# CYBERCRIMINALITE ET CYBERSECURITE COMME OBJETS SCIENTIFIQUES: ETAT DE LA RECHERCHE RECENTE EN AFRIQUE

**GUY MVELLE**

PROFESSEUR DES UNIVERSITES

DIRECTEUR SCIENTIFIQUE DU COLLOQUE

SECRETAIRE GENERAL DE L'UNIVERSITE DE DSCHANG

# « NOTRE LIBERTE EST MENACEE PAR LE BESOIN DE SECURITE ET LA SECURITE ELLE-MEME EST MENACEE PAR LE SOUCI OBSEDANT QU'ON EN A »

Norbert BENSAID (1922-1994)

Médecin psychanalyste exerçant à Paris

1970-1993: Des appareils de cryptage truqués sont vendus à plus de 120 pays par la société suisse CRYPTO AG pour fournir des renseignements aux services secrets américains et ouest-allemands
Des phreakers modifient du matériel et des logiciels pour voler du temps de téléphone à longue distance (appels internationaux)
42 ordinateurs et plus de 20 000 disquettes saisies par le FBI sur les cartes bancaires et les services téléphoniques

## EUROPE/AMERIQUE

- **1999**: Attaque des sites web de l'OTAN par des nationalistes serbes
- **2007**: cyberattaque conflit russo-géorgien, conflit en Estonie…
- **2013**: Affaire Edouard Snowden (CIA et NSA) et multiplication des cyberattaques de plus en plus sophistiquées (programmes de surveillance de masse)

## AFRIQUE

**2017:** Attaque de plusieurs pays par des logiciels de rançon: Maroc, Algérie, Tunisie, Egypte, Sénégal, Ouganda, Sud-Soudan, Côte d'Ivoire, Kenya, Namibie, Zimbabwe, Madagascar…

**2018:** Constat alarmant de l'UIT sur la vulnérabilité de la presque totalité des pays africains (excepté Ile Maurice, Kenya et Rwanda)

**U**ne augmentation et sophistication des actes criminels sur le cyber espace malgré l'absence de données statistiques suffisantes et actualisées, malgré l'adoption de nouvelles législations et des actions des sensibilisation et prévention par les Etats

## CAMEROUN

- **2011:** Camair-Co victime d'une piraterie de 500 billets d'avion
- **2015-2017**: 7 sites web d'administrations publiques victimes d'attaques de type web defacement (modification non sollicitée de la présentation d'un site Web),
- 34 sites gouvernementaux attaqués par des programmes malveillants

## CAMEROUN

- Plusieurs centaines de cas d'usurpations d'identités dont celles de 182 membres du gouvernement
- Environ 4 milliards de pertes économiques liées au *scamming* (escroquerie ou cyber arnaque, fraude 419)

**Classification**: cyber hacktivisme ou cyber vandalisme, cyber crime, cyber espionnage, cyber terrorisme, cyber guerre (*Center for Security Studies, 2010*): **un brouillard sémantique? Cybercriminalité un terme générique!**

## Cybercriminalité/UA

- « actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes, technologies de l'information et de la communication, les données et les infrastructures réseaux sous-jacentes » (art. 25 Conv. UA sur la cyber sécurité et la protection des données personnelles, 2014).

## Cybercriminalité/CMR

- « Ensemble des infractions s'effectuant à travers le cyber espace par d'autres moyens que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique » (Art. 4, loi du 21/12/2010 sur la cyber sécurité et la cybercriminalité au CMR).
- « Activités qui consistent à utiliser les systèmes et réseaux informatiques en général et internet en particulier pour poser les actes criminels et proscrits par la loi » (ANTIC)

# De multiples autres définitions

- ONU: 10e congrès des Nations unies à Vienne, avril 2000
- Conseil de l'Europe: Convention sur la cybercriminalité, Budapest, 2001 (formes traditionnelles de crimes, publication des contenus illicites par voie électronique, infractions propres aux réseaux informatiques)
- UIT: Guide pour comprendre la cybercriminalité, 2009
- Département de la justice américaine
- Office de police suisse
- Computer Emergency Response Team (CERT)

# Définitions de la cyber sécurité: entre prudence et audace

- **Cyber sécurité/ UA**
- Pas définition de la cyber sécurité
- Objectif: harmonisation des législations, encouragement de la mise en place des dispositifs nationaux de cyber sécurité
- Enumération des infractions spécifiques aux TIC: atteintes aux systèmes informatiques, aux données informatisées, infractions se rapportant au contenu, et aux mesures de sécurisation des échanges électroniques.

- **Cyber sécurité/ CMR**
- « Ensemble de mesures de **prévention**, de **protection** et de **dissuasion** d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes » (Art. 4, loi du 21/12/2010 sur la cyber sécurité et la cybercriminalité au CMR).

# Acteurs de la cybercriminalité

## Acteurs (Hackers ou brouteurs)

- Criminels ordinaires faisant usage des TIC
- Ex-employés désireux de se venger suite à leur licenciement
- Entreprises espionnant leurs concurrents
- Etudiants désireux d'éprouver leur maitrise des TIC
- Toute personne malveillante opérant à partir des TIC

## Acteurs (Hackers ou brouteurs)

- Les services d'espionnage gouvernementaux
- Terroristes
- Utopistes désirant mettre internet à la portée de tous
- Les charlatans

# Les buts de la cybercriminalité

## Buts

- Vol d'informations ou de service à des fins pécuniaires
- Destruction des systèmes
- Nuisance à la réputation d'autrui
- Dégradation de la qualité des services
- Test de technicité et de la capacité de nuisance
- Fraudes économiques et financières

## Buts

- Revendications politiques, religieuses, corporatistes, idéologiques…
- Escroquerie
- Philanthropie: désintéressement, accès de tous aux ressources numériques

# Les modes opératoires de la cybercriminalité

**Modes opératoires**

- **Phishing ou hameçonnage:** usurpation d'identité pour dérober des données personnelles
- **Spamming:** inondation des courriels indésirables pour des fins publicitaires
- **Logiciels malveillants:** zombies ou botnet
- **Virus:** destruction et atteinte négative du fonctionnement des systèmes
- **PUPs:** logiciel désinstallant les logiciels utiles dans votre système
- **Scamming**: escroquerie en ligne
- **Defacement**: défiguration des sites
- **Black markets**
- **Attaque DDos**
- **Cyberromance:** manipulations romantiques et sexuelles à des fins d'escroquerie et de criminalité
- **Cyber charlatanisme:** manipulations mystiques miroitant des gains et des succès à venir

# Les principales catégories techniques

- **Crimes visant des réseaux ou des appareils informatiques:** usages de tous les logiciels malveillants possibles: virus informatique, vers, cheval de Troie, rasomware, spyware, adware, scareware, attaques Ddos (saturation de la bande passante d'un serveur, épuisement des ressources système d'un machine), etc.

- **Crimes utilisant des dispositifs numériques pour participer à des activités criminels**: phishing mail (ou hameçonnage: usurpation d'identité pour dérober des données personnelles), cyber harcèlement, vol d'identité, Cyberromance, Cyber charlatanisme, etc.

**Problématique:** La cybercriminalité et la cyber sécurité sont-elles saisies par la recherche en Afrique et au Cameroun?

**Hypothèse:** Deux objets effectivement saisis par la recherche africaine mais qui doivent être renouvelés et élargis dans le cadre d'un dialogue des disciplines et d'une pluralité des regards

---

**I/ Des objets saisis par la recherche africaine**

- **La double décennie 1990-2010, le droit pénal et les infractions à partir des TIC**
  - Diouf Ndiaw: infractions en relation avec les NTIC et procédures pénale: l'inadaptation des réponses nationales face à un phénomène de dimension internationale
  - J.P. Malonga Younas: La répression des agissements liés aux nouvelles technologies de l'information au Congo (2003)
  - A. Kabore: La problématique des perquisitions et saisies en ligne en Afrique de l'ouest: Burkina Faso, Mali, Sénégal et Togo (2007).

# I/ Des objets saisis par la recherche africaine

- Medhat Ramadan: sur « Legal protection of e-commerce » (2001) et « Attacks on individuals and Internet » (2004).
- E. Elsonbaty « Cybercrime : insights from the Egyptian law » (2007)
- H. Ghafry examine « The role of Internet in software piracy » (2009)
- H. Ahwany « Protection of intellectual property rights on the Internet » (2009).
- O.B. Longe: « Cybercrime and Criminality in Nigeria : What roles are Internet Access Point Playing ? (2008)
- D. Olowun a pour préoccupation « Cybercrimes and the Boundaries of Domestic Legal Responses : case for an inclusionary framework for Africa » (2009).

# I/ Des objets saisis par la recherche africaine

- CRDI: Exploration de la cybercriminalité et la sécurité en Afrique : état des lieux et priorités de recherche; Afrique du Sud, Egypte, Cameroun, Ghana, Kenya, Nigéria, Maroc et Sénégal (2011).
- Edouard Epiphane Yogo dans « La cybersécurité et la cyberdéfense au Cameroun » (2015)
- Anmonka Jeannine: la répression de la cybercriminalité dans les Etats de l'UE et de l'Afrique de l'Ouest, thèse de droit public, Paris V, 2015
- Samuel Tepi: examine la cybercriminalité au Cameroun sous le prisme des enjeux d'une législation en quête d'efficacité (2020).
- Edi Donal Kuate: Les problèmes juridiques contrariant la répression internationale de la cybercriminalité, (2020).

# I/ Des objets saisis par la recherche africaine

- Les problèmes nouveaux qu'entraîne la cybercriminalité dans le droit pénal de fond et la procédure pénale (difficile administration de la preuve, l'impossibilité des poursuites)
- Les questions légales et règlementaires entravant l'existence, l'effectivité, et l'efficacité d'un traitement approprié de la cybercriminalité
- La protection juridique des activités commerciales en ligne
- La protection de la propriété intellectuelle
- La cybercriminalité et les limites des réponses juridiques nationales
- La pertinence et l'applicabilité de la loi camerounaise de 2010
- La sauvegarde des libertés des individus par rapport à leurs données personnelles

**Fin Partie 1**

# II/ DES OBJETS DE RECHERCHE A ELARGIR ET A RENOUVELER

- **Les études philosophiques, psychologiques sociologiques:** problème de la quantification du crime en ligne, observation de la surveillance inversée, représentations sociales sur la cybercriminalité, psychologie des cybercriminels, la déshumanisation et l'incivisme dans le cyberespace…
- **Etudes politiques, diplomatiques et stratégiques:** l'action de l'Etat au quotidien et au concret, la sécurisation des infrastructures critiques, la transposition des paradigmes classiques à la cyberguerre, Prévention, gestion et lutte contre les cyberattaques par les FDS, les dérives de l'administration à l'égard des administrés

**Etudes économiques, financières et managériales:** évaluation des cyberattaques et de la cyber sécurité dans les entreprises, gestion du risque cyber par les entreprises, rémunération des cyber protecteurs, incidences des cyberattaques sur la productivité des entreprises, le Change management…

# II/ DES OBJETS DE RECHERCHE A ELARGIR ET A RENOUVELER

## Dans le domaine des SI

- Le *machine learning*
- Les modèles d'accès basés sur la confiance zéro
- La modélisation des serveurs d'identité
- Les nouveaux débats sur la cryptologie
- La maturité de la sécurité des TIC en Afrique

## Dans le domaine des SI

- **la blockchain:** registre public de qui détient quoi en ordre chronologique et mis à jour automatiquement
- **Internet des objets:** Connection des objets physiques capables de communiquer les uns avec les autres (Colloque UDs)
- **Intelligence artificielle:** la simulation de l'intelligence humaine à travers les machines= permettre à des ordinateurs d'agir et penser comme des êtres humains…

# II/ DES OBJETS DE RECHERCHE A ELARGIR ET A RENOUVELER

- **Robotique**: Techniques permettant la conception et la réalisation des machines automatiques ou robots (mécatroniciens, opérateurs de commandes numériques, techniciens de maintenance, etc)
- **Identité digitale ou numérique:** lien technologique entre une entité réelle et une entité virtuelle. Identification de l'individu en ligne ainsi que sa mise en relation avec l'ensemble des communautés virtuelles présentes sur le Web
- **Les big data ou mégadonnées** (petaoctets, zettaoctets, etc): ensemble des données numériques produites par l'utilisation NTIC à des fins personnelles ou professionnelles: données d'entreprises, données issues des capteurs, des contenus publiés sur le web, des transactions du commerce électronique, échanges sur les réseaux sociaux, etc. **Fin Partie 2**

# CONCLUSION GENERALE

- Le cyberespace: du pacifique village globale plein d'opportunités au champs d'affrontement, d'escroquerie, de haine, d'espionnage, de rançonnage, etc.
- Défis stratégiques, sécuritaires, politiques et sociaux pour les gouvernements, les collectivités, groupes organisés, individus, etc.
- Défis pour le partenariat public-privé (synergie incontournable en le secteur public et les firmes de télécoms)
- Défis économique pour les entreprises (pertes économiques, rentabilité, réputation…)
- Défis sociopolitique: cohésion nationale, la paix sociale, et l'unité nationale

# CONCLUSION GENERALE

- Défis heuristique pour le monde universitaire: renouveler et élargir sa réflexion (interdisciplinaire et pluridisciplinaire)
- Défis académique= e-National higher Education
- Défis pour les sciences et les techniques de l'informatique: réinventer et analyser chaque jour de nouveaux outils de lutte contre la cybercriminalité
- Défis pour le Cameroun et l'Afrique face aux espoirs portés sur le e-commerce, la digitalisation de l'administration, la sécurisation des infrastructures critiques, l'arrimage général à la mondialisation…

# CONSEILS PRATIQUES

- 1.Devenez vigilants lorsque vous naviguez sur des sites web
- 2. Signalez les mails suspects
- 3. Ne cliquez jamais sur les liens ou des annonces provenant des gens que vous ne connaissez pas
- 4.Utilisez un VPN (réseau privé virtuel): tunnel sécurisé entre vous et internet
- 5. Assurez-vous que les sites web sont sécurisés avant d'entrer les informations d'identification
- 6. Maintenez vos antivirus et applications à jour
- 7. Evitez le transfert systématique d'informations avant plusieurs vérifications

# FIN DE LA LECON

- **« LE SEUL MOYEN D'ETRE SAUF C'EST DE NE PAS SE CROIRE EN SECURITE »**

THOMAS FULLER, Physicien anglais

guymvelle@gmail.com