RÉPUBLIQUE DU CAMEROUN
*****
Paix - Travail - Patrie
*****

UNIVERSITÉ DE YAOUNDÉ I
*****

ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
*****

DÉPARTEMENT DE GÉNIE
*****

REPUBLIC OF CAMEROON
*****
Peace - Work - Fatherland
*****

UNIVERSITY OF YAOUNDE I
*****

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
*****

COMPUTER ENGINEERING
*****

Techniques et pratiques de l'investigation numérique

Sous le thème : Résumé Techniques et pratiques de l'investigation numérique

EMBOLO MVOGO SHAWN DOUGLAS

Matricule : 22P072

Filière : CIN4

Sous la supervision de : **Mr Minka**

Année Scolaire : **2025 – 2026**

1 Partie 1 : Analyse Historique et Épistémologique

1.1 Analyse Comparative des Régimes de Vérité

Périodes choisies : Les Prémices (1970-1990) vs L'Ère de l'IA et du Quantique (2020-Présent.
Notre périodisation repose sur quatre axes d'analyse dont la dominance relative dé nit chaque régime :
T : Transformations Technologiques
J : Évolutions Juridiques et Normatives
S : Mutations Sociales et Culturelles
P : Pratiques Professionnelles et Méthodologiques

Vecteurs de dominance

1.2 Les Prémices (1970-1990) : L'Émergence de la Trace Électronique

Ici, le paysage est dominé par la :

- Technique (T ≈ 0.7)
- Juridique (J ≈ 0.1)
- Social (S ≈ 0.1)
- Pratique (P ≈ 0.1)

Vecteur $\mathbf{R_{(1970-90)}} \approx (0.7, 0.1, 0.1, 0.1)$

1.3 L'Ère Post-Quantique et IA (2020-Présent) : Le Grand Saut

- Technique (T ≈ 0.4)
- Juridique (J ≈ 0.3)
- Social (S ≈ 0.1)
- Pratique (P ≈ 0.1)

Vecteur $\mathbf{R_{(2020-)}} \approx (0.4, 0.3, 0.1, 0.2)$

1.4 Discontinuités épistémologiques

De la preuve-objet à la preuve-système : Dans les prémices, la preuve était un **artefact tangible** : un fichier log, une disquette. Aujourd'hui, la preuve est un **phénomène émergent** d'un système complexe. Personne ne « tient » la preuve; elle est distribuée dans des milliards de lignes de logs, des comportements réseau anormaux, et les prédictions d'un modèle d'IA. La preuve n'est plus une chose, c'est une **relation**.

La mort de l'expert omniscient et la naissance du prêtre de la boîte noire : L'autorité, dans les prémices, était l'**expert technique**. C'était un sorcier qui comprenait les incantations (le code) et pouvait raconter l'histoire du crime. Aujourd'hui, l'autorité est souvent l'**algorithme d'IA**. L'expert moderne n'est plus celui qui sait, mais celui qui sait **interroger l'oracle**. Il est le gardien du temple, celui qui peut interpréter les signes (les sorties du modèle) pour le commun des mortels (les juges). C'est un changement de statut métaphysique de la vérité : elle n'est plus démontrée, elle est **révélée** par une intelligence non-humaine.

L'échelle qui a tué le contexte : Dans les années 80, on analysait un piratage comme un roman policier : on suivait une piste, on comprenait les motivations, les moyens. Aujourd'hui, face à des attaques comme SolarWinds, l'échelle est telle que la compréhension narrative est impossible. On ne comprend plus *pourquoi*, on constate *comment*. La vérité devient statistique, probabiliste, déshumanisée.

1.5 La tempête sociotechnique

- **La poussée technologique (T)** a été la plus violente : le cloud a dissous les frontières physiques, et l'IA a introduit une couche d'intelligence non-humaine, créant ce « régime de vérité algorithmique » où la preuve peut être à la fois probante et incompréhensible.
- **La réaction juridique (J)** a été un rattrapage frénétique. Les affaires Snowden ou les attaques transnationales ont forcé le droit à sortir de son cadre national et à se confronter à l'ubiquité de la data. Le RGPD est un exemple de cette tentative désespérée de reprendre le contrôle.

1.6 Question critique : Révolution ou évolution ?

C'est une **révolution qui a pris l'apparence d'une évolution**.

La transition a semblé progressive, mois après mois, outil après outil. Mais si l'on compare les deux extrémités du spectre, le saut est abyssal. On est passé d'un monde où la vérité numérique était une **affaire humaine, locale et artisanale** à un monde où elle est une **affaire post-humaine, globale et industrielle**. Le point de rupture, le « Big Bang », se situe probablement au tournant des années 2010, lorsque le volume de données a dépassé le seuil au-delà duquel l'intelligence humaine seule est devenue inadéquate. C'est une révolution silencieuse, qui s'est jouée non pas dans la rue, mais dans les data centers.

Exercice 2 : Étude de Cas Archéologique Foucaldienne

1.7 Affaire choisie : L'Opération Sundevil (1990)

Plongeons-nous dans le monde mental de 1990. L'Internet public n'existe pas encore. Le « cyberespace » est une terre de légendes, peuplée de hackers et de pirates.

1.7.1 1. Le corpus : Ce qui constituait la « réalité » de l'époque

- **Sources primaires :** Les communiqués du Service Secret américain, les articles de journaux au ton souvent sensationnaliste (« La grande chasse aux hackers ! »), les témoignages dans des magazines comme *Phrack*.
- **L'imaginaire collectif :** Des films comme *War Games* ont préparé le terrain culturel. Le hacker est perçu comme un génie adolescent ou un dangereux anarchiste.

1.7.2 2. Ce qui était « pensable » et « dicible » en 1990 : La formation discursive

Énoncés possibles (le « dicible ») :

- « Les hackers sont une menace pour la sécurité nationale. »
- « Il faut des lois spécifiques pour criminaliser ces intrusions. »
- « La preuve réside dans les systèmes saisis (les ordinateurs, les disquettes). »
- « Nous menons une opération de police traditionnelle, mais avec de nouveaux outils. »

Énoncés impensables (l'« impensable ») :

- « Le piratage est un service de renseignement économique pratiqué par les États. » (C'était impensable comme accusation officielle).
- « La vraie menace viendra un jour de la chaîne d'approvisionnement logicielle. » (La notion de « supply chain attack » n'existait pas).
- « La preuve la plus cruciale est volatile et réside dans la mémoire vive. » (L'importance de la forensique sur la mémoire live n'était pas établie).
- « Ces opérations pourraient un jour nécessiter une collaboration internationale de journalistes. » (Le modèle des Panama Papers était inimaginable).

1.7.3 3. Le régime de vérité en action : Une opération de police qui s'invente

- **Preuve paradigmatique :** La **saisie physique**. La vérité est littéralement **matérialisée** dans les 42 ordinateurs saisis. C'est une vision très « policier de quartier » étendue au numérique : on entre par la porte et on saisit les preuves.
- **Autorité épistémique :** L'**État**, incarné par le Service Secret. C'est lui qui dit le vrai. L'expert technique est au service de cette autorité, il ne la constitue pas encore pleinement.
- **Condition d'acceptabilité sociale :** L'opération est un **rituel**. Son but est autant de punir que de **montrer la force de l'État** face à une nouvelle forme de délinquance incomprise. Elle doit être spectaculaire pour être crédible. C'est un « fait social total » qui permet à la société de se rassurer en catégorisant et en réprimant une menace floue.

1.7.4 4. Comparaison avec une affaire contemporaine : L'Attaque SolarWinds (2020)

- **Sundevil (1990) :** Le régime de vérité est **juridico-policier**. La vérité se construit par la **raideur** (des perquisitions, des saisies) et vise à produire un **coupable** pour un tribunal.
- **SolarWinds (2020) :** Le régime de vérité est **technico-stratégique**. La vérité se construit par l'**analyse comportementale IA** et vise d'abord à **comprendre une campagne d'action** pour s'en défendre. L'attribution est complexe, floue, souvent politique. La « preuve » n'est plus pour le tribunal, mais pour le conseil de sécurité nationale. On est passé de la police à la **guerre algorithmique**. La vérité n'est plus une fin, c'est une arme.

2 Partie 3 : Investigation Historique Appliquée

Exercice 6 : Reconstruction Archéologique d'Investigation

2.0.1 Affaire choisie : Le Virus Michelangelo (1992)

En 1992, la nouvelle fait le tour du monde : un virus informatique, le « Michelangelo », est programmé pour se déclencher le 6 mars (anniversaire de l'artiste) et effacer les disques durs. C'est une panique médiatique mondiale.

1. L'enquête à l'ancienne : Dans la peau d'un expert en 1992

- **L'état d'esprit :** C'est la **Grande Peur** du numérique. Le public découvre que ces machines peuvent être « malades ». L'expert est un **médecin légiste** face à une nouvelle peste.
- **La boîte à outils :**
  - Un **éditeur hexadécimal** pour disséquer le corps du virus, instruction par instruction.
  - Des **antivirus de première génération** qui fonctionnent par signatures simples.
  - Des **disquettes de boot « propres »** pour ne pas contaminer la machine d'analyse.
  - Beaucoup de **café et de patience**. L'analyse est lente, fastidieuse. On « sent » le code.
- **La méthode :** C'est de la **microchirurgie statique**. On isole le virus sur une machine quarantaine. On le désassemble. On cherche ses signatures, son point d'activation. On comprend son mode de propagation (les disquettes !). L'enquête est rétrospective, après la découverte de la menace.

2. L'enquête revisitée avec un regard moderne (2024)

- **L'état d'esprit :** Le Michelangelo serait aujourd'hui un **nuisanceware** parmi des millions. L'approche n'est plus curative mais **préventive et systémique**.
- **La boîte à outils :**
  - Des **sandbox dynamiques** qui exécutent le virus dans un environnement virtuel et cartographient tous ses comportements en quelques minutes.
  - Des **plateformes EDR (Endpoint Detection and Response)** qui auraient détecté le comportement d'écriture du boot sector en temps réel sur tous les postes de l'entreprise.
  - L'**analyse heuristique et comportementale** qui aurait identifié le code comme malveillant même sans signature spécifique.
  - Des **systèmes de threat intelligence** qui auraient partagé les indicateurs de compromission (IOCs) à l'échelle mondiale en quelques secondes.
- **La méthode :** C'est une **réponse automatisée et en temps réel**. Le virus serait contenu avant même d'avoir pu se propager largement. L'enquête ne porterait plus sur « qu'est-ce que c'est ? » mais sur « d'où vient-il et qui est derrière ? » via l'OSINT et la corrélation avec d'autres campagnes.

3. Le choc des régimes de vérité : De la peur à l'indifférence

- **En 1992 (Régime Artisanal) :** La vérité sur le Michelangelo était **anxiogène et narrative**. Elle était construite par quelques experts dans des labos, relayée par une presse sensationnaliste. La vérité était : « Ce virus est dangereux, voici sa date d'activation, voici comment s'en protéger. » Elle avait un **impact émotionnel fort** sur la société.
- **Aujourd'hui (Régime Industriel) :** La vérité sur une menace équivalente serait **froide et statistique**. Elle serait produite automatiquement par des machines. La vérité serait : « Un malware de la famille X avec un score de sévérité de 4/10 a été détecté et contenu sur 0.001% des endpoints. Les IOCs ont été partagés. » C'est une **vérité opérationnelle**, dénuée de récit, conçue pour être consommée par d'autres machines (les systèmes de sécurité). La panique de 1992 est devenue une ligne dans un dashboard.

4. Le prix de la modernité : La perte de l'intimité avec la menace L'expert de 1992 connaissait le Michelangelo intimement. Il l'avait disséqué, compris. Sa vérité était profonde, mais lente et non-scalable. L'expert de 2024 ne « connaît » plus les virus individuellement. Il connaît les **systèmes qui les gèrent**. Sa vérité est large, rapide, mais superficielle. Il a gagné en efficacité ce qu'il a perdu en familiarité. La vérité numérique est devenue un produit industriel, et comme tout produit industriel, elle est standardisée, efficace, mais a perdu l'âme de l'artisanat.

Conclusion : Cette plongée dans l'archéologie de nos vérités numériques montre que chaque outil que nous forgeons pour voir plus loin modifie aussi notre propre vision. Nous ne cherchons plus les mêmes choses, et ce que nous trouvons, nous ne le voyons plus de la même manière.