Séminaire 1

Cyberresilience et sécurité quantique des données et des communications : enjeux et défis

Date : 21 novembre 2024
Horaire : 16h00 GMT - 17h30 GMT
Format : En ligne (Zoom)
Intervenant : Professeur Djiby Sow
Modérateur : Serigne Moustapha Bassirou KA, mastérant sciences de l'ingénieur option informatique (ESP)

1. Objectifs de la séance

Ce séminaire avait pour objectif d'explorer les enjeux actuels de la cybersécurité en Afrique, avec un focus particulier sur la cyberrésilience et la sécurité quantique, qui constituent des défis clés pour les infrastructures de données et de communications modernes. Les principales interrogations portaient sur :

- les défis techniques à surmonter pour implémenter efficacement la cryptographie post-quantique dans les systèmes existants ;
- le schéma de signature post-quantique EagleSign ;
- le rôle de l'IA dans la cybersécurité ;
- les technologies émergentes et la cyberrésilience.

2. Contenu et activités

La séance a débuté par une introduction de 10 minutes par le modérateur, Serigne Moustapha Bassirou Ka, qui a présenté le contexte de la discussion, l'intervenant et l'importance du sujet.

Le Professeur Djiby Sow a ensuite pris la parole pour une intervention d'environ 45 minutes, structurée autour des thématiques suivantes :

- **Les technologies émergentes :**
    - Cyberdéfense, Cryptographie post quantique, Intelligence Arti_cielle, Blockchain, Cloud, Quantum computing, IoT, Edge computing.

- **Cyberresilience enjeux et défis :**
    - Quelques chiffres et motivation pour la cyberresilience.
    - Confiance et sérénité dans le cyberespace
    - Les enjeux du citoyen sont à confondre avec les problèmes fondamentaux qui le préoccupe
    - La majorité du patrimoine de l'entreprise.
    - Développer des capacités de résilience pour faire face aux attaques les plus dévastatrices
    - Verrouiller les premiers vecteurs d'attaques afin de protéger les technologies et acteurs du cyberespace
    - Remédier au faible engagement des pays africains
    - Lutter contre la perception qui amoindrit la dangerosité des attaques cybercriminelles
    - Combattre la fréquente rétention d'informations sur les attaques pour des raisons d'image commerciale ou de marque ce qui rend difficile le travail des CERTs
    - Protéger les infrastructures et les systèmes vitaux
    - Se doter de moyens pour la cyberguerre
    - Avoir une maitrise minimale sur la technologie assurer la cyberrésilience IoT (IoT domestique, IoT médical, IoT humain, IoT industriel)
    - Gérer la montée en puissance des hackeurs
    - Définir et appliquer des politiques adaptées

3. Méthodologie

Le séminaire s'est déroulé en ligne sur Zoom et a été structuré en deux parties :

- Une présentation de 45 minutes par le Professeur Djiby Sow ;
- Une session interactive de 30 minutes consacrée aux questions-réponses. Les participants ont eu la possibilité de poser leurs questions oralement ou via le chat.

4. Résultats et apprentissages

Les échanges ont permis de mettre en lumière plusieurs points clés :

- **Souveraineté technologique et pourquoi c'est important d'y arriver :**

  Les africains ne doivent être d'éternels consommateurs, il faudra développer un écosystème qui permettras de produire localement un certain nombre d'infrastructures numériques mais aussi essayer d'avoir une main mise sur les technologies émergentes.

- **Protection contre les ordinateurs quantiques :** un système conçu avec l'un des huit (8) familles de réseaux arithmétiques (chiffrement symétrique, les fonctions de hachages, code correcteur d'erreur, polynômes multivariés …) actuellement constitue le meilleur moyen de se protéger contre ces machines quantiques.
- **Super calculateur sénégalais dénommée TAOUEY** : Pour la gestion des capacités nationales de calcul scientifique et les apports de cette machine pour le développement de la recherche scientifique
- **Normes et règlementations pour la cyberresilience des IOT :**
  - ✔ En 2018 ; la Chine publie le "China's Internet of Things Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission
  - ✔ En 2022, le NIST des USA a produit " Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products",
  - ✔ En 2022 Le Royaume Uni a adopté la loi "The Product Security and Telecommunications Infrastructure (PSTI) Act" pour gérer la cyberrésilience IoT

✔ En 2022, l'Union Européenne publie le Cyber Resilient Act et l'adopte définitivement en 2024

- **Le Dark Web :** la manière de l'utiliser via un navigateur dénommé TOR conçu pour anonymiser la navigation sur internet.

5. Feedback des participants

Le séminaire a rassemblé une trentaine de participants, issus de divers horizons. Ces derniers ont salué la profondeur de l'analyse du Professeur Sow et l'actualité du sujet abordé. Les interventions ont permis d'éclairer plusieurs points et d'ouvrir des perspectives de recherche.

Des recommandations aux Etats africains :

- Posséder des textes législatifs et réglementaires ;
- Créer plusieurs formations académiques.
- Créer un CERT (computer emergency response team) / CSIRT national, des SOCs (Security Operation Center) et des CERTs locaux
- Créer un centre de recherche sur la cyberrésilience et les technologies émergentes connexes

6. Conclusion

Cette séance a permis de comprendre que la cyberresilience et la sécurité quantique sont des enjeux essentiels pour protéger les données et les communications face aux avancées de l'informatique quantique. En outre cette dernière bien qu'innovante pourrait constituer une réelle menace pour les systèmes de sécurité traditionnels. Le Professeur Djiby Sow a été chaleureusement remercié pour ce moment d'enrichissement intellectuel et nous a profondément impressionné par la qualité et la profondeur de ses analyses ce qui démontre encore une fois son niveau d'expertise dans le domaine.