académie Nantes

RÉGION ACADÉMIQUE
PAYS DE LA LOIRE

MINISTÈRE
DE L'ÉDUCATION NATIONALE
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

IHEDN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

Citoyenneté et Cybersécurité : enjeux de la sensibilisation et de la formation

TRINÔME ACADÉMIQUE

INTRODUCTION

Honoré d’être parmi vous.

Bio.

- Vincent LHOSTE
- Auditeur IHEDN Cyberdéfense
- Ingénieur et Formateur Cybersécurité

SOMMAIRE

1. Cyber-Défense et Citoyens : Enjeux et État des Lieux
   - Le/La citoyen/ne, un/e Cybercitoyen/ne ?
   - La stratégie institutionnelle de Cyberdéfense vis-à-vis des Citoyens.
   - La menace de la cybersécurité.

2. Comment construire une culture de Cyber-Défense pour l'ensemble des Citoyens ?
   - Prévenir le Risque
   - Renforcer la sécurisation des actes cyber du Citoyen.

3. Cybernétique, sociologie de l'information
   - Prospectives

INTRODUCTION

1. Selon le baromètre externe de la Défense, IFOP-DICoD 2017, seulement **12% de la population française considère les cyberattaques** comme une menace inquiétante, au même niveau que la menace nucléaire.

2. Alors que la **société est de plus en plus connectée**, la cyberdéfense devient une nécessité.

3. La menace est **protéiforme** et s'attaque aussi bien aux intérêts militaires, industriels que civils.

4. Le ministère des Armées la définit comme « l'ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère »[1].

INTRODUCTION

5. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit la cyberdéfense comme « l'ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels » élargissant de fait le sujet au domaine civil.

6. Les Livres blancs de la cyberdéfense ont affirmé, dès 2008, **l'importance** de prendre en compte cette cybermenace.

7. La cyberdéfense doit donc être pensée **comme globale** et recouvrir l'ensemble des forces vives du pays.

8. Alors que la cyberdéfense institutionnelle est en place, il reste encore à **créer une cyberdéfense citoyenne**. Il est donc nécessaire et indispensable de construire un lien entre ces deux dimensions.

INTRODUCTION

9. Pour ce faire, il convient de développer un ensemble de compétences et de comportements, partagés par l'ensemble des citoyens, qui conduirait à la mise en place d'une culture citoyenne indispensable au renforcement de la défense numérique globale de la Nation.

10. Face à une menace en évolution et au regard du lien entre les citoyens et la stratégie de défense, cette culture citoyenne de la cyberdéfense sera le fruit d'une politique d'information et de formation et de mise en œuvre de mesures de prévention et de protection.

11. Comment **construire cette culture citoyenne de la cyberdéfense**, nécessaire pour assurer la défense numérique globale de la Nation ?

Cyber-Défense et Citoyens : Enjeux et État des Lieux

1. Le/La citoyen/ne, un/e Cybercitoyen/ne ?
2. La stratégie institutionnelle de Cyberdéfense vis-à-vis des Citoyens.
3. La menace de la cybersécurité.

PEU D'EXPERTS, TOUS VOLONTAIRES

Elus départementaux

Informatique

Enseignement

Energie

Agroalimentaire

Banque

Culture

Administration préfectorale

Armée de Terre

Gendarmerie

Sécurité civile

Elus municipaux

+

Le/La citoyen/ne, un/e Cybercitoyen/ne ?

- Le citoyen d'aujourd'hui navigue dans le cyberespace, lieu de partage des cultures, de la diffusion des idées et des informations en temps réel.

- Le citoyen-utilisateur ?

- Dans cet esprit, le législateur a défini à travers le RGPD (Règlement général sur la protection des données personnelles, entré en application le 25 mai 2018) les nouveaux droits des citoyens.

Le/La citoyen/ne, un/e Cybercitoyen/ne ?

Mais qu'en est-il des devoirs afférents au cybercitoyen ?

- Aussi, pour favoriser l'adhésion des citoyens à la cyberdéfense, il convient d'évaluer leur sensibilité à « l'esprit de Défense ».

- Un début de réponse peut nous être apporté par l'étude réalisée en 2017 sur « la perception de la défense dans l'opinion publique européenne et chez les jeunes »[2].

- Il en ressort **trois éléments significatifs** :
  - La confiance dans les armées a évolué positivement entre 2010 et 2016 en Europe pour atteindre 84 % d'opinion favorable ;
  - 63 % des jeunes apprécient les « armées » et les « militaires » ;
  - A l'issue des Journées de défense citoyenne (JDC), 70 % des participants ont une image positive de l'armée.

Le/La citoyen/ne, un/e Cybercitoyen/ne ?

- Au final, si les notions de citoyen et de cybercitoyen, ne sont pas aisément compréhensibles ou appréhendables, de nombreux Français, **les jeunes** notamment, souhaitent que la République redonne du sens à l'action collective.

- Ils s'engagent ou sont prêts à s'engager pour y contribuer.

- Serait-ce le début du **citoyen cyber-responsable** ?

STRATEGIE DE CYBERDEFENSE ET CITOYEN

La place du citoyen : Être informé !

2025 : Loi de programmation militaire

2018 : Revue Stratégique de Cyberdéfense (livre blanc)

2015 : Stratégie nationale pour la sécurité du Numérique – SGDSN,

2011 : Défense et Sécurité des systèmes d'information -ANSSI

Stratégie de Défense et sécurité 2008, SGDSN

La stratégie institutionnelle de Cyberdéfense vis-à-vis des Citoyens

- La **cyberdéfense** est l'ensemble des actions entreprises dans le cyberespace et conduites de façon autonome ou en combinaison de moyens militaires conventionnels.

- Elle ne se limite pas à une posture défensive ;

- « Le gouvernement français a admis la nécessité de mesures actives voire offensives en octobre 2015 »[3].

La stratégie institutionnelle de Cyberdéfense vis-à-vis des Citoyens

- La Stratégie nationale pour la sécurité du numérique de 2015 précise de nouveaux objectifs - réaffirmés par la Revue stratégique de cyberdéfense de février 2018 - en priorisant la dimension économique :
  - garantir la souveraineté nationale,
  - apporter une réponse forte contre les actes de cybermalveillance,
  - informer le grand public,
  - faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises
  - et renforcer la voix de la France à l'international.

- Par ailleurs, l'Etat devient responsable de la cyberdéfense pour l'ensemble de la Nation.

La stratégie institutionnelle de Cyberdéfense vis-à-vis des Citoyens

- Un des objectifs prioritaires de la stratégie de cyberdéfense est de renforcer la **résilience des systèmes vitaux** de la France.

- **Quatre domaines** ont ainsi été définis :
  - les **intérêts fondamentaux de la Nation**,
  - la **sécurité intérieure et civile** ;
  - la **population et l'environnement**;
  - **l'économie**[4].

- **Cependant, la place du citoyen bien qu'évoquée dans les stratégies de cyberdéfense reste à développer.**

CITOYEN ET MENACE CYBER

- https://threatmap.checkpoint.com/

CITOYEN ET MENACE CYBER

- Il est aujourd'hui presque impossible au citoyen, quel que soit son âge ou sa motivation, de ne pas être connecté au cyberespace, qu'il en soit conscient ou non.

- Les chiffres varient selon les sources, mais il est certain que les actes malveillants dans le cyberespace (estimés à plus d'un milliard par an), visant aussi bien les individus , les entreprises que les organismes de l'Etat, sont légions.

- Même si « 91% des citoyens pensent que la sécurité et la protection des données sont très importantes » , l'hygiène cybernétique est loin d'être prise en compte par la grande majorité d'entre eux.

EXEMPLE WANNACRY

IMPACTS SUR LES ORGANISATIONS / INDIVIDUS

Cibles préférentielles des CYBERCOMBATTANTS :

- Tous les champs concernés : médias, services bancaires, défense, santé, etc…
- Et à une échelle bien plus importante qu'aujourd'hui.
- 2 Raisons au moins :
  - Le déploiement généralisé de la 5G renforcera les interdépendances et donc les vulnérabilités, en particulier sur les infrastructures critiques comme les OIV, les télécoms, les réseaux énergétiques, les BITD (Base industrielle et technologique de défense) et les hôpitaux.
  - Les avancées des systèmes d'IA « automatiseront » et accroîtront les manipulations de l'information et les risques de conflit ouvert, dans ce dernier cas via des systèmes d'armes autonomes échappant à la seule décision humaine.

IMPACTS SUR LES ORGANISATIONS / INDIVIDUS

- <u>Exemples de Cyberattaques :</u>
  - En 2015 /2016 Ukraine, attaque du réseau électrique ukrainien, et donc privation de chauffage durant l'hiver.
  - En 2017 France, par l'hameçonnage, les pirates sont rentrés dans les systèmes des équipes de campagne du mouvement « En marche »
  - NotPetya a atteint le réseau d'hôpitaux de Pennsylvannie causant près d'un milliard de dollars de perte et paralysant le système de santé; aussi les JO d'hiver de Corée du Sud en 2018.

COMMENT CHOISIR LES PRENOMS DE VOS ENFANTS ?

- Le site de l'INSEE sur la fréquence d'attribution des prénoms (https://www.insee.fr/fr/statistiques/3532172) est passionnant.

- Pour choisir le prénom de la chair de sa chair, les critères de choix ne manquent pas : la tradition, l'histoire familiale, la religion, la littérature, le cinéma ou la télévision – voire la bande dessinée, pourquoi pas. Mais pourquoi ne pas utiliser la sécurité des systèmes d'information pour choisir un prénom ? Oui, pourquoi pas ?

COMMENT CONSTRUIRE UNE CULTURE DE CYBER-DEFENSE ?

1. Prévenir le Risque

2. Renforcer la sécurisation des actes cyber du Citoyen

PRÉVENIR LE RISQUE

- « Le numérique, réseau des réseaux – incluant tous les objets et outils qui y sont liés – est immense, dynamique et omniprésent, impliqué dans tous les échanges, humains ou technologiques. Le numérique n'a pas de forme finie (…) La sécurité du numérique est transversale et mêle militaire et civil, professionnel et personnel[5]».

- <u>Mieux informer les citoyens</u>
  - L'ANSSI a rappelé que « la sécurité des systèmes d'information repose tant sur la vigilance personnelle que sur l'organisation, les choix et mesures techniques portés par les entreprises et l'action des Etats[6]».
  - De ces trois niveaux, le citoyen est sans aucun doute le maillon faible de la chaîne de cyberdéfense et, à ce titre, il doit faire l'objet d'une attention toute particulière et être l'objet d'actions de communication ciblées pour renforcer sa capacité de résistance.

PRÉVENIR LE RISQUE

- **Préconisation n°1 :** Mettre en place un plan de communication multimédia qui doit être pensé sur le long terme et doit viser l'ensemble des citoyens dans les différentes étapes de leur construction individuelle.

- En appui de ces campagnes de communication globales, pourquoi pas mettre en œuvre des actions de communications propres à chaque catégorie d'âge, afin d'être le plus efficient possible et toucher personnellement chaque citoyen :
  - Enfants (écoliers) : sensibilisation de type prévention routière, jeux éducatifs, exercices ludiques sur tablettes ou ordinateur ;
  - Adolescents/jeunes adultes (collégiens/lycéens/étudiants) : cours d'éducation civique sanctionné par un diplôme du bon utilisateur, rappel dans une charte du « code de bonne conduite » lors du recensement en mairie à 16 ans, module dispensé (vidéo, exercice d'application et de sensibilisation) lors des périodes de JDC ou du service national universel ;
  - Adultes : messages diffusés par les caisses de retraites, la caisse de sécurité sociale et les mutuelles, la Caisse d'allocations familiales, Pôle Emploi, les employeurs, …

PRÉVENIR LE RISQUE

- L’objectif est que chaque citoyen se pose la question **« Ce que je fais est-il sécurisé ? »**

- et que toutes ses connexions dans le cyberespace soient automatiquement précédées de réflexes permettant une navigation sécurisée.

PRÉVENIR LE RISQUE

- <u>Mieux former les citoyens</u>
  - **L'Education nationale**
    - La culture de la cyberdéfense s'acquiert par infusion dans un environnement qui multiplie les contacts. Les vecteurs doivent être multiples et divers. L'Education nationale est l'un de ces canaux, aussi bien au niveau de l'élève que du professeur.

    - Les programmes scolaires intègrent l'éducation aux médias depuis de nombreuses années :
      - années du primaire et du collège, sanctionnées par le Brevet informatique et internet (B2I) ;
      - l'éducation morale et civique (EMC) en Seconde, axe 2, « Garantir les libertés, étendre les libertés » et en Première : « Défiance vis-à-vis de l'information et de la science » et les « Nouvelles formes d'expression de la violence » ainsi que le programme PIX proposé au lycée, « Protection et sécurité », traitent partiellement de ce sujet.

PRÉVENIR LE RISQUE

- **Trois mesures pourraient être proposées pour remédier à ces manques :**

  - **Préconisation n°2** : Intégrer la cybersécurité de manière plus formelle dans les programmes scolaires.

  - **Préconisation n°3** : Sensibiliser les professeurs.

  - **Préconisation n°4** : Identifier un référent cybersécurité sur le modèle des enseignants référents pour l'action européenne et internationale (ERAEI).

PRÉVENIR LE RISQUE

- **La formation des magistrats**
  - La formation des magistrats paraît également une priorité au regard du nombre croissant d'affaires relevant de la cybercriminalité.
  - Cependant, les magistrats ne sont pas encore tous formés à cette problématique.
  - Malgré le pôle du parquet de Paris, on pourrait noter l'inexistence d'un tribunal spécialisé en cybercriminalité.
- **Préconisation n°5** : l'Ecole Nationale de la Magistrature pourrait être le lieu privilégié de formation en matière de cybersécurité des futurs magistrats, tant du siège que du parquet, et proposer également une formation continue pour les magistrats déjà en poste.

PRÉVENIR LE RISQUE

- **La formation en entreprises, administrations et associations : un cadre normé**
    - La formation aux risques cyber ne doit plus être l'exclusivité des experts mais doit être dispensée dans une politique ambitieuse à l'ensemble des citoyens.

- **Préconisation n°6 :** mettre en place un plan global de formation aux risques cyber, en définissant, sur le modèle des certifications et habilitations professionnelles, le dispositif pédagogique, les contours de la mise en œuvre et les sanctions prévues en cas de non application.

PRÉVENIR LE RISQUE

- **Accompagner au plus près**

  - Inscrire le Cybercitoyen au cœur d'une culture de la cyberdéfense implique un accompagnement.
  - La généralisation des « Maisons de services aux publics » afin de répondre aux attentes des citoyens, serait l'occasion d'intégrer un « référent numérique », interlocuteur privilégié des Cybercitoyens.
  - La réactivité étant primordiale dans le domaine de la cybersécurité, l'accessibilité en présentiel dans les locaux de la « Maison de services aux publics », ou un contact par téléphone via un numéro vert seraient les canaux à privilégier.

- **Préconisation n° 7** : mettre en place un correspondant à l'échelle de chaque commune pour venir en aide aux citoyens démunis face aux menaces du numérique.

RETEX : FORMATION INCLUSIVE PAR UNE PEDAGOGIE ACTIVE INVERSÉE

- La **CYBER POUR TOUTES ET TOUS !**
  - Le « maître ignorant » de Joseph Jacotot
  - Piloter une formation en pédagogie active
  - Montée intensive en compétences d'Apprenant(e)s en réinsertion professionnelle, en situation de différences et en mixité.

RETEX : FORMATION INCLUSIVE PAR UNE PEDAGOGIE ACTIVE INVERSÉE

Joseph
Jacotot

“le maître ignorant”

RETEX : FORMATION INCLUSIVE PAR UNE PEDAGOGIE ACTIVE INVERSÉE

Biographie

[1770-1840]

pédagogue français

créateur d'une méthode d'enseignement dite la **"Méthode Jacotot"**

plusieurs carrières : enseignement, droit, armée puis pédagogue

pédagogue engagé et frondeur :

RETEX : FORMATION INCLUSIVE PAR UNE PEDAGOGIE ACTIVE INVERSÉE

La méthode Jacotot

Pensée

→ s'interroge sur la place du maître et de la division entre savant et ignorant

Origine

→ lors d'un cours de français enseigné par Joseph Jacotot à des Hollandais
→ Joseph Jacotot ne comprend pas le hollandais
→ les étudiants ne comprennent pas le français
→ les étudiants ont été capables d'appréhender la langue française via une édition bilingue SANS l'explication du maître

Principe

→ Joseph Jacotot propose une nouvelle méthode d'enseignement qui s'oppose à la méthode traditionnelle

apprendre par soi-même
émanciper les intelligences
=/=
transfert du savoir par le maître

RETEX : FORMATION INCLUSIVE PAR UNE PEDAGOGIE ACTIVE INVERSÉE

Application

L'élève

→ retient par cœur dans la répétition
→ travail de mémorisation et d'attention : lire, observer, comparer, combiner, retenir
→ une fois que le travail est mémorisé, l'élève est capable d'en parler, de dire ce qu'il voit, ce qu'il pense et ce qu'il fait

Le maître

→ doit ignorer ce qu'il enseigne, car s'il connaît, il peut être tenté de l'expliquer et ainsi empêcher l'élève d'apprendre
→ soutient l'attention de l'élève
→ vérifie l'apprentissage de l'élève en posant des questions

Pour Joseph Jacotot

→ toutes les intelligences sont égales
→ qui veut, peut
→ on peut enseigner ce que l'on ignore
→ on ne retient que ce qu'on répète
→ chacun peut s'instruire tout seul
→ tout est dans tout

RETEX : FORMATION INCLUSIVE PAR UNE PEDAGOGIE ACTIVE INVERSÉE

Débat

ce qu'il en reste aujourd'hui

→ la méthode reste largement méconnue avec très peu de travaux historiques

opposition à cette méthode

→ usage intensif de l'apprentissage par cœur, élèves "perroquets"
→ les enfants ne sont pas capables d'un tel effort de mémorisation
→ les individus ne partageraient pas la même intelligence
→ l'élève ne peut pas s'instruire seul

Renforcer la sécurisation des actes cyber du citoyen

- **Alerter et s'exercer**
  - La sécurisation face au risque cyber ne saurait être complète sans la mise en œuvre de processus de remontées et de signalements d'alerte, de confrontation éthique, ainsi que d'exercices réguliers au risque cyber.

- **Développer les alertes et les signalements**

- **Préconisation n°8 :** Développer et médiatiser la plate-forme d'alerte cybermalveillance.gouv.fr ouverte aux citoyens, entreprises et administrations.

Renforcer la sécurisation des actes cyber du citoyen

- En cas de risque avéré et/ou de suspicion de risque, peut-être obliger les entreprises et les administrations à déclarer via cette plate-forme les attaques d'un niveau « minimum », le plan d'action mis en place et le retour à la normale (à voir avec les solutions existantes ANSSI),

- **Préconisation n°9 :** créer un Comité national d'éthique cyber (CNEC) composé des Ministères des Armées, de l'Éducation Nationale, de la Justice, de la CNIL, du Ministère de l'Economie et des Finances et de l'ANSSI.

Renforcer la sécurisation des actes cyber du citoyen

- <u>Mettre en place des exercices pour mieux anticiper une menace cyber</u>

- **Préconisation n°10** : mettre en place une Cyber-Olympiade, événement national annuel de 2 jours-24h/24 sur le modèle des CTF (Capture The Flag)

Renforcer la sécurisation des actes cyber du citoyen

- Avec pour objectifs de :
  - Déployer simultanément des CTF régionaux organisés par les pôles d'excellence cyber pour exploiter des vulnérabilités affectant des logiciels de manière à s'introduire sur des ordinateurs pour récupérer les drapeaux, preuves de l'intrusion ;
  - Impliquer dans chaque région les entreprises, les établissements scolaires et d'enseignements et de recherche, les administrations et la Défense (IHEDN, DMD…) ;
  - Organiser, en parallèle, des ateliers de sécurité numérique pour le grand public ;
  - …

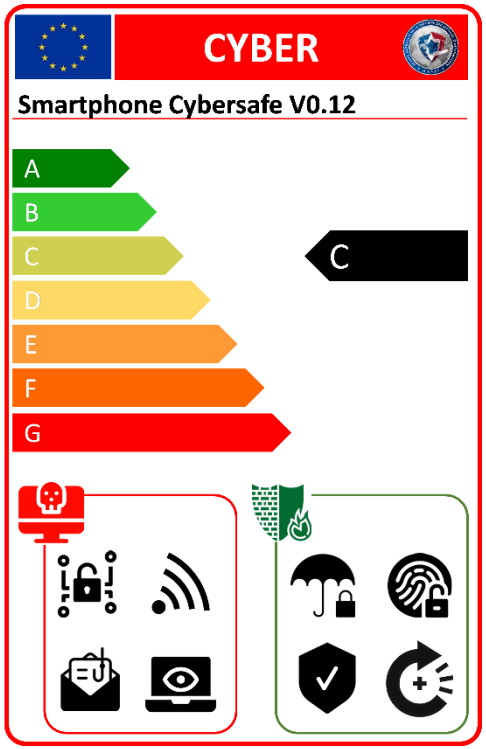
Renforcer la sécurisation des actes cyber du citoyen

- **Disposer d'une identité numérique**
    - Cela pose la question de la confiance dans la transformation numérique de notre société pour garantir la sécurité et éviter la fraude à l'usage. Pour cela, il conviendra de travailler en premier lieu sur des outils nationaux avant de pouvoir les transposer à l'international avec, par exemple, la mise en place d'un passeport e-citoyen.

- **Préconisation n° 11** : mettre en place une carte nationale d'identité (CNI) électronique intégrant une clef de chiffrement unique.
- **Préconisation n°12** : garantir au citoyen la fiabilité maximale de son identité numérique

Renforcer la sécurisation des actes cyber du citoyen

- **Sensibiliser et sécuriser par des repères intelligibles : le Cyber Score**



Un exemple : ce smartphone a une classification de niveau C.
Il a des vulnérabilités car il se connecte avec de nombreux autres matériels ou applications, via le réseau sans fil. Il est susceptible de permettre le vol de données, ou la surveillance malveillante.
Il est protégé par un pare-feu, un antivirus, une identification de type biométrique, et une mise à jour automatique de ses protections.

Loi du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public

Cybernétique, sociologie de l'information

1. Prospectives


YOU HAVE BEEN
HACKED !

CONCLUSION

Merci pour votre bienveillance et intérêt.

Remerciement à l'ancien DMD Adjoint de la Loire Atlantique Mr AGRECH, au Président de l'AR17 Mr Philippe JOSSO, et à l'Inspectrice académique pour la belle organisation et son accueil Mme DUPRE.

« La Cyber, c'est un mélange d'humilité, de résilience et de curiosité. »

Restant à votre entière disposition pour toutes questions.

TABLE DES ABREVIATIONS

- ANSSI : Agence nationale de la sécurité des systèmes d'information
- BITD : Base industrielle et technologique de défense
- CNIL : Commission nationale de l'informatique et des libertés
- COMCYBER : Commandement de la cyberdéfense
- JDC : Journée défense et citoyenneté
- LID : Lutte informatique défensive
- LIO : Lutte informatique offensive
- OIV : Opérateur d'Importance Vitale
- RGPD : Règlement général sur la protection des données personnelles

RÉFÉRENCES

1. Site du ministère des armées – www.defense.gouv.fr
2. Annuaire statistique de la Défense 2017
3. La Cyberdéfense, politique de l'Espace numérique – Ed Armand Colin – 2018.
4. Livre blanc Défense et Sécurité Nationale - Juin 2008.
5. Sécurité numérique et risques : enjeux et chances pour les entreprises, 2015
6. Défense et sécurité des systèmes d'information, Stratégie de la France, février 2011

EN SUPPLÉMENTS

ASPECTS JURIDIQUES

- En France :
  - La loi française condamne les attaques de type « phishing » à travers plusieurs textes du Code Pénal.
  - L'article 226-4-1 du Code pénal qui sanctionne l'usurpation d'identité avec une précision lorsqu'elle intervient dans un contexte numérique ainsi que son usage dans un but malveillant. (délit puni d'1 an d'emprisonnement et de 15 000€ d'amende)
  - L'article 226-18 précise qu'une telle collecte constitue un délit passible d'une peine d'emprisonnement de 5 ans et de 300 000 euros d'amende.
  - C'est l'escroquerie qui est visé par l'article 313-1 du même code celle-ci est passible de 5 ans d'emprisonnement et de 375 000 euros d'amende.
  - L'article suivant le 313-2 lui pose les 5 cas qui aggravent les faits d'escroquerie qui porte donc la peine à 7 ans d'emprisonnement età 750 000 euros d'amende. De plus, il précise que l'escroquerie en bande organisée est punie de 10 ans d'emprisonnement et 1 million d'euros d'amende.