ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

Département : Génie Informatique

Filière : Cybersécurité et Investigation Numérique

Classe : Niveau 4

Année académique : 2025/2026

DEVOIR D'INVESTIGATION NUMERIQUE : Chapitre 2

Nom de l'étudiant : MELONE André Vladmir

Matricule : 22P059

Table des matières

1 Partie 1 : Analyse Historique et Épistémologique **2**
1.1 Analyse Comparative des Régimes de Vérité 2
1.2 Étude de Cas Archéologique Foucaldienne : cas de l'affaire du 414s 2
1.3 Vérification de l'Accélération Technologique 2
1.4 Analyse du Trilemme CRO Historique 3

2 Partie 3 : Investigation Historique Appliquée **4**
2.1 Reconstruction Archéologique d'Investigation 4
2.2 Analyse Prospective des Régimes Futurs 5

1 Partie 1 : Analyse Historique et Épistémologique

1.1 Analyse Comparative des Régimes de Vérité

Prenons 2000-2010 et 2010-2020

Calculons leurs vecteurs de dominance $\vec{R} = (\alpha_T, \alpha_J, \alpha_S, \alpha_P)$

Cas de 2000-2010 : $\vec{R} = (0.1, 0.1, 0.4, 0.4)$

Cas de 2010-2020 : $\vec{R} = (0.1, 0.2, 0.4, 0.3)$

On constate que le besoin de reguler les usages numeriques est devenu crucial. Cela s'explique par le fait que les personnes faisaient un usage non controle des des outils numeriques ce qui entrainait une montee du taux de cybercriminalité.

1.2 Étude de Cas Archéologique Foucaldienne : cas de l'affaire du 414s

Avant l'affaire du 414s, le terme ***hacker*** évoquait avant tout la curiosité technique et la passion pour l'informatique, sans aucune connotation criminelle. Les hackers étaient perçus comme des explorateurs de systèmes, des individus fascinés par la logique des machines et la résolution de problèmes complexes, et l'idée même de cybercriminalité restait largement abstraite. L'affaire du 414s a profondément changé cette perception en montrant que les intrusions dans les systèmes informatiques pouvaient avoir des conséquences réelles et dommageables, et que les traces laissées sur un réseau journaux de connexion, adresses IP, modifications de fichiers, et autres métadonnées pouvaient constituer des preuves légitimes et juridiquement recevables pour établir la culpabilité d'un tiers. Cet événement a ainsi participé à la construction du cadre légal et méthodologique entourant les enquêtes informatiques. Aujourd'hui, le terme ***hacker*** est bien défini et compris tant dans le langage courant que dans le contexte légal et technique, et il est devenu normal et logique d'utiliser les logs, traces numériques et analyses forensic comme instruments centraux dans la conduite d'investigations de cybercrime. L'affaire du 414s illustre donc le passage d'un univers où le hacking était une curiosité technique à un régime de vérité moderne, où la preuve numérique occupe une place centrale dans la définition et la reconnaissance de la culpabilité.

En 1988, le Morris Worm, créé par Robert Tappan Morris, a infecté massivement le réseau ARPANET, perturbant des centaines d'ordinateurs, notamment ceux du MIT, de l'Université de Cornell et de l'Université de Californie à Berkeley. Cet incident a révélé l'importance des traces numériques pour l'investigation et a constitué un précédent juridique. Il s'agit la du premier proces federal pour un acte informatique aux Etats Unis. Morris Worm est reconnu coupable en vertu du computer Fraud and abuse Act qui a vu le jour grace a l'affaire du 414s.

1.3 Vérification de l'Accélération Technologique

- Les dates precises des changements de regimes : 1990, 2000, 2010, 2020
- Verifions que $\Delta t_{n+1} = k \cdot \Delta t_n$: On a :

$$\frac{2000 - 1990}{2010 - 2000} = 1 \implies k = 1$$

  cqfd

- Calcul du prochain intervalle :

  On utilise la loi empirique :

$$\Delta t_{n+1} = k \cdot \Delta t_n$$

  Ici, pour les intervalles précédents $\Delta t_1 = \Delta t_2 = \Delta t_3 = 10$ et $k = 1$:

$$\Delta t_4 = k \cdot \Delta t_3 = 1 \cdot 10 = 10$$

Le prochain changement de régime est donc prévu pour :

$$t_5 = t_4 + \Delta t_4 = 2020 + 10 = 2030$$

— Conclusion :
  — Les intervalles sont constants : $k = 1 \Rightarrow$ pas d'accélération.
  — Le prochain changement de régime est prévu en $t_5 = 2030$.
  — La significativité statistique ne peut pas être testée avec seulement 3 intervalles, mais la loi est parfaitement constante dans cet exemple.

1.4 Analyse du Trilemme CRO Historique

TABLE 1 – Scores pour chaque régime de vérité

Régime de vérité	**Score C**	**Score R**	**Score O**
1970-1990	15	15	70
1990-2000	20	20	60
2000-2010	35	25	40
2010-2020	60	25	15

Le script python suivant nous a permi de tracer ce schema en 3D :

Listing 1 – Visualisation 3D des scores

```
import numpy as np
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D

annees = [1980, 1995, 2005, 2015]
regimes = ["1970-1990", "1990-2000", "2000-2010", "2010-2020"]

score_C = [0.15, 0.2, 0.35, 0.6]
score_R = [0.15, 0.2, 0.35, 0.6]
score_O = [0.7, 0.6, 0.4, 0.15]

fig = plt.figure(figsize=(12,7))
ax = fig.add_subplot(111, projection='3d')

colors = ['tab:blue', 'tab:green', 'tab:red']

ax.plot(annees, score_C, zs=0, zdir='y', label='Score C', color=colors[0], marker
ax.plot(annees, score_R, zs=1, zdir='y', label='Score R', color=colors[1], marker
ax.plot(annees, score_O, zs=2, zdir='y', label='Score O', color=colors[2], marker

ax.scatter(annees, score_C, zs=0, zdir='y', color=colors[0], s=60)
ax.scatter(annees, score_R, zs=1, zdir='y', color=colors[1], s=60)
ax.scatter(annees, score_O, zs=2, zdir='y', color=colors[2], s=60)

ax.set_xlabel('Ann es', fontsize=12)
ax.set_ylabel('Scores', fontsize=12)
ax.set_zlabel('Valeur', fontsize=12)
ax.set_yticks([0,1,2])
```

```
ax.set_yticklabels(['C', 'R', 'O'], fontsize=12)
ax.set_title("  volution   des scores C, R, O au fil des ann es", fontsize=14)
ax.grid(True)
ax.legend()

plt.show()
```

On a le resultat suivant :

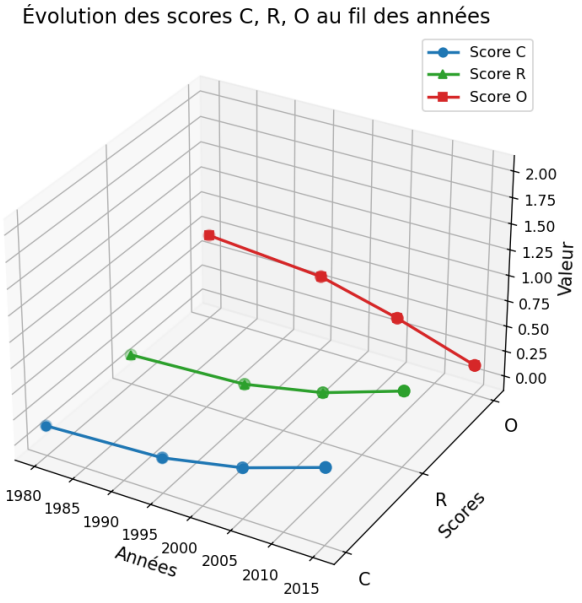

FIGURE 1 – Evolution des valeurs de C, R, O au fil du temps

Au fil des périodes étudiées, l'évolution des scores révèle une transformation progressive du régime de vérité. Dans la période 1970-1990, l'opposabilité (O) domine largement, tandis que la confidentialité (C) et la fiabilité (R) sont marginales. Au cours des décennies suivantes, la confidentialité et la fiabilité connaissent une augmentation constante, particulièrement marquée entre 2000-2010 et 2010-2020, suggérant un renforcement rapide de leur influence. Parallèlement, l'opposabilité décline de manière inverse, passant de la position dominante à une part marginale en 2010-2020. Cette dynamique indique un transfert de poids au sein du régime de vérité, avec un remplacement progressif des priorités initiales par celles représentées par la confidentialité et la fiabilité. Ainsi, le régime de vérité se réorganise, devenant de plus en plus centré sur la confidentialité et la fiabilité, reflétant probablement des changements technologiques, institutionnels ou conceptuels qui redéfinissent les composantes centrales de ce régime.

2 Partie 3 : Investigation Historique Appliquée

2.1 Reconstruction Archéologique d'Investigation

L'affaire Kevin Mitnick dans les années 1990 illustre parfaitement l'évolution des pratiques d'investigation et des régimes de vérité. À l'époque, l'enquête reposait sur des outils rudimentaires : suivi des communications téléphoniques, analyse manuelle des journaux de connexion, interrogatoires et collaboration avec les fournisseurs de services informatiques pour reconstituer les intrusions. Les limitations technologiques, comme l'absence de systèmes de journalisation centralisés et de logiciels de détection automatisée, rendaient la vérification des faits laborieuse et fragmentaire, influençant fortement la construction de la vérité. Si l'on refaisait l'analyse aujourd'hui avec des outils modernes systèmes SI centralisés, analyse des logs automatisée, forensic

numérique, traçage IP et corrélation des événements en temps réel les résultats seraient beaucoup plus précis et rapides. Cette comparaison montre que le régime de vérité de l'époque était marqué par la confiance dans les témoignages et les preuves partielles, tandis qu'aujourd'hui il serait dominé par les preuves numériques vérifiables et les corrélations automatiques. Ainsi, l'évolution technologique transforme non seulement la précision des enquêtes mais également la manière dont la vérité est construite et validée, soulignant l'impact déterminant des contraintes techniques sur l'investigation et la fiabilité des conclusions.

2.2 Analyse Prospective des Régimes Futurs

Entre 2030 et 2050, on peut imaginer un régime de vérité profondément façonné par l'intelligence artificielle avancée et les systèmes distribués de collecte de données, où la vérité est construite par des algorithmes d'analyse en temps réel combinant données massives, simulations prédictives et preuves numériques automatisées. Les conditions de possibilité de ce régime incluent la disponibilité de bases de données globales interconnectées, la transparence algorithmique partielle, et une infrastructure sécurisée garantissant l'intégrité des traces numériques. Dans ce contexte, la méthodologie d'investigation devra combiner forensic numérique automatisé, analyses prédictives, audit des algorithmes et validation croisée par intelligence artificielle et expert humain, afin de reconstruire les événements de manière exhaustive. Cependant, ce scénario soulève des défis éthiques et épistémologiques majeurs : risque de biais algorithmique, dépendance excessive aux systèmes automatisés, difficulté à interpréter les décisions complexes des IA et enjeux de responsabilité juridique. Le régime de vérité futur serait donc caractérisé par une tension constante entre fiabilité algorithmique, transparence humaine et protection des données, redéfinissant les critères de preuve et la manière dont la vérité est validée dans les enquêtes et la société.