours de l'Histoire.
Cependant, la sécurité des systèmes d'information dépasse le cadre de la confidentialité puisqu'elle englobe aussi bien la fiabilité du système lui-même qui doit garantir la disponibilité des informations qu'il traite, que l'authenticité des informations transmises, l'authentification des correspondants ou encore la non répudiation d'une transaction. En outre, les technologies modernes utilisées ont elles-mêmes engendré de nouvelles vulnérabilités d'ordre logique ou physique. De plus, l'interconnexion à outrance de tous les réseaux et systèmes que l'on observe aujourd'hui a ajouté une

dimension nouvelle à la lutte traditionnelle que défenseurs de l'information et attaquants se livrent depuis la nuit des temps : le temps réel. La réactivité face aux attaques, que celles-ci soient ciblées ou massives, est la vertu principale que l'on demande aujourd'hui aux responsables informatiques.
Source : http://www.aconit.org/histoire/colloques/colloque_2004/desvignes.pdf
File : DESVIGNES_Jean-Louis_Un aperçu de lhistoire de la securite.pdf

31. DIOUF, Ndiaw

Infractions en relation avec les nouvelles technologies de l'information et procédure pénale: l'inadaptation des réponses nationales face à un phénomène de dimension internationale
Africalex (Revue d'étude et de recherche sur le droit et l'administration dans les pays d'Afrique), N° 4, décembre 2004

Source : http://afrilex.u-bordeaux4.fr/infractions-en-relation-avec-les.html
File : DIOUF_Ndiaw_Infractions en relation avec les nouvelles technologies.pdf

32. DUPONT, Benoit

L'environnement de la cybersécurité à l'horizon 2022 : tendances, moteurs et implications
Note de recherche N° 14

Sommaire exécutif : En octobre 2010, le Gouvernement du Canada publiait sa stratégie de cybersécurité, prenant acte de l'omniprésence des infrastructures numériques, ainsi que des nouvelles vulnérabilités qui accompagnent cette évolution technologique. En raison des innovations constantes qui caractérisent le secteur numérique, et afin d'y répondre de manière appropriée, toute stratégie de cybersécurité doit s'accompagner d'un exercice de prospective visant à anticiper les tendances technologiques, culturelles et criminelles émergentes.
Ce rapport identifie neuf tendances technologiques émergentes à partir de 21 documents de prospective technologique publiés par des entreprises spécialisées et des organismes publics. Ces tendances regroupent des technologies ayant le potentiel de transformer durablement l'écosystème numérique, que nous définissons comme l'ensemble des infrastructures, des applications logicielles, des contenus et des pratiques sociales qui en déterminent les modes d'utilisation. La notion d'écosystème nous permet d'examiner de manière intégrée les interactions entre les dimensions technique, économique, sociale, politique et juridique de cet assemblage complexe…
Source : http://archives.cerium.ca/IMG/pdf/Dupont_2012_Cybersecurite_2022_note_14.pdf
File : DUPONT_ Benoit_L_environnement de la cybersecurite.pdf

33. DUPONT, Benoit ; GRABOSKY, Peter ; SHEARING, Clifford ; TANNER, Samuel

La gouvernance de la sécurité dans les États faibles et défaillants
Champ penal / Penal field, Vol. IV, 2007

Résumé : Cet article vise à identifier des moyens permettant le renforcement des mécanismes de contrôle social et de résolution des conflits dans les États faibles et défaillants. Après avoir examiné la gouvernance de la sécurité telle qu'elle se développe dans les États forts, nous montrons que certaines configurations institutionnelles peuvent être transposées dans un contexte d'État faible, où les institutions étatiques en charge de la sécurité sont défaillantes ou inexistantes. Nous identifions de nouveaux mécanismes de gouvernance de la sécurité qui rendent envisageable un minimum de sécurité humaine dans les États les plus affaiblis.
Source : http://champpenal.revues.org/620

34. DUPONT, Benoit; GRABOSKY, Peter; SHEARING, Clifford

The Governance of Security in Weak and Failing State
Champ pénal/Penal field, Vol. IV, 2007

Abstract: This article seeks to identify the means to reinforce social control and conflict resolution mechanisms in weak and failing states. First, we examine the governance of security in strong states, then we show that several institutional configurations can be transferred to weak states, were governmental security institutions have failed or are absent. We identify new mechanisms of security governance that could foster a minimum level of human security to the most vulnerable states.
Source : http://champpenal.revues.org/7197

35. DUPONT, Benoît ; LOUIS, Guillaume

Les voleurs d'identité : profil d'une délinquance ordinaire
Chaire de recherche du Canada en sécurité, identité et technologie, Montréal, 2009
Note de recherches, N° 2

Résumé : Le vol d'identité a frappé 6,7% de la population adulte canadienne en 2008, ce qui représente environ 1,7 millions de personnes (Sproule et Archer, 2008). Il a fait environ 340.000 victimes au Québec l'année précédente (Dupont 2008). Malgré le volume significatif de cette forme émergente de criminalité, les connaissances dont nous disposons sur le sujet restent encore relativement limitées, particulièrement en ce qui concerne le profil des auteurs de ces crimes et leurs modes opératoires. En effet, les principales études disponibles à ce jour prennent la forme de sondages menés auprès de victimes (Baum, 2006; ISIQ, 2007; Kim, 2007; Synovate, 2007; ITRC, 2008; Sproule et Archer, 2008), ce qui nous permet de mesurer la prévalence de ce crime, de comprendre l'usage qui est fait des informations dérobées et d'évaluer l'ampleur des préjudices subis. Cependant, l'une des principales limites des sondages de victimisation est que seule une minorité de victimes est en mesure de dire comment leurs informations personnelles se sont retrouvées entre les mains des délinquants, qu'elles sont par ailleurs rarement en mesure d'identifier. En effet, par nature, le vol d'identité et la fraude qui l'accompagne peuvent être commis sans que l'auteur et sa victime n'établissent un contact direct (contrairement aux agressions physiques par exemple)
Source : http://archives.cerium.ca/IMG/pdf/DupontLouisprofilvid.pdf
File : DUPONT_Benoit_Les voleurs d'identité.pdf

36. FICK, Jacqueline

Prevention is better than Prosecution: Deepening the Defence against Cyber Crime
Journal of Digital Forensics, Security and Law, 2009, 4(4):51-72

Abstract: In the paper the author proposes that effectively and efficiently addressing cybercrime requires a shift in paradigm. For businesses and government departments alike the focus should be on prevention, rather than the prosecution of cyber criminals. The Defence in Depth strategy poses a practical solution for achieving Information Assurance in today's highly networked environments. In a world where ―absolute security is an unachievable goal, the concept of Information Assurance poses significant benefits to securing one of an organization's most valuable assets: Information. It will be argued that the approach of achieving Information Assurance within an organisation, coupled with the implementation of a Defence in Depth strategy can ensure that information is kept secure and readily available and provides a competitive advantage to those willing to invest and maintain such a strategy.
Source: http://ojs.jdfsl.org/index.php/jdfsl/article/view/159/76
File : FICK_Jacqueline_Prevention is better than Prosecution.pdf

37. FICK, Jacqueline

Cyber crime in South Africa: Investigating and prosecuting cybercrime and the benefits of public-private partnerships,
Council of Europe octopus interface conference cooperation against cybercrime, 10-11 March 2009, Strasbourg, France

Executive Summary: With the advent of advanced technology has come a new breed of criminals: criminals who are well-organised, well -resourced and have technological savvy. These cybercriminals commit their crimes with great speed, in an environment of cyber - anonymity and in most instances, in multiple legal jurisdictions. Traditional criminals are turning away from crime such as cash-in-transit robberies to an easy and well-paying life of cybercrime, which offers far greater rewards for less risk. Law enforcement agencies are left playing catch –up with criminals. Traditional law enforcement tools, methodologies and disciplines do not successfully address the detection, investigation and prosecution of cybercrime. This type of crime calls for a pro-active approach, for timely international cooperation, and for effective public-private partnerships to ensure the upper-hand over criminals.
This paper aims to provide a broad overview of the South African legal context governing cybercrime, practical examples of cyber investigations and the benefits of public - private partnerships to the prevention, detection and prosecution of cybercrime in South Africa
Source: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres_JaquiFick_report.pdf
File : FICK_Jacqueline_Cyber crime in South Africa.pdf

38. GAGLIARDONE, Iginio; SAMBULI, Nanjira

Cyber Security and Cyber Resilience in East Africa
Global Commission on Internet Governance Paper Series, N° 15, May 2015

Abstract: This paper analyzes continuities and discontinuities of collective efforts toward enhanced cyber security in Eastern Africa, with a particular focus on Kenya, Ethiopia and Somalia. Focusing on the challenges that have followed the contours of East Africa‘s distinctive digital cultures, it challenges the view that cyber security and cyber resilience are simply technical problems that can be solved by reducing the gap with more technically advanced nations. On the contrary, it shows how cyber security is an inherently political challenge and that, in the absence of adequate checks and balances, the increasing securitization of domestic and international politics may require costly trade-offs with individual and collective freedoms. Three concepts are suggested — emulation, extraversion and enculturation — that can serve to better capture how Kenya, Ethiopia and Somalia have respectively answered emerging cyber threats. These concepts, rather than adding to the already abundant jargon in this area, are simply meant to encourage analysts to pay greater attention to how the technical, social and political interact in unique ways and produce distinctive outcomes in each national context. In Kenya, public and private actors have sought to live up to international standards, keeping up with the country‘s reputation as a regional information and communication technology (ICT) powerhouse, but it is unclear how such an ambitious agenda will find concrete applications. In Ethiopia, there is the risk that the need to guarantee better cyber security can further legitimize repressive measures in the new media sector. Finally, in Somalia, in the absence of a functioning state, hybrid solutions have been found that connect traditional practices and new technologies to offer some level of certainty to individuals using services that are vital for the region, such as local and international payments over mobile phones.
Source: https://www.cigionline.org/sites/default/files/no15_web.pdf
File: GAGLIARDONE_Iginio_Cyber Security and Cyber Resilience.pdf

39. GAL-OR, Esther

The Economic Incentives for Sharing Security Information
Information Systems Research, Vol. 16, N° 2, June 2005, p. 186-208

Abstract: Given that information technology (IT) security has emerged as an important issue in the last few years, the subject of security information sharing among firms, as a tool to minimize security breaches, has gained the interest of practitioners and academics. To promote the disclosure and sharing of cyber security information among firms, the U.S. federal government has encouraged the establishment of many industry-based Informa tion Sharing and Analysis Centers (ISACs) under Presidential Decision Directive (PDD) 63. Sharing security vulnerabilities and technological solutions related to methods for preventing, detecting, and correcting security breaches is the fundamental goal of the ISACs. However, there are a number of interesting economic issues that will affect the achievement of this goal. Using game theory, we develop an analytical framework to investigate the competitive implications of sharing security information and investments in security technologies. We find that security technology investments and security information sharing act as "strategic complements" in equi librium. Our results suggest that information sharing is more valuable when product substitutability is higher, implying that such sharing alliances yield greater benefits in more competitive industries. We also highlight that the benefits from such information-sharing alliances increase with the size of the firm. We compare the levels of information sharing and technology investments obtained when firms behave independently (Bertrand-Nash) to those selected by an ISAC, which maximizes social welfare or joint industry profits.
Source: http://www.jstor.org/stable/23015911
File: GAL-OR_Esther_ The Economic Incentives for Sharing Security Information.pdf

40. GARCÍA ZABALLOS, Antonio ; GONZALEZ HERRANZ, Félix

From cybersecurity to cybercrime: a framework for analysis and implementation Inter-American Development Bank, September 2013, 23 p. (IDB Technical Note; 588)

Abstract: This technical note outlines a framework for the analysis of cybersecurity, presenting considerations that are crucial to the success of a holistic and transversal cybersecurity strategy. It describes two essential pieces of the analysis: the broadband ecosystem and the basic terminology and concepts of cybersecurity systems. These two pieces serve as a basis for the introduction and description of five Priority Action Pillars (PAPs), which represent five clear lines of action that any government should embrace and implement in developing an effective cybersecurity strategy. The five PAPs are complemented by four horizontal recommendations that encompass a comprehensive cybersecurity analysis framework.
Source: http://publications.iadb.org/handle/11319/5998?locale-attribute=en
File: GARCÍA ZABALLOS_Antonio_From cybersecurity to cybercrime.pdf

41. GAY, Gale Horton

Vulnerabilities in Cyber Security Mean Opportunities, Too
Women of Color Magazine, Vol. 11, N° 1, spring 2012, p. 28-30

Source: http://www.jstor.org/stable/43752161
File: GAY_Gale Horton_ Vulnerabilities in Cyber Security.pdf

42. GHANEA-HERCOCK, Robert

Why Cyber Security is Hard
Georgetown Journal of International Affairs, 2012, p. 81-89

Introduction: In the twenty- first century we face unprecedented challenges in securing the information assets and intellectual property of our public and private organizations. Yet only a few years ago, the cyber war was often derided and declared a mere nuisance to business as usual. Painful experiences over the past two years, such as the Sony and RSA attacks, have now dispelled this naive stance.The truth of cyber security, how- ever, is both overt and subtle. It is overt in the sense that the arena is now clearly driven by a mix of political expression, such as the Anonymous social activism movement, and economic incentives for criminal gangs to state-sponsored industrial espionage. The subtle facet of cyber security, however, is why it remains a difficult problem. Specifically, the mix of technical, policy, and social dimensions have combined to create and complicate a coevolving, complex adaptive system (CAS). This is the essence of the cyber problem. More importantly, once we accept this is the case, it perforce reshapes our entire policy and technical approach to the problem. Ultimately, we cannot solve a CAS; at best we can merely shape and influence its evolution. The article will first overview what we mean by a CAS in the computer domain, and then will review the characteristics of the technical, social, and legal cyber security themes.
Source: http://www.jstor.org/stable/pdf/43134341.pdf
File: GHANEA-HERCOCK_Robert_Why Cyber Security is Hard.pdf

43. GHERNAOUTI-HÉLIE, Solange

The Cybersecurity Guide for Developing Countries Enlarged edition
Geneva: International Telecommunication Union (ITU), 2009. - 175 p.

Forward: This cybersecurity guide for developing countries has been prepared for facilitating the exchange of information on best practices, related to cybersecurity issues and to meet the stated goal of the Global Cybersecuriry Agenda (GCA) to "enhance security and build confidence in the use of information and communication technologies (ICT)".
The guide is intended to give developing countries a tool allowing them to better understand the economical, political, managerial, technical and legal cybersecurity related issues in the spirit of the Global Cybersecurity Agenda. The purpose of it is to help countries get prepared to face issues linked to ICT deployment, uses, vulnerabilities and misuses.
The content of the guide has been selected to meet the needs of developing and, in particular, least-developed countries, in terms of the use of information and communication technologies for the provision of basic services in different sectors, while remaining committed to developing local potential and Holders increasing awareness among all of the stakeholders. increasing awareness among all of the stakeholders.
Source: http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
File: GHERNAOUTI-HÉLIE_Solange_The Cybersecurity Guide for Developing Countries.pdf

44. GUEYE, Issaka

Survol des enjeux et perspectives au Sénégal
Atelier de l'Afrique de l'Ouest sur les Cadres Politiques et Réglementaires pour la Cybersécurité et la Protection de l'Infrastructure de l'Information Critique, Cap-Vert, 27-29 novembre 2007

Source: http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gueye-senegal-perspective-praia-nov-07.pdf
File : GUEYE_Issaka_Survol des enjeux et perspectives au Sénégal.pdf

45. GUEYE, Issaka

Fondements juridiques et démarche réglementaire : survol des enjeux et perspectives au Sénégal
Atelier de l'Afrique de l'Ouest sur les Cadres Politiques et Réglementaires pour la Cybersécurité et la Protection de l'Infrastructure de l'Information Critique, Cap-Vert, 27-29 novembre 2007.
Source: http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gueye-senegal-perspective-praia-nov-07.pdf
File : GUEYE_Issaka_Fondements juridiques et demarche reglementaire .pdf

46. IKEMELU, Chinelo Rose Keziah

Data Mining for Cyber Security
AFRREV STECH: An International Journal of Science and Technology, Vol. 3, N° 3, 2014.

Abstract: Cyber security is concerned with protecting computer and network system from corruption due to malicious software including Trojan horses and virus. Security of our network system is becoming imperative as massive sensitive information is transmitted across the network. In this research paper, data mining application for cyber security is highly explored. We discussed various cyber-terrorism or attack committed across the network such as malicious intrusion, credit card fraud, identity thefts, and infrastructure attack. Data mining techniques such as classification, anomaly, link analysis and so on are being applied to detect or prevent the aforementioned cyber-terrorism or attack. Recommendations were made and suggestion for further study was indicated.
Source: http://dx.doi.org/10.4314/stech.v3i3.10
File: IKEMELU_Chinelo Rose Keziah_Data Mining for Cyber Security.pdf

47. ITU. Geneva

Cybersecurity guide for developing countries
Geneva: International Telecommunication Union (ITU), 2007

Abstract: Social issues, the economy, public policy, human issues: whichever way one looks at it, and whatever one calls it (IT security, telecom security), cybersecurity touches on the security of the digital and cultural wealth of people, organizations and countries. The challenges involved are complex, and meeting them requires that there be the political will to devise and implement a strategy for the development of digital infrastructures and services which includes a coherent, effective, verifiable and manageable cybersecurity strategy.
Obtaining a level of information security that is sufficient to meet technology and information risks is essential for the proper functioning of governments and organizations. The widespread use of digital technologies goes hand-in-hand with increased dependency on those technologies and interdependency of critical infrastructures. This creates a non-negligible vulnerability in the functioning of institutions, potentially endangering them and even undermining the sovereignty of the State.
The goal of cybersecurity is to help protect organizations' assets and resources in organizational, human, financial, technical and information terms, allowing them to pursue their mission. The ultimate objective is to ensure that no lasting harm is done to them. This consists of reducing the likelihood that a threat materializes; limiting the resulting damage or malfunction; and ensuring that, following a security incident, normal operations can be restored within an acceptable time-frame and at an acceptable cost.
The cybersecurity process involves the whole of society, in that every individual is concerned by its implementation. It can be made more relevant by developing a cyber code of conduct for appropriate use of ICTs and promulgating a genuine security policy that stipulates the standards that cybersecurity users (entities, partners and providers) will be expected to meet…
Source: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf
File : ITU_Cybersecurity guide for developing countries.pdf

48. JAMIL, Zahid

Global Fight against Cybercrime: Undoing the Paralysis
Georgetown Journal of International Affairs, 2012, p. 109-120

Introduction: As the Internet exploded across the globe in the mid-1990s, the Council of Europe was the only intergovernmental treaty organization to recognize that "only a binding international instrument can ensure the necessary efficiency in the fight against [cybercrime]" and began the work of drafting a convention as early as 1996 that would "not only deal with criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements."

At the time, the developed countries from across the globe, which possessed the infrastructure and the majority of Internet users, came together out of a common interest to negotiate a draft convention. Four years of negotiations later, in 200I, they finalized the Treaty - the Budapest Convention on Cybercrime ("the Convention")…
Source: http://www.jstor.org/stable/pdf/43134344.pdf
File: JAMIL_Zahid_Global Fight Against Cybercrime.pdf

49. JUILLET, Alain ; HASSID, Olivier

Face au défi des cybermenaces

Résumé : L'avènement du numérique est bien évidemment une chance pour ceux qui savent la saisir. Cette source d'innovation sans pareille offre à la fois la possibilité d'un renforcement spectaculaire de la connaissance, de la maîtrise des paramètres de la globalisation, d'une accélération des capacités de recherche et, enfin, d'une possibilité d'enrichissement. Mais l'innovation est aussi source de nouvelles vulnérabilités.
Source : http://www.institut-entreprise.fr/sites/default/files/article_de_revue/docs/documents_internes/societal-79-17-juillet-dossier.pdf
File : JUILLET_ Alain_ Face au defi des cybermenaces.pdf

50. KAUFMANN, Stefan; WICHUM, Ricky

Risk and Security: Diagnosis of the Present in the Context of (Post-)Modern Insecurities
Historical Social Research / Historische Sozialforschung, Vol. 41, N° 1 (155), 2016, p. 48-69

Abstract: »Risiko und Sicherheit: Soziologische Zeitdiagnostik im Zeichen (post-)moderner Unsicherheiten «. This essay claims that the upsurge of security nowadays is not caused by specific events such as 9/11, Fukushima, or similar catastrophes. Our assumption is, in contrast, that it is the constitution of functionally differentiated societies itself which allows the security and risk dis- course to be applied to all types of issues and phenomena, even though security and risk have only went viral as universal societal problems in the late 20th century. We will flesh out this approach using three bodies of work essential to the German debate. With regard to social policy, Franz-Xaver Kaufmann argues that the viral nature of the security issue arises from the fact that the security concept in modern society is split into system security and self-confidence. Niklas Luhmann's concept of risk - stemming from systems theory - shows that the promi- nence of the topic is the result of the intrinsically modern compulsion of having to forejudge an uncertain future. In contrast, Ulrich Beck's work on (global) risk societies is centred on the catastrophic potential inherent in (post-)modern risks as a cause for the rise of security debates. The sociological analysis employed here not only explains the rise of risk and security topics; it also provides society with a characterization of itself, which in turn can re-affect society and ultimately motivate a different historiographical self-description
Source: http://www.jstor.org/stable/43783677
File: KAUFMANN_Stefan_ Risk and Security.pdf

51. KRAMER, Franklin D.

Cyber Security: An Integrated Governmental Strategy for Progress
Georgetown Journal of International Affairs, 2011, p. 136-150

Introduction: Cyber security has emerged as a critical challenge in an era defined by global interconnectedness and digital information. While there are multiple ongoing efforts that seek to enhance cyber security, an integrated governmental strategy to meet that challenge has only begun and has yet fully to take shape. All strategies demand recognition of risk and prioritization of resources, and cyber strategy will be no different. An effective approach to creating a risk- adjusted, prioritized cyber strategy for the U.S. government would be to focus on key national security problems, provide solutions for those problems and then use that learning to help create security in the broader cyber arenas. Such a strategy would have the additional benefit of establishing an effective allocation between those efforts where government is significantly…
Source: http://www.jstor.org/stable/pdf/43133822.pdf
File: KRAMER_Franklin D_Cyber Security An Integrated Governmental Strategy.pdf

52. KRITZINGER, E; SOLMS, SH von

A Framework for Cyber Security in Africa
Journal of Information Assurance & Cybersecurity, Vol. 2012, 10 p.

Abstract: This paper deals with at least four major cyber safety concerns in Africa discussed in recent literature. These cyber concerns include aspects such as policies, procedure, awareness, research and the provision of technical security measures. Each concern is examined, the main focus areas are highlighted and a solution is proposed. This paper concludes by combining all relevant solutions into a proposed cyber security framework to assist Africa in decreasing its cybercrime rate especially among home users with no or limited cyber safety knowledge.
Source : http://www.ibimapublishing.com/journals/JIACS/2012/322399/322399.pdf
File: KRITZINGER_E_ Framework for Cyber Security in Africa.pdf

53. MATHIAS, Paul

Cyberterrorismes
Terreurs et Terrorismes, N° 62, Novembre 2008, p. 102-105

Introduction : Il est extrêmement difficile d'isoler le fait du terrorisme de la multiplicité de nos représentations dans lesquelles il se projette. La ligne de partage entre la terreur infligée et la terreur subie est trouble et se perd dans les limbes de la pauvreté, des inégalités, de l'isolement, des croyances, de la peur, du désespoir. Le voile numérique s'étendant désormais sur le monde ne simplifie guère l'approche et la compréhension du terrorisme. Certes, il y a quelque chose d'irréductible dans son fait : la violence et la mort promises, reçues, consternantes de facticité. Mais le fait n'est pas le sens, et les réseaux accroissent assurément la complexité de phénomènes que nous éprouvons comme et nommons « terrorisme ».
Source: http://www.jstor.org/stable/40980741
File: MATHIAS_Paul_Cyberterrorismes.pdf

54. MATTELART, Armand

Société de la connaissance, société de l'information, société de contrôle
Cultures et Conflits, Identifier et surveiller : les technologies de sécurité, N° 64, Hiver 2006, p. 167-183

Résumé : Ce que je voudrais aborder avec vous c'est fondamentalement le thème suivant : ce que l'impératif de sécurité appliqué au traitement de l'information soulève comme enjeux eu égard à l'exercice du pouvoir (et aux contre-pouvoirs que l'on se donne) dans des sociétés habituellement définies comme démocratiques. On pourrait examiner un certain nombre de dichotomies et, en premier lieu, celle que vous signalez comme particulièrement problématique entre « société de l'information » et « société de contrôle ». Quels liens entre les deux ? Quelles interactions ? Quels effets ?
Source: http://www.jstor MATTELART_Armand _.org/stable/23703885
File: Societe de la connaissance_ société de l_information.pdf

55. MINISTERE DE LA DEFENSE, Délégation aux Affaires Stratégiques. Paris

Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes
Paris : Ministère de la défense et des anciens combattants, Délégation aux Affaires Stratégiques, Sous-direction Politique et Prospective de Défense, Novembre 2011. - 43 p.
Etude confiée à Esteral Consulting par la Délégation aux Affaires Stratégiques (DAS - Marché n° 1501839960)

Introduction : Le premier objectif de cette étude est de présenter de manière aussi complète que possible l'ensemble des activités des Institutions européennes en cybersécurité et cyberdéfense, en en montrant la portée mais aussi les limitations, disparités, redondances, voire incohérences.
Sur cette base, il s'agit ensuite de tracer quelques pistes sur les améliorations possibles à apporter à ce dispositif dans le sens d'une meilleure complémentarité entre activités nationales et activités européennes en allant dans le sens d'une « plus grande intégration ».
Après quelques éléments de cadrage, l'étude retrace la manière dont les questions de cybersécurité se sont imposées au sein des grands axes politiques de l'Union (marché intérieur, Europe de la défense, affaires intérieures). Elle décrit ensuite la place actuelle de la cybersécurité et la cyberdéfense au sein des différentes Institutions européennes selon plusieurs plans : les acteurs, les outils de mise en œuvre interne, les thèmes d'activité. Elle s'achève avec une série de remarques et de propositions sur la manière dont pourrait évoluer la prise en compte de la cybersécurité et la cyberdéfense au sein des Institutions européennes.
Enfin, la variété des modes d'implication d'acteurs nationaux dans les activités de cybersécurité et cyberdéfense au sein des Institutions européennes est rappelée en annexe.

Source:http://www.defense.gouv.fr/content/download/149570/1496328/file/Cyberd%C3%A9fense%20et%20cybers%C3%A9curit%C3%A9%20au%20sein%20des%20institutions%20de%20l/'UE.pdf.
File : MINISTERE DE LA DEFENSE_Etude sur la cyberdéfense et la cybersécurité.pdf

56. OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME. Vienne

Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face.
Vienne : Nations Unies, 25-28 février 2013

Introduction : Dans sa résolution 65/230, l'Assemblée générale a prié la Commission pour la prévention du crime et la justice pénale de créer, conformément au paragraphe 42 de la Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux: les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation, un groupe intergouvernemental d'experts à composition non limitée chargé de réaliser une étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, notamment l'échange d'information sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, en vue d'examiner les options envisageables pour renforcer les mesures, juridiques ou autres, prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles1. En outre, dans sa résolution 67/189, l'Assemblée générale a pris note avec satisfaction des activités du groupe intergouvernemental d'experts à composition non limitée et l'a invité à redoubler d'efforts pour achever l'étude et à en présenter en temps voulu les résultats à la Commission pour la prévention du crime et la justice pénale. À sa première session, tenue à Vienne du 17 au 21 janvier 2011, le groupe d'experts a examiné et adopté un ensemble de sujets et une méthodologie pour l'étude. Cette méthodologie prévoyait l'envoi d'un questionnaire aux États Membres, aux organisations intergouvernementales et aux représentants du secteur privé et des institutions universitaires. Les informations ont été recueillies par l'Office des Nations Unies contre la drogue et le crime, conformément à la méthodologie convenue, entre février et juillet 20123. Le présent rapport, qui contient un résumé du projet d'étude approfondie établi par le Secrétariat sur la base des informations recueillies, est soumis pour examen à la deuxième session du groupe d'experts.
Source:https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_F.pdf
File : UNODC_Etude approfondie sur le phenomene de la cybercriminalite.pdf

57. OJEBODE, Ayobami; TOGUNDE, Dimeji; ADELAKUN, Abimbola

Secrecy, Security and Social Exchange: New Media and Cross-generational Dating in Nigeria
International Journal of Sociology of the Family, Vol. 37, N° 2, autumn 2011, p. 307-327

Abstract: Although studies that examine the uses and influence of new media in Africa have always focused on national trends and mainstream groups, the peculiar appropriation of the new media by sub-cultural groups has received little attention. This paper examines the appropriation of the new media by female undergraduate students involved in cross-generational dating in southwestern Nigeria. It addresses how this group of students deploy the new media in their dating practice with older male partners, and how the new media in turn influence their activities. Drawing on ethnographic fieldwork on three Nigerian university campuses, findings indicate that female students involved in cross generational dating employ the new media to connect with older male partners, nurse the connections and/or to disconnect. The respondents also reveal that the new media are highly valued because they ensure secrecy, which is important in their practice of cross-generational dating. Through their utility in tracking members of the group, the new media are helpful for security purpose. The media have also come to be a status symbol within and outside the group, and to signify a currency of exchange. There is a reciprocal relationship between cross-generational dating and the use of exotic new media accessories: each accelerates and improves the other.
Source : http://www.jstor.org/stable/23028815
File: OJEBODE_Ayobami_Secrecy Security and Social Exchange.pdf

58. OLOWU, Dejo

Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa
Journal of Information, Law & Technology (JILT), N° 1, 2009.

Abstract: As the world marches deeper into the unknown passageway of digital revolution, it is becoming apparent that the tremendous benefits of the internet age are being challenged by the formidable menace of cyber-crime, not the least

in the African region. While African States vary in the degree to which their economies and peoples are affected by cyber-crime, there is no gainsaying the fact that the collective ability of African States to track and trace the source(s) of any criminal use of the internet or cyber-attacks on infrastructures, economies or individuals is central to the deterrence of such attacks as well as to long-term survival of these States. An acknowledged and concerted ability to respond to cyber-crimes, to track, trace and apprehend domestic and international cyber-criminals can forestall future attacks through fear of severe penalties. This paper highlights the general weakness or inertia of African States in curbing the menace of cyber- crimes and particularly draws attention to the inherent limitations and failures in current domestic legal responses to cyber-crime. Acknowledging the complex and often extra-territorial nature of cyber-crimes, this paper makes a case for a redefinition of the notion of sovereignty and its implications for the recurring decimal of cyber-crime against African economies and societies. Extrapolating from learned experiences around the world, this paper explores the trajectory of a regional normative initiative that would streamline and synergise the efforts of African States in responding to the phenomenon of cyber-crimes.
Source: http://go.warwick.ac.uk/jilt/2009_1/olowu
File : OLOWU_Dejo_Cyber-Crimes and the Boundaries of Domestic Legal Responses.pdf

59. PAINTER, Christopher M.; BALTINK, Steven; SCHLEIEN, Samuel J. COX, Samuel J.; STRELTSOV, Anatoly; LOTRIONTE, Catherine

National Security and Diplomatic Efforts: Panel 1
Georgetown Journal of International Affairs, 2012, p. 167-188

Source: http://www.jstor.org/stable/pdf/43134347.pdf
File: **PAINTER_Christopher_M_** National Security and Diplomatic Efforts.pdf

60. PORTEOUS, Holly

Cybersécurité et renseignement de sécurité : l'approche des Etats-Unis
Ottawa : Bibliothèque du Parlement, 2011. – 11 p.

Introduction : Des allégations faites en janvier 2010 selon lesquelles la Chine aurait piraté les comptes de courriel de Google et les systèmes informatiques d'au moins 33 autres entreprises américaines mettent en lumière une campagne continue de cyberespionnage de plus en plus audacieuse menée contre les intérêts des États-Unis et de leurs alliés En effet, les soupçons de cyberespionnage qui pèsent contre la Chine ont d'abord attiré l'attention du public en 2003, lorsque des rapports sont venus affirmer que celle-ci était à l'origine d'une opération massive et coordonnée qui avait compromis la sécurité de systèmes informatiques confidentiels des gouvernements et du secteur privé aux États-Unis, au Royaume-Uni, en Australie, en Nouvelle Zélande et au Canada. Qualifiée de « Pluie de Titan » aux États-Unis, cette opération d'espionnage n'a jamais vraiment cessé. Elle s'est seulement transformée en attaques constantes, au moyen d'une vaste infrastructure secrète de systèmes compromis, contre les États-Unis, leurs partenaires des Five Eyes (le Canada, le Royaume-Uni, l'Australie et la Nouvelle-Zélande) et d'autres pays. La Chine est l'un des États de plus en plus nombreux dont on croit qu'ils se servent d'Internet pour voler des renseignements classifiés ou exclusifs et, selon de nombreux analystes, à préparer des actes de sabotage en prévision d'un conflit.
Les États-Unis, considérant le cyberespionnage et les cyberattaques comme des menaces de premier ordre, ont reformulé leur stratégie nationale en matière de cybersécurité. Trois de leurs plus proches partenaires du milieu du renseignement (Five Eyes) – l'Australie, la Nouvelle-Zélande et le Royaume-Uni – leur ont emboîté le pas. En 2004, le Canada a lui aussi commencé à préparer une stratégie nationale en matière de cybersécurité, mais, au moment où nous écrivons ces lignes, il n'a pas encore fait connaître publiquement sa position. Puisque l'expérience qu'ont connue les États-Unis a profondément influé sur les stratégies de leurs alliés, le présent document se concentrera sur leur approche. Pour des raisons qui seront explorées plus loin dans ce document, le renseignement sur les transmissions (SIGINT – interception de signaux électroniques de tout genre en vue de réunir des renseignements sur une cible) y joue un rôle central.
Source : http://www.bdp.parl.gc.ca/content/lop/researchpublications/2010-02-f.pdf
File : PORTEOUS_Holly_Cybersecurite et renseignement de securite.pdf

61. POULLET, Yves

Comment appliquer les règles de protection des données aux transferts de données personnelles dans une société à la fois globale mais également multi-économique et multiculturelle ?
Lex Electronica, Vol. 12, N°1, printemps / spring 2007

Résumé : Dans son texte, l'auteur répond à une question posée lors d'une Conférence organisée conjointement par l'US Department of Commerce et le Groupe de l'article 29 et qui appelle à déterminer la façon dont les règles de protection

des données doivent s'appliquer lors des transferts de données personnelles dans une société globale, multi-économique et multiculturelle. La question est pertinente dans une telle société, caractérisée par le besoin, d'une part d'assurer, sans considération de frontières, un certain régime de protection des données et d'autre part, de respecter la diversité des réalités économiques et culturelles qui se côtoient de plus en plus. L'auteur rappelle d'abord comment l'Europe a progressivement mis en place le système du droit à la protection des données personnelles. Il explique ensuite comment l'Union européenne a considéré la question de la réglementation des flux transfrontières pour en arriver au développement d'un système de protection adéquat et efficace lors des transferts de données hors de l'Union européenne. Toutefois, un tel système mis en place ne semble plus répondre de nos jours à la réalité des flux transfrontières, d'où la nécessité éventuelle de le réformer.
Source:http://www.lex-electronica.org/articles/v12-1/poullet.pdf
https://depot.erudit.org/bitstream/002645dd/1/Comment%2bappliquer.pdf https://depot.erudit.org/id/002645dd
File : POULLET_Yves_Comment appliquer les règles de protection des données.pdf

62. PRATES, Fernanda; GAUDREAU, Frédérick; DUPONT, Benoit

La cybercriminalité: état des lieux et perspectives d'avenir
Cowansville : Éditions Yvon Blais, 2013, p. 415 - 442

Introduction : Internet fait désormais partie intégrante de nos vies, tant au niveau personnel que professionnel. Une enquête menée auprès de 50.000 personnes dans 46 pays montre en effet que l'Internet est devenu le média le plus utilisé pour plus de la moitié des internautes dans le monde, 61% d'entre eux s'y rendant quotidiennement, alors qu'ils sont 54% à faire de même avec la télévision, 36% avec la radio et 32% avec les journaux papier (TNS Sofres, 2010). Selon l'Union internationale des télécommunications, en janvier 2011, 2,08 milliards d'individus utilisaient Internet sur la planète, alors qu'ils étaient seulement 1,03 milliard en 2005 (ZDNet France). Au Québec, en décembre 2011, 78,9% des adultes ont utilisé Internet au moins une fois par semaine, contre 74,4% en décembre 2010 (CEFRIO, 2011a). Le nombre toujours grandissant d'acteurs présents dans l'univers virtuel demande d'ailleurs le renforcement du modèle de gouvernance multipartite soutenu par l'ICANN2 pour assurer ainsi que les points de vue de ces multiples acteurs (les gouvernements, la société civile, les entreprises et la communauté technique) soient pris en considération (ICANN, 2011)…
Source : http://benoitdupont.openum.ca/files/sites/31/2015/07/Prates-Gaudreau-Dupont-2013-cybercriminalit%C3%A9.pdf
File : PRATES_Fernanda_ La cybercriminalite.pdf

63. SALEH, Ibrahim

The impact of ICT on peace, security & governance in Africa United Nations Alliance of Civilizations Media Literacy Education

Abstract: One of the most important features of the digital age is the use of new communications technologies to build digital citizenships. Cultures could be a source of conflict that affect the use of new media to make powerful collaborations among online communities across societies, and within the same society, however, there are still altercation between digital citizens, groups and nations (Hofstede, 2002). New media could help citizens in many directions such appreciating their diversities; solving their problems, sharing experiences and voicing out their salient issues without worries and shame. There is urgency for this research to help update data base to improve the current media governance and address vital issues of conflict and violence in Africa that are permanently on record, which might be occasionally contested in some African countries but almost impossible to erase or block. ICT in Africa could be the refuge for peace, security through embracing participatory governance principles on the one hand, and is implemented through user friendly harmonized, effective and efficient management tools and mechanisms on the other. The latter and more specifically those responsive to the populations needs in harmony with the environment, will allow governments to better channel development actions in order to obtain a positive and sustainable impact and address the challenges faced by African countries
Source: http://www.academia.edu/393239/The_impact_of_ICT_on_Peace_Security_and_Governance_in_Africa

64. SAMAAN, Jean-Loup

Mythes et réalités des cyberguerres
Politique étrangère, Vol. 73, N° 4, Hiver 2008, p. 829-841

Introduction : Il y a plus de vingt ans, lorsque William Gibson publia son roman Neuromancien - sur un informaticien pourchassé dans l'espace virtuel, le cyberspace - les choses semblaient bien confuses et en laissèrent perplexe plus d'un. Or, à l'automne 2007, la perplexité a apparemment laissé place aux convictions, et l'US Air Force a annoncé en grande

pompe la création de son tout nouveau Cybercommand, un commandement composé d'environ 600 officiers. De son côté, le dernier Livre blanc sur la défense et la sécurité nationale français annonce que « dans la mesure où le cyberespace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace ». Aujourd'hui, le terme de « cyberespace » fait donc partie du langage commun et le Département de la Défense américain en a même une définition propre : « un domaine caractérisé par l'usage de l'électronique et du spectre électromagnétique pour stocker, modifier et échanger des données via des systèmes en réseaux et les structures physiques qui y sont attachées »…
Source: http://www.jstor.org/stable/42715588
File : SAMAAN_Jean-Loup_ Mythes et realites des cyberguerres.pdf

65. SAMUEL, Cherian ; SHARMA, Munish, Eds.

Securing Cyberespace: International and Asian Perspectives
New Delhi: Pentagon Press, 2016. – 362 p.

Introduction: The use of cyberspace by governments, businesses and individuals to ease and accelerate all kinds of activities has led to the global expansion of cyber-enabled networks in a relatively short period of time. While cyber experts have repeatedly warned that the many inherent and existing vulnerabilities in devices and networks have neither been resolved nor can be adequately managed to ensure security of the networks, these have largely been ignored or downplayed. The escalation in the number and magnitude of attacks has meant that most policymakers are now cognisant of the wide gamut of issues associated with cybersecurity. The varying perspectives of different countries on cyber issues and the sheer complexity of issues have made cybersecurity a concern for not just national but also international security: the geo-political overtones have increased the cybersecurity challenges…
Source: http://www.idsa.in/book/securing-cyberspace_csamuel-msharma
File: SAMUEL_Cherian_Securing Cyberespace.pdf

66. SHEA, Jamie

How is NATO Dealing with Emerging Security Challenges?
Georgetown Journal of International Affairs, Vol. 14, N° 2, Summer/Fall 2013, p. 193-201

Introduction: For most of human history, states have seen their primary role in the field of security as the defence of their borders and their territories against the predations of other states. Though populations faced other threats, such as famine, major epidemics or starvation, governments felt no need to intervene unless there was an immediate threat to the state or social order. Today, states have taken on the responsibility to cope with a much broader spectrum of threats because of voters' increased expectations of protection and the impact of globalization, which has made states much more vulnerable to non-traditional security threats. These can be easily transmitted across borders and can originate virtually everywhere: local and international terrorism, cyber threats to public and private networks, the spread of diseases and pandemics, vulnerabilities to critical infrastructure and energy grids, dependency on globalized supply chains, extreme weather conditions, uncontrolled immigration, organized criminal networks, and the proliferation of chemical, biological, radiological and nuclear (CBRN) devices with greater use of delivery vehicles such as missiles. The national security strategies of most NATO countries today prioritize these non-traditional threats before the more traditional.
Source: http://www.jstor.org/stable/43134426
File: SHEA, Jamie_ How is NATO Dealing with Emerging Security.pdf

67. SIMON, Steven

The New Terrorism: Securing the Nation against a Messianic Foe
The Brookings Review, Vol. 21, N° 1, winter, 2003, p. 18-24

Abstract: In the minds of the men who carried them out, the attacks of September 11 were acts of religious devotion a form of worship, conducted in God's name and in accordance with his wishes. The enemy was the infidel; the opposing ideology, "Western culture."That religious motivation, colored by a messianism and in some cases an apocalyptic vision of the future, distinguishes al-Qaida and its affiliates from conventional terrorists groups such as the Irish Republican Army, the Red Brigades, or even the Palestine Liberation Organization. Although secular political interests help drive al-Qaida's struggle for power, these interests are understood and expressed in religious terms. Al-Qaida wants to purge the Middle East of American political, military, and economic influence, but only as part of a far more sweeping religious agenda: a "defensive jihad" to defeat a rival system portrayed as an existential threat to Islam. The explicitly religious character of the "New Terrorism" poses a profound security challenge for the United States. The social, economic, and political conditions in the Arab and broader Islamic world that have helped give rise to al-Qaida will not

be easily changed. The maximalist demands of the new terrorists obviate dialogue or negotiation. Traditional strategies of deterrence by retaliation are unlikely to work, because the jihadists have no territory to hold at risk, seek sac rifice, and court Western attacks that will validate their claims
Source: http://www.jstor.org/stable/20081085
File: SIMON_Steven_The New Terrorism.pdf

68. STEIN, Schjorberg; GHERNAOUTI-HELIE, Solange

A Global Treaty on Cybersecurity and Cybercrime Second edition, 2011

Introduction: Cyberspace, as the fifth common domain – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. A cyberspace treaty or a set of treaties at the United Nations level, including cybersecurity, cybercrime and other cyberthreats, should be the framework for peace, justice and security in cyberspace.
The International Law Commission adopted at its forty-eight session in 1996 The Draft Code of Crimes against Peace and Security of Mankind, and submitted it to the United Nations General Assembly. Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable for binding Parties under national law.
Crimes against peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol at the United Nations level.
A Treaty or a set of treaties at the United Nations level on cybersecurity and cybercrime should be a global proposal for the 2010s that is based on a potential for consensus. The final draft code may be prepared by the International Law Commission or the Commission on Crime Prevention and Criminal Justice. Mankind will in the future be completely dependent on information and communication technologies.
Serious crimes in cyberspace should be established under international law, whether or not they are punishable under national law.
The International Telecommunication Union (ITU) launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges to cybersecurity could be coordinated. In order to assist the ITU in developing strategic proposal, a global High-Level Experts Group (HLEG) was established in October 2007. This global experts group of almost 100 persons from around the world delivered the Chairmans Report in August 2008 with recommendations on cybersecurity and cyber crime legislations. The Global Strategic Report was delivered in November 2000 and included strategies in five work areas: Legal measures, Technical and prosedural measures, Organizational structures, Capacity building, and International cooperation…
Source:http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Seco nd_edition_2011.pdf
File: STEIN_Schjorberg_A Global Treaty on Cybersecurity.pdf

69. STEIN, Schjorberg; GHERNAOUTI-HELIE, Solange

A Global Protocol on Cybersecurity and Cybercrime: an initiative for peace and security in cyberspace
Cybercrimedata, 2009. – 92 p.

Preface: The International Law Commission adopted at its forty-eight session in 1996 The Draft Code of Crimes against Peace and Security of Mankind, and submitted it to the United Nations General Assembly. Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable under national law.
Crimes against peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol on the United Nations level.
A Convention or a Protocol on the United Nations level on cybersecurity and cybercrime should be a global proposal for the 2010s that is based on a potential for consensus.
The final draft code may be prepared by the International Law Commission.
Mankind will in the future be completely dependent on information and communication technologies. Serious crimes in cyberspace should be established under international law, whether or not they are punishable under national law.
A combined global initiative on the United Nations level by organizations such as United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) should be established. This initiative could have as a final goal a Draft Convention that should be submitted to the International Law Commission for considering a United Nations Convention on Peace and Security in Cyberspace.
ITU launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges to cybersecurity could be coordinated.

In order to assist the ITU in developing strategic proposals, a global High-Level Experts Group (HLEG) was established in October 2007. This global experts group of almost 100 persons delivered the Chairmans Report in August 2008 with recommendations, including on cyber crime legislations. The Global Strategic Report was delivered in November 2008, including strategies in five work areas: Legal measures, Technical and procedural measures…
Source:http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf
File : STEIN_Schjorberg_A Global Protocol on Cybersecurity and Cybercrime.pdf

70. TAVAGLIONE, Nicolas

Liberté ou sécurité: autopsie d'un faux dilemme
Le Temps, 2013, 2 p.

Introduction : La plaidoirie était sans surprise: «Vous ne pouvez pas avoir 100% de sécurité et 100% de protection de la vie privée […]. Je pense que nous avons trouvé le juste équilibre», affirmait Obama, le 7 juin dernier, pour justifier le programme PRISM. Nous avons trouvé le juste équilibre: we've struck the right balance. Obama recycle ainsi une image omniprésente depuis le 11 septembre: il faut trouver «le juste équilibre entre les besoins de sécurité et la protection de la liberté» (Lord Strathclyde, Chef des conservateurs à la chambre des Lords, 2001). La «balance» doit être réajustée.
Cette image constitue, depuis plus de dix ans, le principal argument des partisans d'une ligne sécuritaire dure. Et il jouit d'une grande puissance persuasive. Car le terme «balance» n'a pas d'«alternative viable», note le juriste A. Ashworth: il implique l'équité et la juste mesure, et nul n'est assez fou pour revendiquer la démesure et l'iniquité. Les adversaires du durcissement sécuritaire sont donc coincés. Mais depuis plus de dix ans, des débats académiques nourris ont permis de mesurer les faiblesses de l'image de la balance. Rappelons-en cinq.
L'image de la balance suppose une «relation hydraulique» entre liberté et sécurité: quand l'une croît, l'autre décroît. Mais une restriction des libertés n'entraîne aucune augmentation mécanique de la sécurité. Primo, la recherche en criminologie démontre peu de liens entre répression et augmentation de la sécurité. Secundo, dans le cas du terrorisme, en partie alimenté par le ressentiment face à des injustices réelles ou imaginaires, frapper fort risque uniquement de gonfler les rangs ennemis. Tertio, certaines mesures sécuritaires peuvent entraîner de nouvelles vulnérabilités: si, à des fins de surveillance accrue, vous rassemblez divers fichiers de police épars en une seule grande base de données informatisées, il suffit d'un hacker efficace pour qu'un flot d'informations sensibles tombe dans sa besace…
Source : http://archive-ouverte.unige.ch/unige:30511
File : TAVAGLIONE_Nicolas_Liberte ou securite: autopsie d'un faux dilemme.pdf

71. TOURE, Papa Assane

La cyberstratégie de répression de la cybercriminalité au Sénégal : présentation de la loi n° 2008-11 du 25 janvier 2008, portant sur la cybercriminalité.
Conseil de l'Europe-Programme octopus interface 2010, Conférence sur la coopération contre la cybercriminalité, Strasbourg, France, 23-25 mars 2010.

Introduction : Depuis sa première connexion officielle au réseau Internet en 1996, le Sénégal contemporain n'a cessé d'accomplir des avancées considérables dans le secteur des TIC. La vision du e-Sénégal a vite placé notre pays au cœur de la société de l'information et lui a valu de se voir confier le volet TIC dans le cadre du NEPAD1.
Cependant, comme l'enseignait déjà le Doyen Jean CARBONNIER « l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance »
En effet, comme pour la plupart des grandes découvertes contemporaines, la révolution numérique a engendré des retombées négatives parmi lesquelles figure en bonne place la criminalité. Ainsi, le développement des TIC a généré une nouvelle forme de criminalité dénommée cybercriminalité, charriée par les premières lueurs de la société sénégalaise de l'information. L'attaque dont a été victime le site officiel du Gouvernement du Sénégal en mai 2001 de la part d'un pirate informatique se disant membre de la « Hack Army » ainsi les actes sabotage informatiques par cheval de Troie envoyé depuis le forum de discussion dirigés contre le site d'informations en ligne nettali.com en janvier 2008, ont fini de convaincre sur l'expansion de la cybercriminalité au Sénégal.
Face aux enjeux suscités par l'avènement de la cybercriminalité, les pouvoirs publics sénégalais ont, dès janvier 2005, entrepris, un vaste chantier juridique de mise en place des textes législatifs et réglementaires favorables au développement des TIC au Sénégal, en vue de protéger les biens, les personnes et les institutions publiques contre le phénomène cybercriminel.
Source:http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%203/Loi%20Senegal_workshop%203_fr.pdf
File: TOURE_Papa Assane_La cyberstrategie de repression de la cybercriminalite au Senegal.pdf

72. TOURE, Pape Assane

La cybercriminalité dans les législations communautaires intégrées en Afrique
Porto Novo : Organisation pour l'Harmonisation en Afrique du Droit des Affaires (OHADA) ; Ecole Régionale Supérieure de la Magistrature (ERSUMA), 2013. - 26 p.

Formation de Magistrats, Avocats et Officiers de Police Judiciaire des services d'Interpol, du 02 au 05 septembre 2013, Porto Novo, Bénin
Thème « La législation communautaire intégrée en matière de criminalité d'affaires, criminalité transfrontalière, cybercriminalité, propriété intellectuelle »
Source :
File: TOURE_Papa Assane_cybercriminalite-legislations-communautaires-integree-afrique.pdf

73. UNECA. Addis Ababa

Tackling the challenges of cybersecurity in Africa Policy brief, NTIS/002/2014

Introduction: The 2013 Economic Report on Africa, a joint publication of the Economic Commission for Africa (ECA) and the African Union Commission (AUC), states that ―following two decades of near stagnation, Africa's growth performance has improved hugely since the start of the 21st century. Since 2000, the African continent has experienced a prolonged commodity boom and a sustained growth trend. The report further states that ―Africa's medium-term growth prospects remain strong, too, at for example 4.8 per cent in 2013 and 5.1 per cent in 2014‖. Also of note, highly regarded publications, such as The Economist and the International Business Times4 and organizations, such as the African Development Bank (AfDB), have asserted that Africa is home to some of the world's most rapidly growing economies.
Source: http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf
File: **UNECA_T**ackling the challenges of cybersecurity in Africa.pdf

74. UIT,Genève

Indice de cybersécurité dans le monde et profils de cyber bien-être
Genève, Union internationale des télécommunications (UIT), Avril 2015. – 528 p.

Introduction : L'Indice de cybersécurité dans le monde (GCI) est le fruit d'une relation de partenariat entre le secteur privé et l'organisation internationale, destiné à placer la question de la cybersécurité au premier rang des priorités des programmes nationaux. En tant que projet conjointement mené par ABI Research et l'Union internationale des télécommunications, l'indice GCI fournit des informations sur le niveau d'engagement des Etats souverains en matière de cybersécurité.
Ancré dans le Programme mondial cybersécurité de l'UIT, le GCI évalue le niveau d'engagement dans les cinq domaines d'activités suivants: cadre juridique, mesures techniques, structures organisationnelles, renforcement des capacités et coopération internationale. Il s'agit d'un indice national permettant un classement mondial de l'état de préparation en matière de cybersécurité. Le GCI ne cherche pas à prouver l'efficacité ou le succès d'une mesure en particulier, mais simplement l'existence des structures nationales en place pour mettre en œuvre et promouvoir la cybersécurité.
L'initiative résulte d'intenses recherches primaires et secondaires menées conjointement par l'UIT et ABI Research. Des enquêtes nationales, de même qu'une étude qualitative approfondie, ont été envoyées à tous les Etats Membres de l'UIT et ont permis de collecter des informations sur les lois, les réglementations, les équipes CERT et CIRT, les politiques, les stratégies nationales, les normes, les certifications, la formation professionnelle, la sensibilisation et les partenariats…
Source : http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-F.pdf
File : UIT_ Indice de cybersécurité dans le monde.pdf

75. UIT. Genève

Atelier de l'Afrique de l'Ouest sur les Cadres Politiques et Réglementaires pour la cybersécurité et la Protection de l'Infrastructure de l'Information Critique.
Union Internationale des Télécommunications : 27- 29 Novembre 2007- Praia, Cap-Vert

Résumé : L'atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP) s'est tenu à Praia (Cap-Vert), du 27 au 29 novembre 20071. Il a rassemblé des représentants des pouvoirs publics, des professionnels du secteur et d'autres parties prenantes de la région de l'Afrique de l'Ouest qui ont débattu, échangé des informations et collaboré à l élaboration et à la mise en œuvre de cadres nationaux politiques et réglementaires pour faire appliquer des mesures liées à la cybersécurité et à la CIIP. Cet atelier devait intéresser les parties prenantes suivantes: décideurs en matière de technologies de l'information et de la communication dans les ministères et administrations de la région; institutions et départements responsables des politiques et législations dans le domaine de la cybersécurité et de leur mise en application; représentants des opérateurs, équipementiers, prestataires de services, associations de professionnels et de consommateurs qui cherchent à encourager une culture de la cybersécurité. Les participants à l'atelier ont également examiné des initiatives prises aux niveaux régional et international pour renforcer la coopération et la coordination entre ces différentes parties prenantes. Cet atelier a été suivi par quelque 120 personnes, venant de la région de l'Afrique de l'Ouest, y compris du pays hôte, le Cap-Vert, du continent africain dans son ensemble, ainsi que d'autres régions du monde. Une documentation complète sur l'atelier, comprenant l'ordre du jour définitif et tous les documents présentés, est affichée sur le site web correspondant (www.itu.int/itu-d/cyb/events/2007/praia/). Le présent document résume la teneur des trois jours de débats, donne un aperçu des sessions et des présentations des orateurs ainsi que de certaines prises de position communes.
Source : http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/praia-cybersecurity-workshop-report-dec-07- f.pdf
File : UIT_Atelier de lAfrique de lOuest sur les Cadres Politiques et Reglementaires.pdf

76. UIT. Genève

Question 22-1/1: sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité
Rapport final, UIT-D Commission d'études 1
Genève : Union internationale des télécommunications (UIT), 2014. – 300 p.
(5ème Période d'études 2010-2014, Secteur du développement des télécommunications)

Introduction : Dans le cadre de la Question 22-1/1 qui lui a été confiée, la Commission d'études 1 de l'UIT-D établit des rapports sur les bonnes pratiques concernant divers aspects de la cybersécurité. Il s'agit ici du rapport final sur les activités menées au titre de la Question 22-1/1 au cours du dernier cycle d'études de quatre ans, qui couvre la période 2010-2014. Le programme de travail du Groupe du Rapporteur pour la Question 22-1/1 a été défini par la Conférence mondiale de développement des télécommunications (CMDT) lors de la réunion qui s'est tenue à Hyderabad (Inde) en 2010. Au cours des quatre dernières années, le Groupe du Rapporteur pour la Question 22-1/1 a traité toutes les questions mentionnées dans le programme de travail, de manière partielle ou complète. Le rapport final sur la Question 22-1/1 se compose de plusieurs rapports sur les bonnes pratiques concernant différents aspects de la cybersécurité, à savoir 1) un guide pour la mise en place d'un système national de gestion de la cybersécurité; 2) les bonnes pratiques relatives à la création de partenariats entre le secteur public et le secteur privé visant à appuyer les buts et objectifs en matière de cybersécurité; 3) développer la capacité nationale de gestion des incidents liés à la sécurité informatique; 4) gérer un CIRT national à l'aide des facteurs essentiels de réussite; et 5) les bonnes pratiques en matière de protection des réseaux des fournisseurs de services Internet (ISP). De plus, l'Annexe E du présent rapport fournit des supports pour des cours de formation sur la création et la gestion d'un CIRT. En outre, une contribution décrivant un programme supplémentaire de cours en ligne pour les enfants a été présentée par la National Academy of Telecommunications A.S. Popov d'Odessa dans le cadre de l'étude de la Question. Le Groupe a également reçu des informations présentées par le BDT sur ses activités menées aux niveaux mondial et régional…
Source : http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22.1-2014-PDF-F.pdf
File : UIT_Question 22-1/1: sécurisation des réseaux d'information.pdf

77. VISNER, Samuel

Cyber Security's Next Agenda
Georgetown Journal of International Affairs, 2013-14, p. 89-99

Introduction: Since 2007, the United States has made considerable- -yet uneven- -progress in recognizing cyber threats to not only public sector and commercial information infrastructures, but also critical infrastructures that depend on information technology. The government must enhance cyber infra- structure security by focusing more strongly on information sharing and collaborative action as well as the cybersecurity of new information technologies, infrastructures, and applications, particularly those that unify traditional information technology systems with the operational systems that control infrastructures and manufacturing. Adding to the challenge is the asymmetry that exists

between U.S. and foreign conceptions of cybersecurity. Some countries, notably China and Russia, view cybersecurity as an instrument of state power and the cyberspace in which they operate as sovereign territory. At the same time, they understand that their cyber operations outside of that sovereign territory may represent willful incursions into other states' sovereign territory. This view contrasts strongly with the Western perspective, namely that cybersecurity pertains primarily to the protection of information, information systems, and the infrastructures that depend on information technology…
Source: Stable URL: http://www.jstor.org/stable/43134325
File: VISNER_Samuel_Cyber Securitys Next Agenda.pdf

78. VLADIMIR, Aman

Concevoir la sécurité informatique en entreprise : penser des stratégies efficaces dans la mise en œuvre de la sécurité informatique en entreprise

Introduction: Internet, a-t-on coutume de le dire, est un espace virtuel transfrontalier offrant d'énormes opportunités, tant sur les plans économique, scientifique, que culturel. Comme toute société humaine, ce monde virtuel reste soumis aux principes fondamentaux régissant « le monde réel ». Les sociétés humaines ont de tout temps consentis des efforts colossaux quant à l'édition de règles et de principes directeurs, définissant le cadre général de leur fonctionnement. Ainsi, depuis les codes d'Ur-Nammu et d'Hammourabi, jusqu'aux différents CODES (pénal, civil, etc.) de l'époque contemporaine, l'on a toujours tenté d'encadrer autant que possible le fonctionnement de la société humaine. Mais, les crimes et actes allant à l'encontre des principes érigés ont toujours existé et constituent même dans un sens, le moteur de l'appareil législatif.
Si son apparition nous a grandement simplifiés la vie, il est indiscutable que l'informatique nous a également apporté son corolaire de problèmes, inhérents à tous progrès scientifiques. De nos jours, presque tout est effectué par le biais de l'informatique : la sécurité, les transactions financières, la santé, l'administration (e- gouvernement), le divertissement, etc. Avec l'avènement des réseaux et du développement des TIC, la Sécurité des Systèmes d'Information (SSI) est devenue un sujet plus que capital, car de nos jours le système d'information (SI) est un élément absolument vital pour la plupart des entreprises.
Au-delà de la stratégie commerciale et marketing proprement dite, ce qui permet aux entreprises d'atteindre leurs objectifs et de distancer leurs concurrents est de loin le SI1, qui de ce point de vue apparait comme un outil vital pour celles-ci.
La mondialisation s'est avérée être un facteur déterminant dans le problème qui nous intéresse dans le cadre de cet ouvrage. En effet, la concurrence s'accroît davantage, ce qui potentialise les risques d'attaques de tous genres et offre plus de travail aux espions industriels et autres pirates informatiques.
Source:https://cybercrimactu.files.wordpress.com/2014/01/concevoir-la-sc3a9curitc3a9-informatique-en-entreprise_aman-vladimir1.pdf
File: VLADIMIR_Aman_Concevoir la sécurité informatique en entreprise.pdf

79. WATNEY, Murdoch

The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism
Journal of Digital Forensics, Security and Law, Vol. 2, N° 2, (2006)

Abstract: Internet regulation has evolved from self-regulation to the criminalization of conduct to state control of information available, accessed and submitted. Criticism has been leveled at the different forms of state control and the methods employed to enforce state control. After the terrorist attack on the USA on 11 September 2001, governments justify Internet state control as a law enforcement and national security tool against the abuse and misuse of the Internet for the commission of serious crimes, such as phishing, child pornography; terrorism and copyright infringement. Some Internet users and civil rights groups perceive state control as an abomination which results in an unjustifiable infringement of civil rights. Since countries worldwide are focusing attention on the control of information on the Internet, the debate in respect of state control and the consequences of state control is relevant on a global level as it impacts on all Internet-connected countries.
Source: http://ojs.jdfsl.org/index.php/jdfsl/article/view/198/144
File: WATNEY_Murdoch_The Evolution of Internet Legal Regulation.pdf

80. WESTBY, Jody R.

Countering Terrorism with Cyber Security
Jurimetrics, Vol. 47, N° 3, spring 2007, p. 297-313

Abstract: Terrorist cells in more than 60 countries are using information and communication technologies (ICTs) to recruit and spread propaganda, raise money, train jihadists, and communicate and conspire. Their high-tech strategy outpaces the traditional approach of the United States and other countries who are relying upon traditional strategies aimed at tracking, capturing, and killing an enemy. The three problems that most frustrate governments in countering terrorists' use of ICTs are (1) difficulties in tracking and tracing cyber communications, (2) the lack of harmonized laws and procedures in investigating cybercrimes, and (3) inadequate or ineffective information sharing. Governments around the globe need to address these three areas of cyber security if they are to hope to win the battle against terror.
Source: http://www.jstor.org/stable/pdf/29762975.pdf
File: WESTBY_ Jody R_Countering Terrorism with Cyber Security.pdf

81. WOLTER, Detlev

The UN Takes a Big Step Forward on Cybersecurity
Arms Control Today, Vol. 43, N° 7, September 2013, p. 25-29

Introduction: By acknowledging the full applicability of international law to state behavior in cyberspace, by extending traditional transparency and confidence-building measures, and by recommending international cooperation and capacity building to make information and communications technology (ICT) infrastructure more secure around the world, the report lays a solid foundation for states to address the mutual risks that arise from rapidly increasing cyberthreats. For the United Nations, it was high time to act to address this new international security challenge. Increasingly, more-sophisticated…
Source: http://www.jstor.org/stable/23629424
File: WOLTER_Detlev_ The UN Takes a Big Step Forward on Cybersecurity.pdf

82. ZIOLKOWSKI, Katharina, Ed.

Peacetime Regime for State activities in Cyberspace: International Law, International Relations and Diplomacy
Tallinn: NATO CCD COE, 2013. – 782 p.

Introduction: Stability and security in international relations are preconditioned by predictability of State behaviour. The latter requires a common understanding within the international community with regard to the very core of applicable rules of international law, contemporary concepts of international relations and diplomatic agendas. With regard to cyberspace, the development of such a common understanding is in its early days. By offering a broad overview of the relevant topics and proposing interpretive approaches, this volume aims to bring increased clarity to this complex and important subject and to support further discussions within the international community of States.
The choice of focus on peacetime is vindicated by the fact that the vast majority of malicious cyber activities relevant to international relations occur during peacetime. Worldwide, nearly 200,000 new malware samples are identified each day; governmental, commercial and private computers are being probed every minute and sometimes hacked sucessfully. Additionally, the peacetime regime for State activities is, generally speaking, not automatically suspended during times of armed conflict, but rather augmented or partly amended. This applies also to governmental activities undertaken in order to 'maintain or restore international peace and security' as authorised by the United Nations Security Council under its powers pursuant to Chapter VII of the Charter of the United Nations…
Source: https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf
File: ZIOLKOWSKI_Katharina_Peacetime Regime for State activities.pdf

83. YUEN, Samson

Devenir une cyber-puissance : le renforcement de la politique de cybersécurité chinoise et ses conséquences
Perspectives chinoises, N° 2, 2015, p. 55-61

Introduction : Le 21 janvier 2015, les internautes chinois essayant d'accéder à des sites ou des applications censurés ont rencontré des difficultés pour se connecter à certains réseaux privés virtuels (VPN), un outil très répandu de contournement de la censure dans un pays où le contrôle du gouvernement sur Internet est notoire. Astrill, StrongVPN et Golden Frog, trois fournisseurs importants de VPN commerciaux ayant signalé des interruptions de service, ont tous imputé l'ingérence aux autorités chinoises en charge du cyberespace. Ils prétendent que l'attaque a été menée à un niveau de sophistication jamais atteint jusqu'alors (1).
Possédant le nombre d'internautes le plus élevé au monde – plus de 600 millions d'utilisateurs –, la Chine est déjà connue pour son contrôle très restrictif d'Internet, contrôle qui s'inscrit dans la vaste surveillance du flux d'informations par le gouvernement, allant des médias à la culture. Un rapport récent de l'organisation Freedom House détaille les

techniques sophistiquées du gouvernement pour imposer le contrôle de l'information, que ce soit le contrôle stratégique des nœuds de communication clés, l'externalisation de la censure, une direction plus forte du Parti, un nouvel accent sur l'idéologie, ou une répression des réseaux sociaux (2). Mais jusqu'à présent, les autorités chinoises se sont abstenues d'intervenir sur les VPN, qui laissent une légère ouverture aux internautes chinois – de l'utilisateur ordinaire aux élites privilégiées – pour profiter d'un Internet non entravé pour les loisirs ou pour une utilisation professionnelle. La chasse aux VPN suggère donc une nouvelle réflexion gouvernementale au sujet du contournement de la censure, ou du Grand Pare-feu chinois. Comment expliquer ce changement ? Et pourquoi à ce moment précis ?
Source : http://www.cefc.com.hk/fr/la-recherche/actualites-chine/synthese-de-presse-du-cefc/
File : YUEN_Samson_ Devenir une cyber-puissance.pdf

PART III / 3ème PARTIE

ANNEXES

Announcement / Annonce

III - Annexes: Announcement/Annonce

DEMOCRATIC GOVERNANCE INSTITUTE

Topic: **The African State and Public Cyber-Security Service**
Date: 18 – 29 **July 2016**
Venue: **Dakar, Senegal**

Call for Application: 2016 Session

The Council for the Development of Social Science Research in Africa (CODESRIA) is pleased to announce the 2016 session of its Democratic Governance Institute. Researchers are invited to send their applications for that institute which will take place from 18 – 29 **July 2016** in Dakar, Senegal.

The CODESRIA Democratic Governance Institute, which was launched in 1992, is an annual interdisciplinary forum which brings together about fifteen researchers from various regions of the continent and the Diaspora as well as a few non-African researchers conducting innovative research on topics related to the general topic of governance.

Structure
The Institute's sessions are supervised by a scientific director who, with the support of carefully selected resource persons, ensures that a large spectrum of research and policy issues is presented to the laureates. Each laureate is expected to write an article from his/her research work for presentation during the Institute. The revised version of the articles will be peer-evaluated for publication by CODESRIA. The CODESRIA Documentation and Information Centre (CODICE) will provide participants with a comprehensive bibliography on the topic of the Institute. The participants will also have access to the facilities of a number of documentation centres in and near Dakar.

Languages
The CODESRIA Democratic Governance Institute's working languages will be English and French. Simultaneous translation will be available during the session.

The 2016 Democratic Governance Institute: "The African State and public cyber-security service **"**

The 2015 Democratic Governance Institute session's topic was "Cyber-Security, Sovereignty and Democratic Governance in Africa". Among its recommendations was the need to deepen understanding on the theme of cyber-security by holding a second session. Thus the topic of the 2016 Institute is: "The African State and Public Cyber-Security Service".

In an environment marked by growing insecurity, a widening digital gap at the expense of Africa, which, just like poverty, is becoming commonplace, the continent has not yet benefitted from all the advantages of the digital era but rather, undergoes more than anywhere else in the world its adverse effects. The collective work of the 2015 session researchers has enabled the study of cases that illustrate that democratic cyber-governance is at work; cyber-citizenship is under construction; Africa is starting to develop responses to cyber-threats and is aware of the need for building a prospective vision of cyber-security governance.

It is in the perspective of building a relevant and efficient cyber-security governance system that this year's session is organized around the topic of public cyber-security service.

African States are settling in a digital vulnerability which spares no sector and, consequently, must protect themselves against the risk of digital dependency by encouraging thought on the place of digital technologies in the management of security and strategic threats (cyber-spying, cyber-sabotage, cyber-terrorism, cyber-war, etc.).

At the same time, the growing dematerialization of public service activities exposes the State and territorial communities to new computer-based threats in a period of more complex cyber-criminality and there is an increase of sensitive data leakages, loss of intellectual property, insecurity of crucial infrastructure exacerbated by the development of innovative technology (the multiplication of connected devices, cloud computing, social computing and next

generation mobile computing). To add to this, the legal and regulatory framework is not always in alignment with current cyber-security challenges, which raises the issue of conciliating digital risks management with the requirement of the permanence of public service.

These are issues calling for reflection during the 2016 Democratic Governance Institute.

The overall objective of the 2016 session is to anticipate on the construction of an African vision of public cyber-security service with a view to strengthening state integrity and sovereignty in Africa.

Several specific objectives will also be considered among which are:

- the conceptual and legal grounding of public cyber-security service ;
- The analysis of public service principles (continuity, equality, mutability) as against a fully digital environment, specifically in relation to cyber-security;
- The analysis of the State's capacity to implement public cyber-security service;
- Reflection on the role and place of the various users: internal users (civil-servants and other stakeholders) and public service users;
- Analysis digital identify and access management systems with regards to the e-administration and cyber-surveillance of public spaces;
- Analysis of protection regimes of critical infrastructure, data and intellectual property;
- Reflection on ways and means for strengthening political and legal cooperation in cyber-security matters.

The 2016 session of the Democratic Governance Institute will cover a large spectrum of topics around the five axes below:

1. Public policies for sovereign public cyber-security service
2. Ethical issues and cyber-security culture
3. The models of digital administration and e-governance
4. Compliance and legal surveillance of cyber-security, and
5. Public service and usages in matters of cyber-security.

The Director

Professor Abdoullah Cissé, an expert in cyber-law and cyber-security, will lead the 2016 session of the Democratic Governance Institute. He will ensure the following tasks:

- Read and comment on the laureates' proposals before the kick-off of the Institute;
- Develop the Institutes' lectures, including the specific sub-topics;
-Give a series of conferences and conduct a critical analysis of the submissions presented by the resources persons and the laureates;
-Draft and submit a scientific report on the session;
-(Co-) edit the revised versions of the submissions presented by the resource persons towards their publication in one of the CODESRIA's collections. For publication purposes, the Director will also assist CODESRIA in the evaluation of the submissions presented by the laureates during the Institute.

The Resource Persons

The objective of the lectures which will be given during the Institute is to provide the laureates with the opportunity to deepen their thinking on the topic. Consequently the resource persons will be confirmed academics or researchers who have published vastly on the topic and who have an important contribution to make in the debates. They will produce written materials which will incite the laureates to engage the discussions and debates on their papers as well as on all the available documentation on the topic.

Once selected, the resource persons must:

- Interact with the Director of the Institute and the laureates to help the latter readjust their research questions and their methodological approaches;
- -Submit a copy of their course materials for reproduction and circulation to the participants no later than a week before the presentation of their lectures;
- -Give their lectures, participate in the debates and comment on the laureates' research proposals and articles;
- -Submit an article based on their lecture notes for publication by CODESRIA no later than two months after the Institute.

The Laureates
The applicants must be PhD students writing their theses or scholars at the beginning of their careers with proven capacity to conduct research on the topic of the Institute. Intellectuals active in the political process and/or in social movements and civil society organizations are also encouraged to apply. The number of places offered by CODESRIA for this session is ten (10) maximum. Non-African researchers who can finance their participation can also apply within the limits of the available places.

Application Files
The resource persons' application files must contain:

1. A letter of application;
2. A curriculum vitae;
3. Two (2) published articles;
4. A proposal of five (5) pages maximum describing the topics which will be dealt with in their **three (3) lectures**, one of which will focus on methodology issues.

The laureates' application files must contain:

1. A letter of application;
2. A letter testifying to his/her institutional or organizational affiliation;
3. A curriculum vitae;
4. A research proposal of ten (10) pages maximum which includes a descriptive analysis of the work the applicant wants to undertake, a summary explaining the theoretical interest of the topic chosen by the candidate, the relationship between the topic and the problematic and centres of interest taken into account by the 2015 Institute's topic;
5. Two (2) letters of reference from renowned academics or researchers with competence and expertise in the area of the applicant's research (from the geographical point of view and in relation to the discipline), with their names, addresses, telephone numbers and electronic mail addresses.
6. A copy of the applicant's internationalpassport.

Deadline for Applications
Deadline for application is 30 April 2016. Laureates will be informed of the selection results in the last week of May 2016. It is expected that June willbe used to finalize field work or collect information to prepare the draft research report to be presented during the Institute. That research report must be submitted to CODESRIA by 30 June 2016 at the latest. Laureates will have to work on that document (and not on the proposal's summary) and prepare it for publication during the Institute.

Submission of Applications
All application or additional information requests should be sent by email to: governance.institute@codesria.sn

For specific questions, please contact:

The Democratic Governance Institute
CODESRIA
Avenue Cheikh Anta Diop x Canal IV
BP 3304, CP 18524, Dakar, Sénégal
Tél. : (221) 33 825 98 21/22/23
E-mail : governance.institute@codesria.sn
http://www.codesria.org/
http://www.facebook.com/pages/CODESRIA/181817969495
http://twitter.com/codesria

INSTITUT SUR LA GOUVERNANCE DEMOCRATIQUE

Thème : **L'Etat africain et le service public de la cybersécurité**
Date : **18-29 juillet 2016**
Lieu : Dakar, Sénégal

Appel à candidatures : Session 2016

Le Conseil pour le développement de la recherche en sciences sociales en Afrique (CODESRIA) a le plaisir d'annoncer la session 2016 de son Institut annuel sur la Gouvernance démocratique. Il invite les chercheurs à soumettre leurs candidatures afin de participer à cet institut devant se dérouler du **18 au 29 juillet 2016** à Dakar (Sénégal).

L'Institut sur la gouvernance démocratique lancé en 1992 par le CODESRIA est un forum interdisciplinaire qui réunit chaque année une quinzaine de chercheurs provenant des diverses régions du continent et de la diaspora, ainsi que quelques chercheurs non africains qui entreprennent des recherches innovantes sur des sujets liés au thème général de la gouvernance.

Organisation
Les sessions de l'institut sont dirigées par un directeur scientifique qui, avec le soutien de personnes ressources, s'assure qu'un large éventail de recherches et de questions politiques est exposé aux lauréats. Chaque lauréat doit rédiger un article découlant d'un travail de recherche destiné à être présenté durant l'institut. La version révisée de l'article fera l'objet d'une évaluation par les pairs en vue de sa publication par le CODESRIA. Le Centre de documentation et d'information du CODESRIA (CODICE) mettra à la disposition des participants une bibliographie aussi complète que possible se rapportant au thème de l'institut. Les participants auront également la possibilité d'accéder à un certain nombre de centres de documentation situés à Dakar et dans ses environs.

Langues
L'Institut sur la gouvernance démocratique du CODESRIA se tiendra en français et en anglais par le biais d'un système de traduction simultanée.

L'Institut sur la Gouvernance 2016 : « L'Etat africain et le service public de la cybersécurité »

La session 2015 de l'Institut sur la gouvernance démocratique a été consacrée au thème « Cybersécurité, souveraineté et gouvernance démocratique en Afrique ». Elle a formulé, entre autres recommandations, la nécessité d'approfondir la thématique de la cybersécurité à travers notamment l'organisation d'une seconde session de l'Institut sur le thème : « l'Etat africain et le service public de la cybersécurité ».
Dans un environnement marqué par une insécurité grandissante, la fracture numérique se creuse au détriment de l'Afrique en se banalisant, à l'instar de la pauvreté. Le continent ne profite pas encore de tous les avantages du numérique mais en subit, plus que tous, les travers. La réflexion collective des chercheurs de la session 2015 a permis d'étudier des cas qui illustrent que la cybergouvernance démocratique est en marche, que la cybercitoyenneté est en construction, que l'Afrique commence à ébaucher des réponses face aux cybermenaces et qu'elle est consciente de la nécessité de construire une vision prospective de la gouvernance de la cybersécurité.
C'est dans la perspective de bâtir un système pertinent et efficace de gouvernance de la cybersécurité que la présente session est organisée autour de la problématique du service public de la cybersécurité.
Les Etats africains s'installent de plus en plus dans une vulnérabilité numérique qui n'épargne aucun secteur et doivent, en conséquence, se prémunir contre le risque de dépendance numérique en encourageant la réflexion sur la place du numérique dans la gestion de la sécurité et de la menace stratégique (cyberespionnage, cybersabotage, cyberterrorisme, cyberguerre etc.).
Dans le même temps, la dématérialisation croissante des activités de service public expose l'Etat et les collectivités territoriales à de nouveaux risques informatiques au moment où la cybercriminalité se complexifie et où l'on assiste de plus en plus à la fuite de données sensibles, à la perte de propriété intellectuelle, à l'insécurité des infrastructures essentielles exacerbées par le développement des technologies de rupture (la multiplication des objets connectés, le développement de l'informatique en nuage, l'informatique sociale et l'informatique mobile de prochaine génération). Il s'y ajoute que le cadre juridique et réglementaire n'est pas toujours en phase avec les défis du moment en matière de cybersécurité, ce qui pose la question de la conciliation de la gestion des risques numériques avec l'exigence de continuité du service public.

Autant de questions qui interpellent les participants à la session 2016 de l'Institut de la Gouvernance.

L'objectif global de la session 2016 est d'anticiper la construction d'une vision africaine du service public de la cybersécurité en vue du renforcement de l'intégrité et de la souveraineté de l'Etat en Afrique.
Plusieurs objectifs spécifiques sont poursuivis dont notamment :

- construire l'assise conceptuelle et juridique du service public de la cybersécurité ;
- analyser les principes du service public (continuité, égalité, mutabilité) à l'épreuve du tout-numérique et particulièrement de la cybersécurité ;
- analyser la capacité de l'Etat à assurer le service public de la cybsersécurité ;
- réfléchir sur le rôle et la place des publics d'utilisateurs : utilisateurs internes (agents de la fonction publique et autres intervenants) et usagers du service public ;
- analyser les systèmes de gestion de l'identité numérique et des accès en regard avec la dématérialisation de l'administration et la cybersurveillance des espaces publics ;
- analyser les régimes de protection des infrastructures essentielles ainsi que de protection des données et de la propriété intellectuelle ;
- étudier les voies et moyens du renforcement de la coopération politique et juridique en matière de cybersécurité.

La session 2016 de l'Institut sur la gouvernance démocratique couvrira un large éventail de thèmes articulés autour des cinq axes suivants :

6. les politiques publiques pour un service public souverain de la cybersécurité ;
7. Les questions éthiques et la culture de cybersécurité ;
8. Les modèles d'administration électronique et d'e-gouvernance ;
9. La conformité et l'encadrement juridique de la cybersécurité ;
10. Le service public et les usages en matière de cybersécurité.

Le Directeur
Le Professeur Abdoullah Cissé, expert en cyberdroit et cybersécurité, dirigera la session 2016 de l'Institut sur la Gouvernance démocratique. En tant que Directeur de l'institut, il assurera les tâches suivantes :
- Lire et commenter les propositions des lauréats avant le démarrage de l'Institut sur la gouvernance.
- Concevoir les cours de la session, notamment les sous-thèmes spécifiques.
- Faire une série de conférences et mener une analyse critique des communications présentées par les personnes ressources et les lauréats.
- Rédiger et soumettre un rapport scientifique relatif à la session.
- (Co-)éditer les versions révisées des communications présentées par les personnes ressources, en vue de leur publication dans l'une des collections du CODESRIA. Pour la publication, le Directeur devra également assister le CODESRIA dans l'évaluation des communications présentées par les lauréats au cours de l'Institut.

Les personnes ressources
Les cours devant être dispensés durant l'institut sont destinés à offrir aux lauréats l'occasion d'approfondir leurs réflexions sur le thème. Les personnes ressources doivent, par conséquent, être des universitaires ou des chercheurs confirmés qui ont beaucoup publié sur le sujet, et qui ont une contribution importante à apporter aux débats. Elles devront produire des supports écrits qui inciteront les lauréats à engager la discussion et le débat sur leur exposé ainsi que toute la documentation disponible sur le thème.
Une fois sélectionnées, les personnes ressources doivent :
- Interagir avec le directeur de l'institut et les lauréats afin d'aider ces derniers à réajuster leurs questions de recherche et leur approche méthodologique ;
- Soumettre un exemplaire de leurs supports de cours pour reproduction et distribution aux participants au plus tard une semaine avant la présentation de leurs exposés ;
- Présenter leur exposé, participer aux débats et commenter les propositions de recherche et les articles des lauréats ;
- Soumettre un article basé sur leurs notes de cours pour publication par le CODESRIA au plus tard deux mois après l'institut.

Les lauréats
Les candidats doivent être des étudiants en thèse ou des universitaires en début de carrière, ayant une capacité prouvée à faire de la recherche sur le thème de l'Institut. Les intellectuels actifs dans le processus politique et/ou dans les mouvements sociaux et les organisations de la société civile sont également encouragés à se porter candidats. Le nombre de places offertes par le CODESRIA pour la session est limité à dix (10). Les chercheurs non-africains qui peuvent financer leur participation peuvent également faire acte de candidature sous réserve des places disponibles.

Les dossiers de candidature
Les dossiers de candidature des personnes ressources doivent comprendre :
1. Une lettre de candidature ;
2. Un curriculum vitae ;
3. Deux (2) articles publiés
4. Une proposition de cinq (5) pages au plus, décrivant les questions qui seront couvertes dans leurs **trois (3) exposés** dont un portant sur les questions de méthodologie ;

Les dossiers de candidature des lauréats doivent comprendre :
1. Une demande de candidature ;
2. Une lettre attestant de l'affiliation institutionnelle ou organisationnelle ;
3. Un curriculum vitae ;
4. Une proposition de recherche (de dix (10) pages au plus en deux exemplaires), comprenant une analyse descriptive du travail que le candidat veut entreprendre, un résumé exposant l'intérêt théorique du thème choisi par le candidat, la relation entre le sujet et la problématique et les centres d'intérêt pris en compte par le thème de l'Institut 2015 ;
5. Deux (2) lettres de référence provenant d'universitaires ou de chercheurs connus pour leur compétence et leur expertise dans le domaine de recherche du candidat (du point de vue géographique et concernant la discipline), avec leurs noms, adresses, numéros de téléphone et/ou de fax et adresses électroniques.
6. Une copie du passeport.

Date limite de soumission des candidatures
La date limite de soumission des candidatures est fixée au **30 avril 2016**. Les lauréats seront informés du résultat de la sélection dans la dernière semaine du mois de mai **2016**. Le mois de juin pourra ainsi être utilisé pour mener à bien un travail de terrain ou recueillir de l'information pour préparer le projet de rapport de recherches à présenter lors de l'institut. Ce rapport de recherches devra être soumis au CODESRIA au plus tard le **30 juin 2016**. Les lauréats seront appelés à travailler sur ce document (et non sur le résumé de la proposition) et le préparer pour publication au cours de l'Institut.

Soumission des candidatures
Toutes les candidatures ou demandes de renseignements complémentaires devront être adressées à :

Institut sur la Gouvernance démocratique
CODESRIA
Avenue Cheikh Anta Diop x Canal IV
BP 3304, CP 18524, Dakar, Sénégal
Tél. : (221) 33 825 98 21/22/23 - Fax : (221) 33 824 12 89
E-mail : governance.institute@codesria.sn
Pour des renseignements complémentaires, consultez le site : http://www.codesria.org/
Visitez notre page Facebook : http://www.facebook.com/pages/CODESRIA/181817969495
Suivez l'actualité sur Twitter : http://twitter.com/codesria