Table des matières.

1. **QU'EST-CE QUE LA CYBERCRIMINALITÉ** ?..... 9
Une activité criminelle comme une autre
• De la cybernétique au cyber-crime
• Une dimension juridique et éthique – *Une question de loi – Une question de culture – La Convention européenne sur la cybercriminalité*
• Des atteintes aux personnes – *De multiples escroqueries – Trop beau pour être honnête – Faux intermédiaires de confiance*
• Des atteintes aux organisations – *Manipulation des marchés financiers – Monnaies virtuelles – Espionnage, fuite et pillage de données*
• Des atteintes aux États
• Des atteintes aux critères de sécurité informatique – *Disponibilité – Confidentialité – Intégrité – Manipulation de l'information et fausses nouvelles*
• Les problèmes de sécurité n'ont pas forcément une origine criminelle – *Une prise de conscience*

2. **QUI SONT LES CYBERCRIMINELS ?..... 27**
***Une typologie des cybercriminels** – *Les hackeurs et les autres – Des concours de* hacking *– Des crackers, nerds et script kiddies – Des professionnels et des amateurs – Du citoyen lambda au criminel – Des compétences au service d'employeurs – Des motivations diverses – Illégal ou moralement répréhensible ? – Des fabricants de programmes malveillants– Éthique le* hacking *?*
• Philosophie du hacking et défis de la cybersécurité
– Une question de perspective, d'intérêt et de finalité – Cyber-menaces omniprésentes, atteintes bien réelles – Des défis de société – Des compétences à acquérir – Des capacités à continuer de développer

3. INTERNET AU SERVICE DE LA CRIMINALITÉ…….... 45
***Technologies et opportunités criminelles** – *Contexte – Des conditions optimales pour les cybercriminels – Une couche d'isolation protectrice*
• Internet victime de son origine et de son succès – *Bref aperçu technologique – Des rustines de sécurité – Des vulnérabilités*
• Internet : une place de marché de la cybercriminalité – *Une économie de service – Une logique de marché – Des marchés noirs au service du crime – À qui profite le crime ? – Un paradoxe – Une cyber-proximité criminelle – Des valeurs inestimables*
• Difficultés de la lutte contre la cybercriminalité – *Rationalité et efficacité des acteurs criminels – Le chiffre noir de la cybercriminalité – Des ressources insuffisantes*

4 DÉPENDANCE, CONFLIT ET TERRORISME ……..... 69
*__Maîtrise des infrastructures, services et données__ – *Recherche et accès à l'information – Noms et adresses Internet – Infrastructure de routage et de transmission – Câbles sous-marins et informatique en nuage – Satellites de télécommunication et militarisation du cyberespace*
• **Guerre informatique et cyber-conflit** – *Attaques informatiques majeures – Actes de guerre – Attribution de l'origine d'une cyber-attaque – Capacités offensives et défensives – Cyber-actions visant à nuire à un État – Guerre sémantique et guerre du sens – Manipulation et intimidation – Guerre psychologique – Espionnage et perte de confiance – Une question de cyber-pouvoir et de souveraineté – Une question de perception de la guerre*
• **Rapprochement des mondes criminel et terroriste** – *Dimension terroriste de la cybercriminalité – Terrorisme informatique – Acte de cybercriminalité ou de terrorisme ? – Prudence et devoir de vigilance – Convergence d'intérêts – Cyber-attaques contre le terrorisme islamique*
• **Être vulnérable n'est pas une fatalité**

5. DIGNITÉ, IDENTITÉ ET DÉRIVES 101
*__Atteintes à la dignité et à l'intégrité des personnes –__ *Amitiés trompeuses et harcèlement – Faux sentiment de sécurité et prédateurs – La confiance est-elle possible ? – Inventer autrement le numérique et ses codes de bonne conduite – Existences numériques et plateformes de socialisation – Bruit numérique et appauvrissement*
• **Identité et identification** – *Contexte et besoins – La biométrie au secours de l'identité ? – Criminalité identitaire – Innovation technologique et responsabilité*
• **Transparence et surveillance** – *Au sujet de la transparence et du « cas Assange-Wikileaks » – Prisons électroniques – Une traçabilité permanente – Surveillance et prédiction – Libre arbitre et responsabilité*

6. PERSPECTIVES..... 123
*__Menaces persistantes__ – *Menaces intelligentes et intelligence des menaces – Cas WannaCry*
• **Transformation numérique** – *Saisir les opportunités, maîtriser les cyber-risques – Sécuriser et défendre son patrimoine numérique*
• **Pour une déclaration de Genève du cyberespace**
• **Éléments de conclusion**

BIBLIOGRAPHIE..... 137