ParIdigi MasterClass

Grand Conseil de la République et Canton de Genève

Cybersécurité

Genève, 26 janvier 2024

Dr. Eduardo Solana, Chargé de cours, Département d'Informatique, Université de Genève

Pauline Meyer, Doctorante en cybersécurité, Université de Lausanne

---

Un événement organisé par:

Universität Zürich[UZH]
Digital Society Initiative

ParIdigi

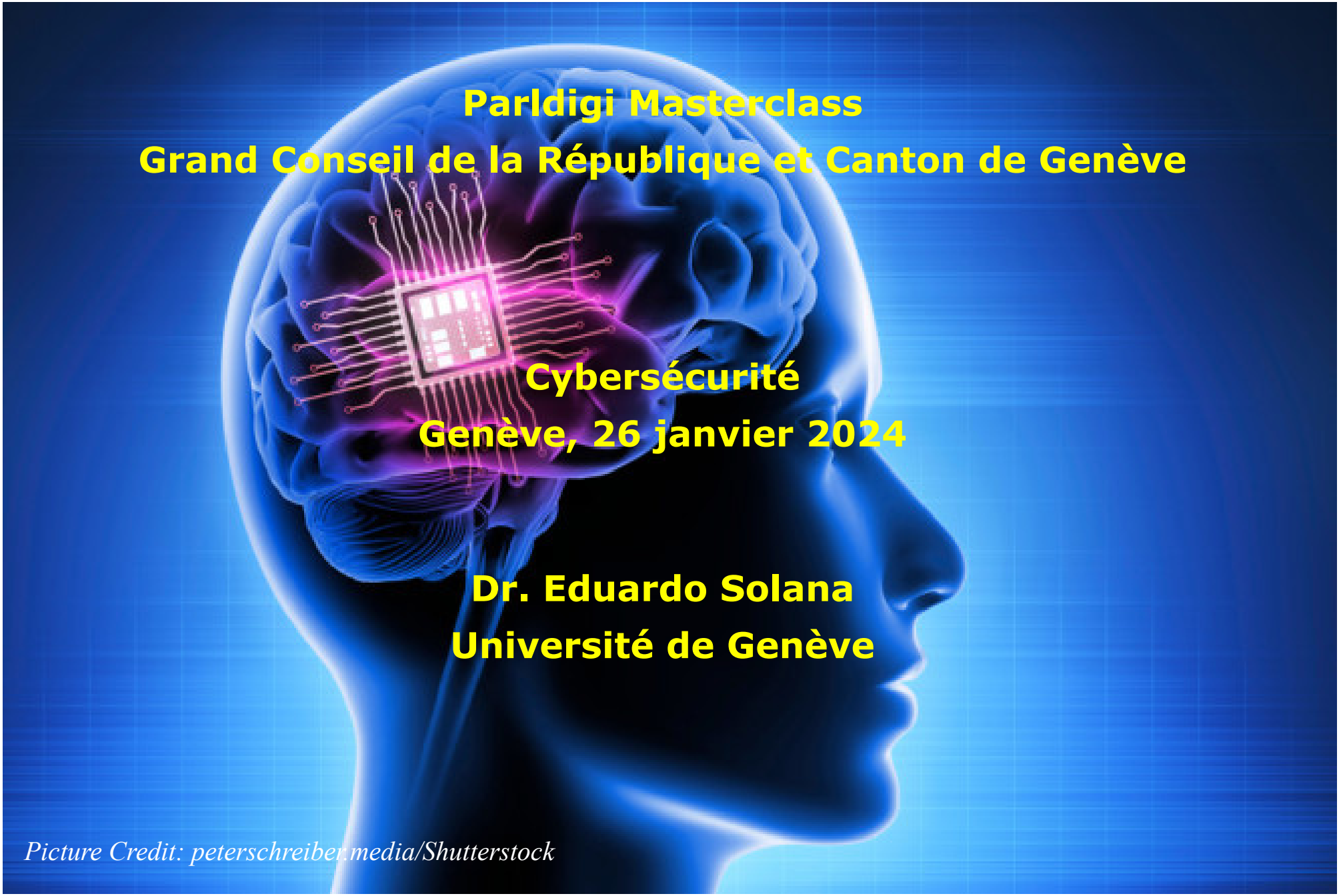
UNIVERSITÉ DE GENÈVE
CENTRE UNIVERSITAIRE D'INFORMATIQUE

Partenaire:

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

Soutenu par:

Stiftung Mercator Schweiz



ParIdigi Masterclass
Grand Conseil de la République et Canton de Genève

Cybersécurité
Genève, 26 janvier 2024

Dr. Eduardo Solana
Université de Genève

Picture Credit: peterschreiber.media/Shutterstock

La Cybersécurité en Chiffres

- Les attaques de type **ransomware ont augmenté de 74% en 2023** et celles sur les **chaines d'approvisionnement** (*supply-chain*) **de 633%**. Les attaques basées sur **l'ingénierie sociale** sont **en hausse de 135%** boostées par ***IA générative***[1]
- "*Sur les quatre dernières années, le monde de la cybersécurité a dépensé 716 milliards de dollars dans le monde, tandis que le coût des cyber-attaques a été de 8 billions.* ***Un rapport de 11 contre 1 en faveur des pirates***"[1]
- **60% des entreprises interrogées** ont déclaré avoir été confrontées à un incident de cybersécurité au cours des 12 derniers mois alors que **seulement 15% des organisations se considèrent suffisamment préparées** aux risques *cyber*[2]
- **2200 cyber-attaques par jour** ou **une toutes les 39 secondes**. ***Première attaque reçue en moyenne 1-2 minutes*** après avoir connecté un système à Internet pour la première fois

1. La Tribune.*https://www.latribune.fr/technos-medias/informatique/cybersecurite-pourquoi-les-menaces-sont-plus-elevees-que-jamais-983903.html*. Consultée le 24 janvier 2024
2. *Cisco Cybersecurity Readiness Index*. *March 2023*

Attaques et Attaquants

- **Professionalisation** des attaques:
  - En 1999 **un adolescent** a pénétré dans les réseaux du Département de la Défense (*DoD*) américain et dans la *NASA* et provoqué des indisponibilités dans ces réseaux pendant 3 semaines
  - En 2021 une attaque de type ***ransomware*** visant la société *Colonial Pipeline* a paralysé la distribution de combustible dans la côte est des Etats Unis avant qu'une **rançon de 4.4 millions de dollars** soit payée. Les enquêtes pointent vers le groupe russe ***Darkside***
  - En octobre 2023 une attaque ***DDOS*** contrée par *Google* a réussi à générer **398 millions de requêtes frauduleuses par seconde**
- Exemple type d'**acteurs/ennemis potentiels** :
  - Une **organisation criminelle** qui **facture 500 M US$** en cyber-attaques et dépense **un 5% (soit 25M US$)** en recherche et développement
  - Une **organisation étatique** ou parrainée par un état ayant des objectifs politiques ou belliqueux

Topologie des Risques Liés à Internet

- Programmes malveillants transmis par e-mail (*e-mail malware*)
- Programmes malveillants transmis sur le web (*web malware*)
- Hameçonnage (*Phising*)
- Pourriels (*spam*)
- Rançongiciels (*ransomware*)
- Attaques sur les dispositifs “Internet des Objets” (*Internet of Things/ IoT related attacks*)
- Modification illicite des informations publiées *(information spoofing and website defacement*)
- Attaques dénis de service (*denial of service* ou *DDoS*)
- ...

Voir Annexe

Excellente source d’information pour le sujet: **Office Fédéral de la Cybersécurité (OFCS): https://www.ncsc.admin.ch/ncsc/fr/home.html**

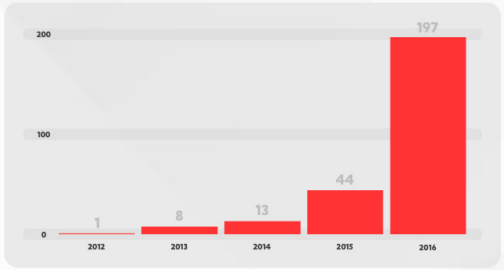
Dissection d'une Attaque: ***Ransomware***

- "Un ***rançongiciel*** (de l'anglais ***ransomware***), ***logiciel rançonneur***, ***logiciel de rançon*** ou ***logiciel d'extorsion***, *est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un* ***rançongiciel*** *chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Un rançongiciel peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent* "[1]
- Le comportement des ***nouvelles générations*** de *ransomware* évolue constamment et constitue une menace contre toutes les sphères de protection de l'information: **confidentialité (**attaques *Fedpol, Fondation de Verdeil* et *Unico Data AG* en 2023**)** , **intégrité** et **disponibilité (***Colonial Pipeline***)**
- Avec **un nombre d'attaques global chiffré en milliards par année**, "***Ransomware Everywhere***" est globalement considérée la menace la plus directe, visible et dangereuse pour utilisateurs et entreprises!

1.Wikipedia. Consulté le 14 janvier 2024

L'Univers du Ransomware[1]

THE RANSOMWARE TUBE MAP



New ransomware families by year of discovery.

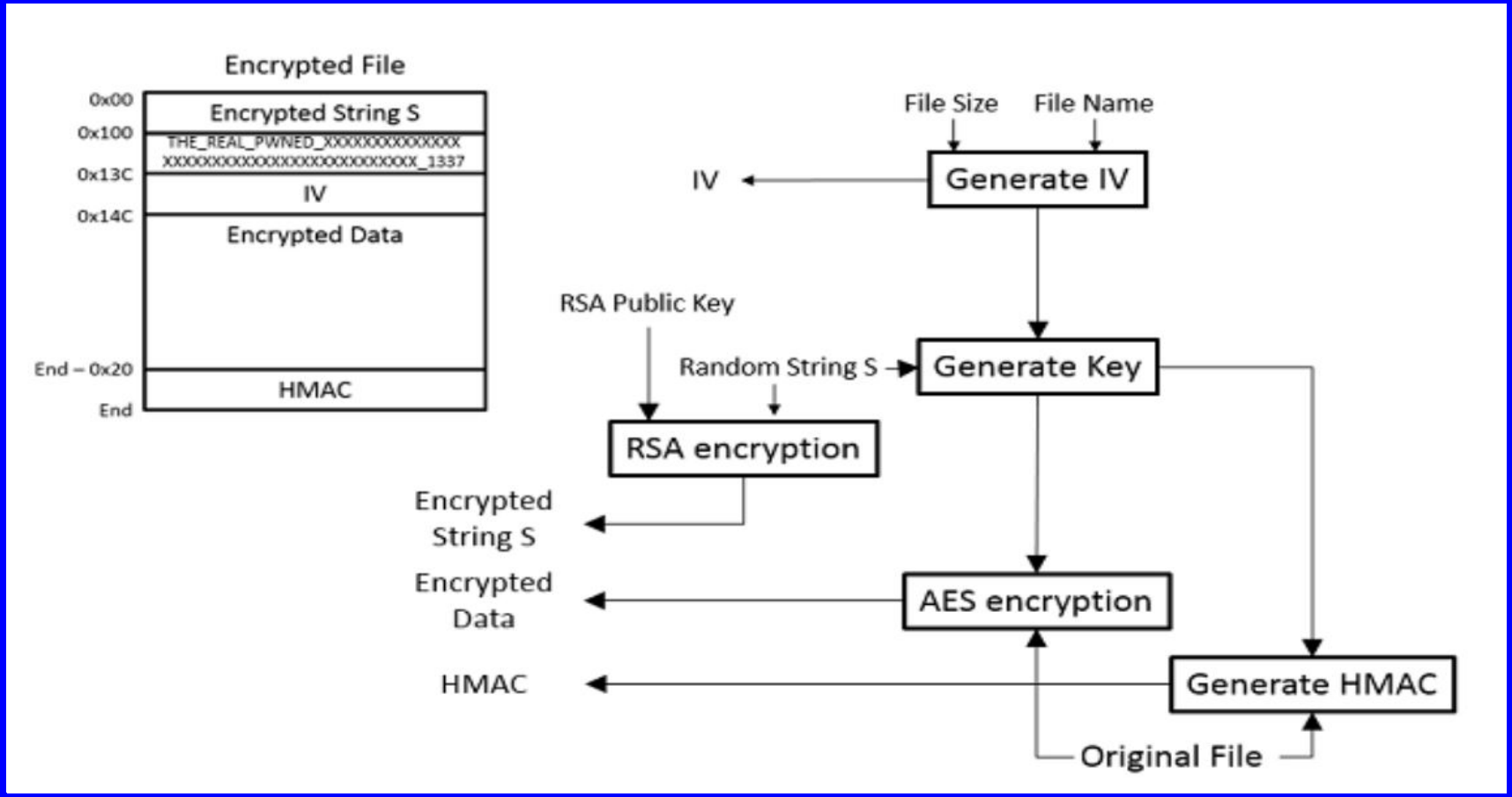
THE SITUATION with crypto-ransomware changed with the emergence of Cryptolocker in 2013. Cryptolocker defined the business model and proved the opportunity. The growth in that business model has been explosive as this graphic clearly shows. Need we say more?

1. *2017 State of Cybersecurity. F-Secure Inc.*

Ransomware: Vue Intégrale

- Prévision, Remédiation et Réaction
  - Application des correctifs *(Patching)*
  - Détection active et passive (*Firewalls*, *WAFs*, *IDS*, *IPS*, *e-mail malware scan*, etc.)
  - *Backups offline* !
  - Politique de Sécurité - Règles de bon usage de la messagerie
  - Formation !
  - Payer ou pas payer...
- Dissection Technique de l'Attaque
  - Infection et propagation
  - Exécution
  - Paiement (*Crypto-currencies* / *Bitcoin*)
  - Occultation (*Obfuscation*, *TOR Networks/Deep Web*)

Schéma Générique d'un *Ransomware Cryptolocker*



- Les **clés privées** de déchiffrement sont **stockées dans les serveurs de l'attaquant**
- Elles sont envoyées à la victime après **paiement en *bitcoins***
- La **trace** est **broyée** à l'aide des **réseaux *TOR (Darkweb)***

Cybersécurité: Nouvelles Tendances

- Prolifération d'attaques ***zero-day***: **vulnérabilités non répertoriées**, inconnues des éditeurs de logiciel et **indétectables** par les systèmes de protection (*antivirus*, *pare-feux*, *filtreurs*, etc.)
- Attaques **hybrides** impliquant plusieurs plate-formes (téléphone fixe, smartphone, tablettes, montres intelligentes, etc.) : ***phising, vishing, smishing***
- Attaques spécifiques aux **téléphones portables / *smartphones***: ***SIM swapping, sms et whatsapp frauduleux, zero-click***, etc.
- A titre d'exemple, une **vulnérabilité *zero-day* exploitable sur *whatsapp*** permettant de prendre le contrôle du smartphone sans intervention de l'utilisateur (***zero-click)*** **cotise à 20 millions de dollars** dans le ***Darkweb***[1]
- ***L'Apocalypse Quantique*** et ses risques pour la cryptographie (**long terme**)
- Menaces associées à l'**Intelligence Artificielle** permettant de viser l'**ingénierie sociale, l'offuscation de code, l'automatisation d'attaques, l'authentification biométrique**, etc.

1.*https://techcrunch.com/2023/10/05/zero-days-for-hacking-whatsapp-are-now-worth-millions-of-dollars/* consultée le 24 janvier 2024

Attaques sur les Empreintes Digitales

ars TECHNICA

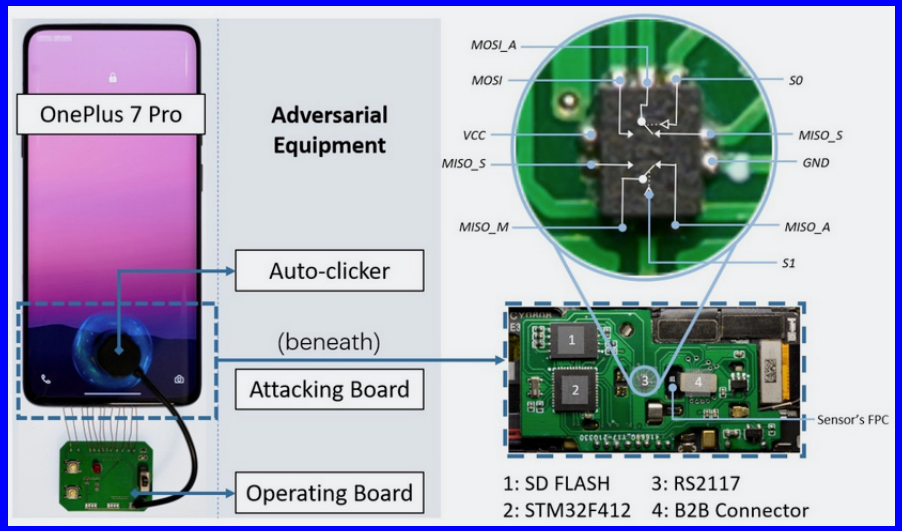
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

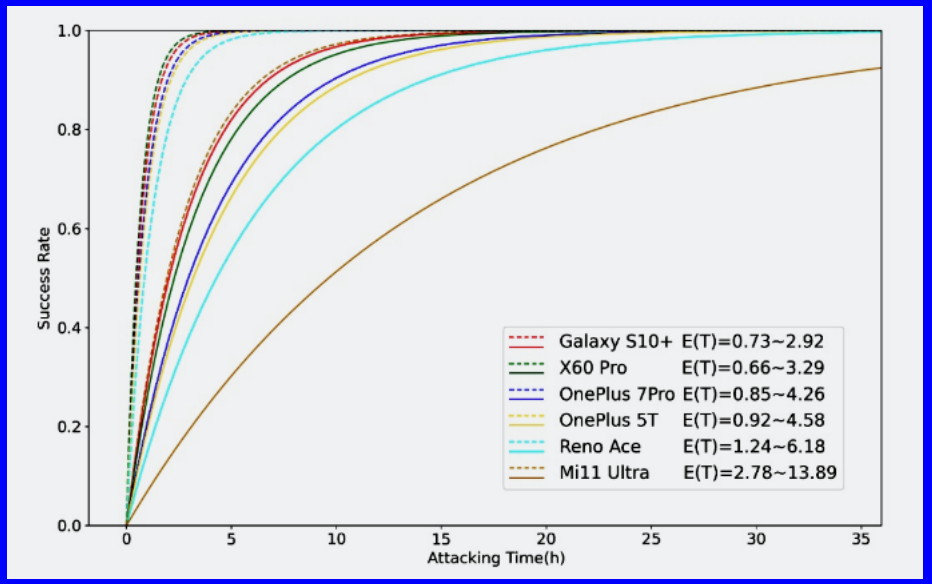
BRUTEPRINT —

Here's how long it takes new BrutePrint attack to unlock 10 different smartphones

BrutePrint requires just $15 of equipment and a little amount of time with a phone.

DAN GOODIN - 5/23/2023, 12:31 AM





Attaques sur l'Identification par la Voix

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

MY VOICE IS NO LONGER MY PASSWORD —

Microsoft's new AI can simulate anyone's voice with 3 seconds of audio

Text-to-speech model can preserve speaker's emotional tone and acoustic environment.

BENJ EDWARDS - 1/9/2023, 11:15 PM

Ars Technica

Enlarge / An AI-generated image of a person's silhouette.

Vidéo Falsifiées (*Fakes* et *Deep-Fakes)*

***La démocratie à l'épreuve du fake*. Conférence d'Alain Berset à l'Université de Genève - 9 mars 2018.**

Fausse vidéo d'Alain Berset dans un site frauduleux d'investissement !
Source: NCSC - 7 décembre 2023

Attaques sur le Comportement (*Frappes Clavier)*

A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards

Joshua Harrison[1], Ehsan Toreini[2], and Maryam Mehrnezhad[3]

[1]Durham University, joshua.b.harrison@durham.ac.uk
[1]University of Surrey, e.toreini@surrey.ac.uk
[1]Royal Holloway University of London,
maryam.mehrnezhad@rhul.ac.uk

August 3, 2023

Abstract

With recent developments in deep learning, the ubiquity of microphones and the rise in online services via personal devices, acoustic side channel attacks present a greater threat to keyboards than ever. This paper presents a practical implementation of a state-of-the-art deep learning model in order to classify laptop keystrokes, using a smartphone integrated microphone. When trained on keystrokes recorded by a nearby phone, the classifier achieved an accuracy of 95%, the highest accuracy seen without the use of a language model. When trained on keystrokes recorded using the video-conferencing software Zoom, an accuracy of 93% was achieved, a new best for the medium. Our results prove the practicality of these side channel attacks via off-the-shelf equipment and algorithms. We discuss a series of mitigation methods to protect users against these series of attacks.

Index terms— Acoustic side channel attack, Deep learning, User security and privacy, Laptop keystroke attacks, Zoom-based acoustic attacks

Attaques sur l'Ecriture Manuscrite

Homework Machine

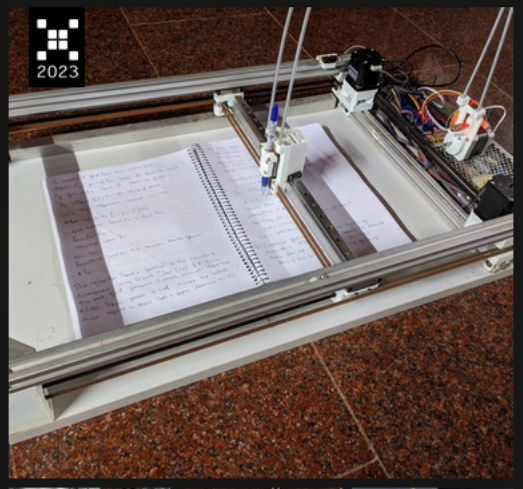
A machine that writes stuff for you- in your own handwriting- so you don't have to!

Devadath P R

Follow project | Like project

14.6k views | 34 comments | 119 followers | 133 likes

Description | Details | Files 0 | Components 0 | Logs 2 | Instructions 0 | Discussion 34

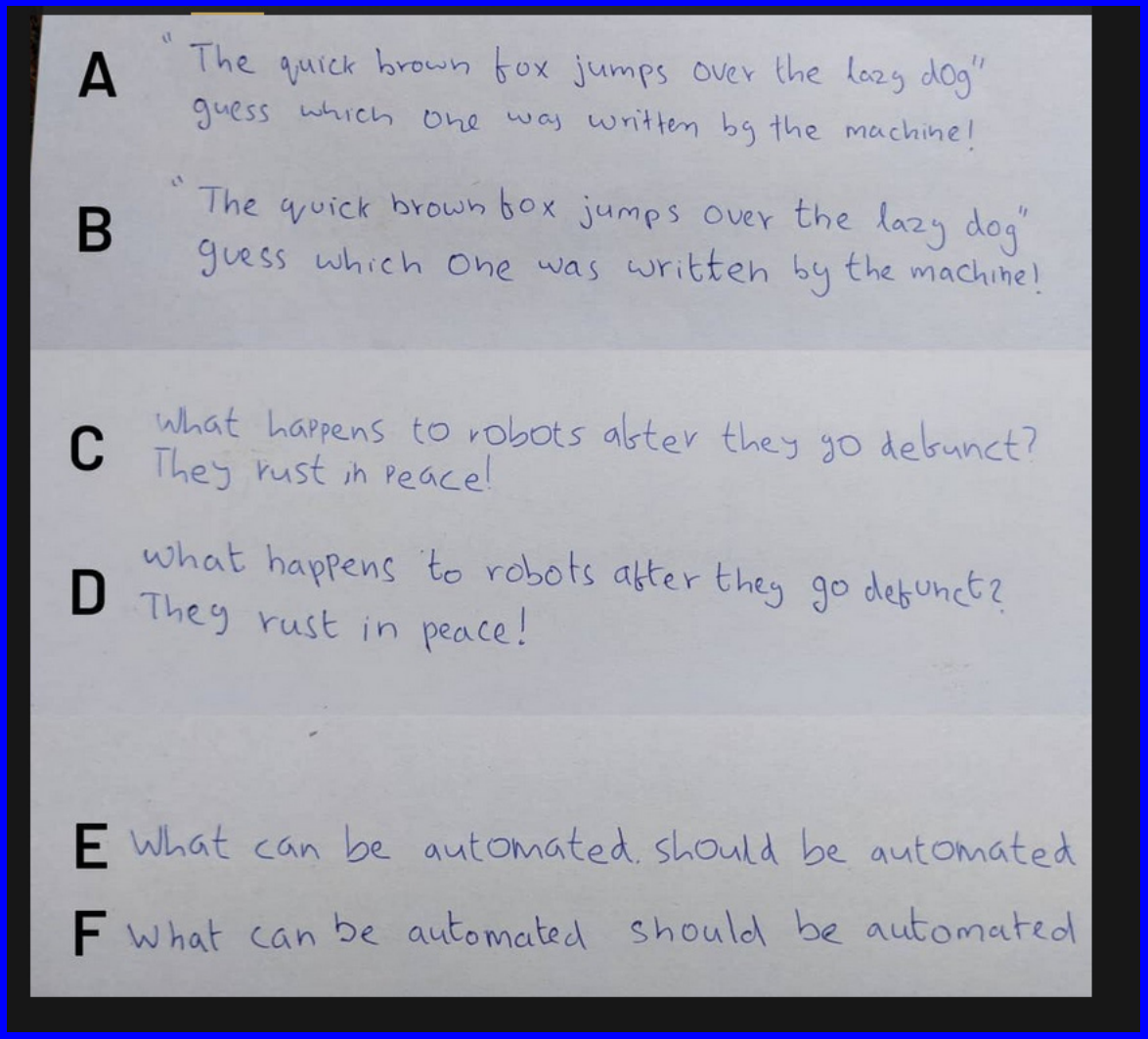


DESCRIPTION

The aim of this project is to create a machine to write stuff for us- In our own handwriting- so we don't have to! When the project is complete, you should be able to upload a question to an app for generating the answers with ChatGPT and Wolfram alpha. A timeslot can be booked for your homework to be written by the machine using the same app. It will write the content in your own handwriting and turn pages of the book automatically until it's done writing.

This is not just any other pen plotter, it has the software and hardware to efficiently and effectively do your homework without getting caught by the teacher. More on that in the details section. I plan to open source this project for students to learn how to create their dream homework machine and develop their skills making one. Hopefully, this will help force the education system to move from rote memorization to a more skill development based learning system.

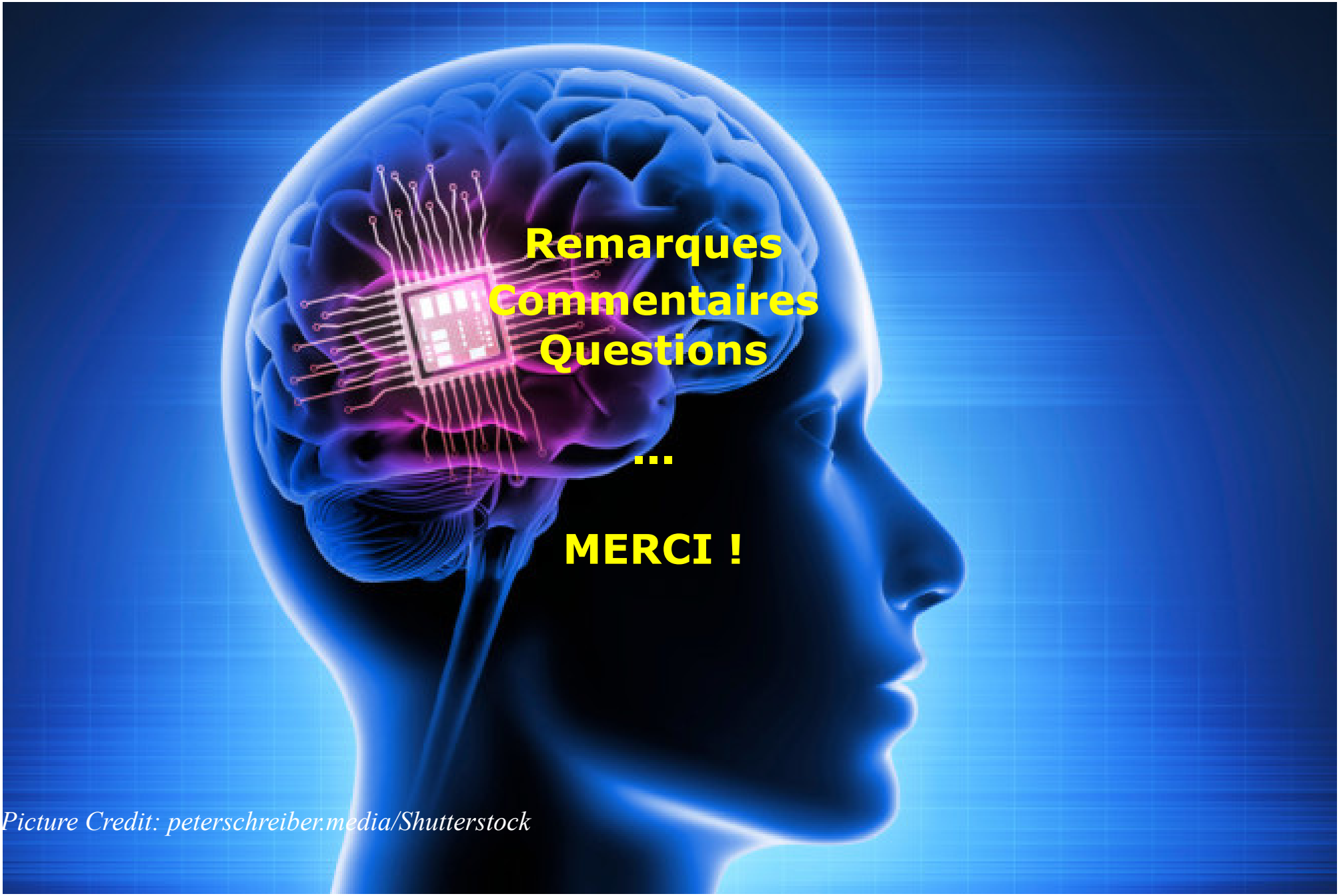
Trouvez la Différence !



A retenir…

- La ***cybersécurité*** est une problématique grandissante qui **nécessite des décisions et des actions fortes des pouvoirs politiques à tous les niveaux** (communal, cantonal et fédéral)
- Une **formation adaptée** à tous les segments de la population est essentielle
- Pensez aux **enfants** et aux **adolescents** dont la vie digitale est devenue indispensable. Une **formation en cybersécurité** est primordiale !
- La **gestion mesurée du risque** (*due diligence*) pour les entreprises est le chemin à suivre mais attention aux attaques indiscriminées
- Un **cadre cybersécurité favorable aux personnes et aux entreprises** deviendra un atout majeur **au même titre que la sécurité physique et juridique**
- **Genève** est un **pôle de compétences** en **cybersécurité** (formation, recherche, expertise académique et professionnelle, etc.). **Financement nécessaire !**

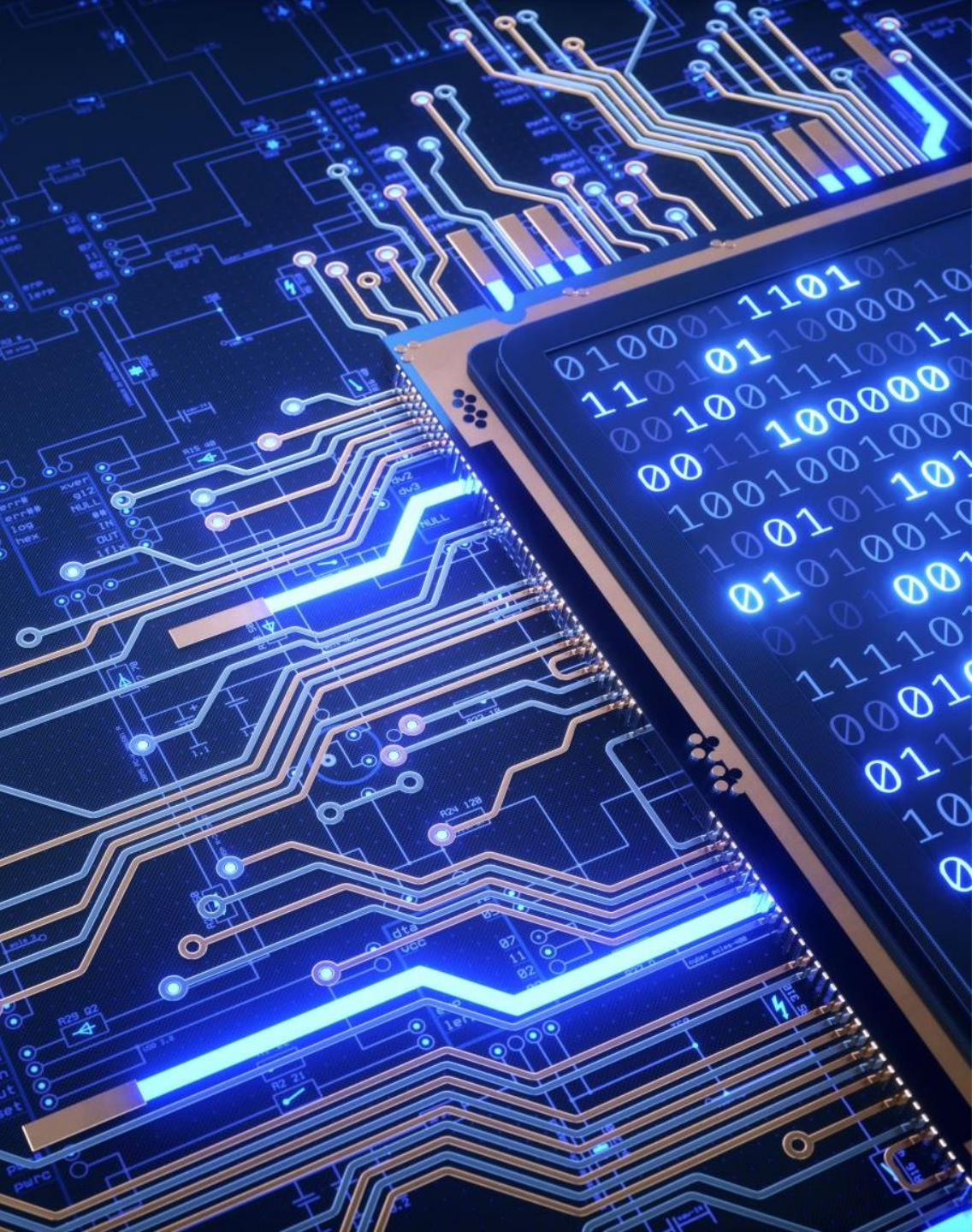
C'est une guerre dont les conséquences et l'évolution sont incertaines



Picture Credit: peterschreiber.media/Shutterstock

Cybersécurité et législation

Les impacts dans le canton de Genève



Plan

- Des exemples
- Qu’est-ce que la cybersécurité ?
- Les difficultés dans la réglementation de la cybersécurité
- La cybersécurité du canton, des communes et des autres infrastructures critiques
  - Une cohabitation des compétences législatives
  - La réglementation cantonale
  - La réglementation fédérale
  - L’influence pour le législateur cantonal
- La cybersécurité des PME
- La cybersécurité de la population
- Une conclusion

Des exemples

LE TEMPS

ÉCONOMIE OPINIONS CULTURE SOCIÉTÉ SCIENCES SPORT DATA ÉVÉNEMENTS VIDÉOS

Anouch Seydtaghia

Publié le 22 janvier 2024 à 07:04. / Modifié le 22 janvier 2024 à 20:13.

La vague de cyberattaques qui frappe la Suisse ne faiblit pas. Ces derniers jours, l'armée de l'air helvétique s'est fait voler des documents. Le Conseil œcuménique des Eglises a été attaqué par un logiciel d'extorsion (rançongiciel), tout comme la ville de Baden. Face à cette déferlante, les

https://www.letemps.ch/economie/la-demande-pour-les-cyberassurances-est-tres-forte-car-les-attaques-peuvent-tuer-une-entreprise

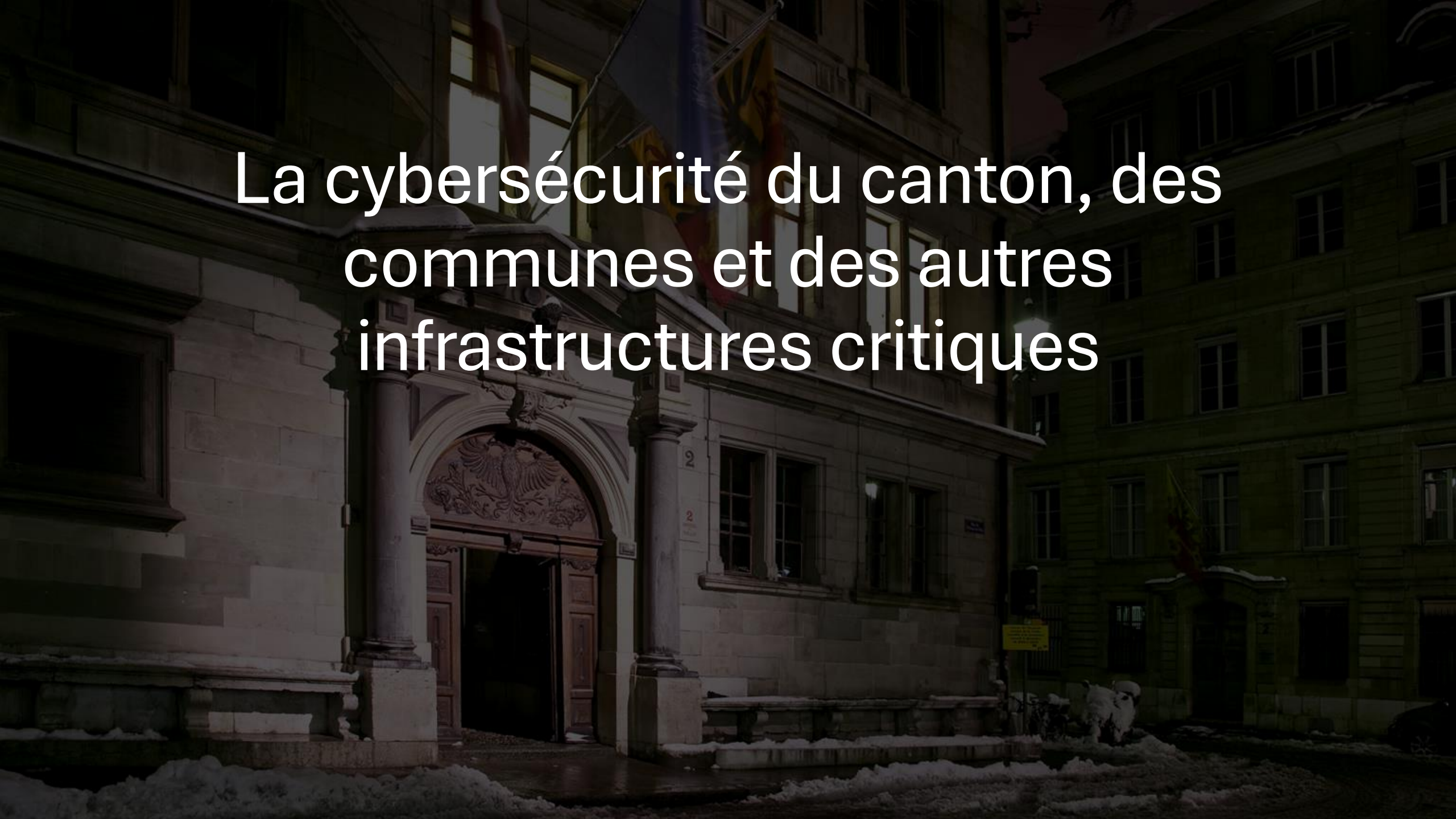
Qu’est-ce que la cybersécurité ?

- La cybersécurité comme domaine :
  - « Ensemble des mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu’à développer la coopération internationale à cet effet » (art. 6 lit. a de l’ancienne Ordonnance sur les cyberrisques, aOPCy)
  - Partie de la transition numérique
  - La transition numérique dans les politiques et les stratégies
  - Les domaines connexes

- La cybersécurité comme état :
  - « La situation dans laquelle le traitement des données, notamment l’échange de données entre les personnes et les organisations par l’intermédiaire d’infrastructures d’information et de communication, fonctionnent comme prévu » (art. 3 lit. a aOPCy)

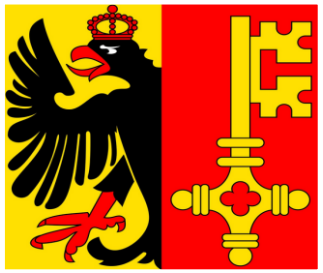
Les difficultés dans la réglementation de la cybersécurité

- Un domaine émergeant et particulièrement évolutif
- La cybersécurité à la croisée d'autres domaines
- Une diversité de parties prenantes concernées
- Un ensemble de compétences
  - L'autoréglementation
  - Des compétences législatives cantonales et fédérales



La cybersécurité du canton, des communes et des autres infrastructures critiques

Une cohabitation des compétences législatives



Des compétences cantonales

Le Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (**ROGSIC**)

La Loi genevoise sur l'administration en ligne (**LAeL**) et son règlement

La Loi sur l'information du public, l'accès aux documents et la protection des données (**LIPAD**)

...

Des compétences fédérales

La Loi sur la sécurité de l'information (**LSI**) et ses ordonnances

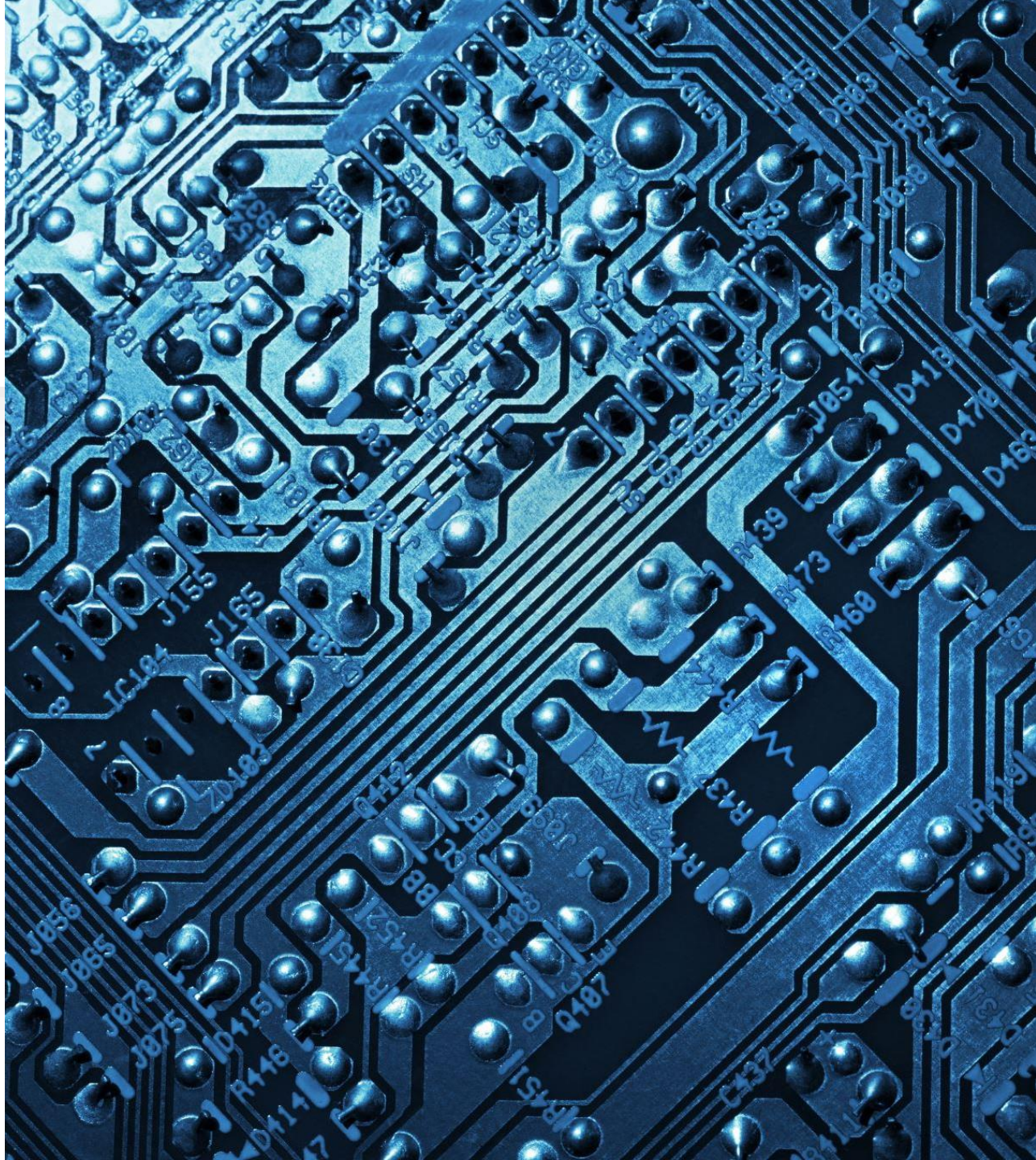
La Loi sur la protection des données (**LPD**) et ses ordonnances

Les lois sectorielles (p. ex. la Loi fédérale sur l'approvisionnement en électricité (**LApEl**) et son ordonnance)

...

La réglementation cantonale

- Le ROGSIC
  - La sécurité de l’information au sein de l’administration cantonale
- La LAeL et son règlement
  - La sécurité des informations et des données dans les services en ligne et sur le site internet officiel de l’Etat
- La LIPAD
  - La sécurité des données personnelles



La réglemenation fédérale

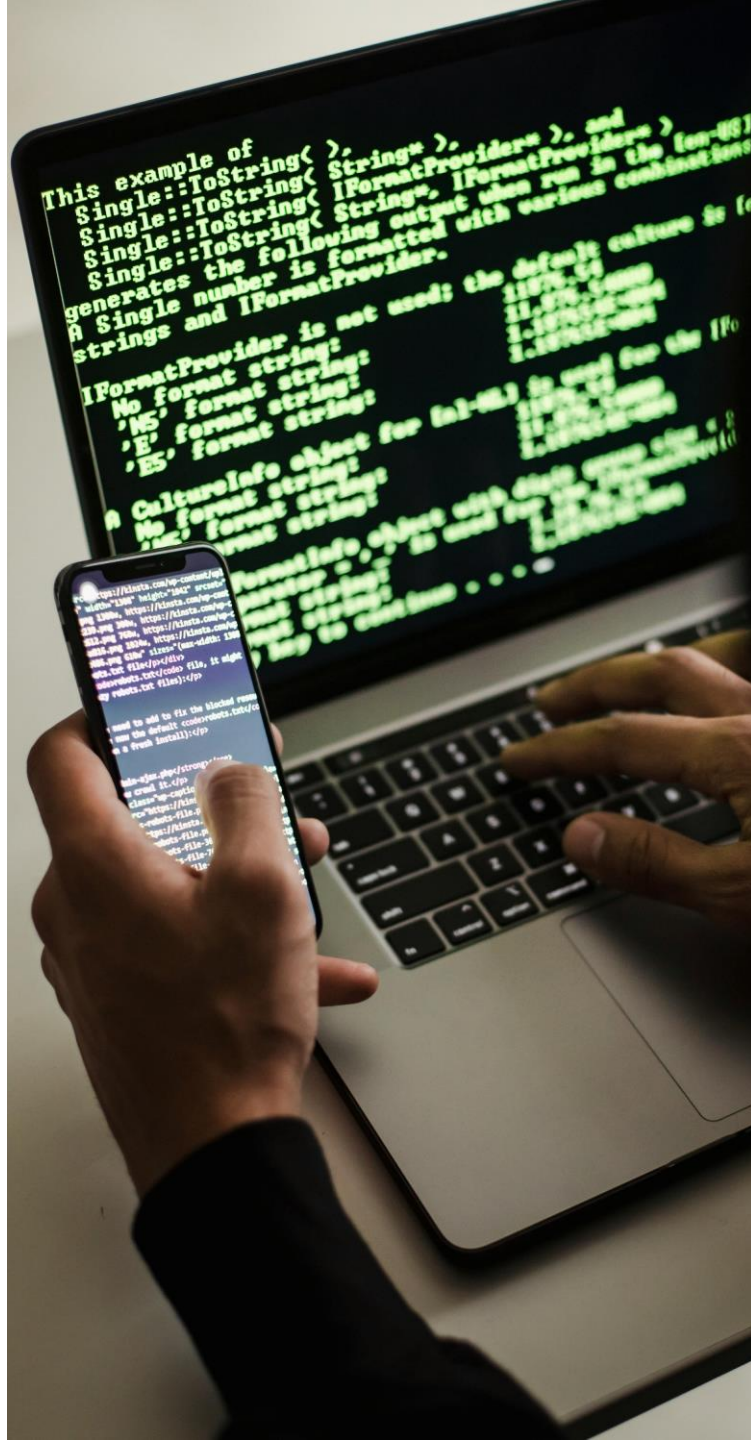
- L’origine et les objectifs de la LSI
- Ses exigences relatives à la sécurité de l’information et à la sécurité des moyens informatiques
- Sa révision ou l’introduction de signaler les cyberattaques ciblant les infrastructures critiques

La législation fédérale

- La LSI : quels impacts au niveau cantonal ?
  - Les exigences minimales applicables aux cantons :
    - Le traitement d'informations classifiées de la Confédération
    - L'accès aux moyens informatiques de la Confédération

La législation fédérale

- La LSI : quels impacts au niveau cantonal ?
  - L’obligation de signaler les cyberattaques visant les infrastructures critiques
    - Les entités concernées
    - Les conséquences concrètes



L’influence pour le législateur cantonal

- Est-ce que la situation cantonale est suffisante ?
- La LSI comme source d’inspiration ?

La cybersécurité des PME

La cybersécurité des PME

- Les autres outils
  - L’accompagnement et le soutien
  - La sensibilisation et la prévention
- La réglementation en soutien aux autres outils pour la cybersécurité des PME

La cybersécurité de la population

La cybersécurité de la population

- La sensibilisation
- Le nouveau droit à l'intégrité numérique
  - La portée
  - La concrétisation légale
- La réglementation en soutien aux autres outils pour la cybersécurité de la population
  - Exemple : le projet de loi modifiant la loi sur la police

Une conclusion

- La réglementation comme levier d'action pour améliorer la cybersécurité des infrastructures critiques…
  - Malgré la complexité pour les législateurs (cantonaux)

- La réglementation en soutien aux autres outils pour la cybersécurité des PME et de la population…
  - Mais nécessité de combiner les différents leviers d'action

Pour aller plus loin…

- Meyer Pauline/Métille Sylvain, Recommandation législative,12.2023, https://www.nfp77.ch/media/fr/ft0PqQ66jRBKDe8k/nfp77-lwp-fr.pdf

  → PNR-77 « Promoting trust in cybersecurity through ethics and law »,

- Meyer Pauline/Métille Sylvain, Loi fédérale sur la sécurité de l'information : version 2.0, Jusletter 10.2022, https://serval.unil.ch/fr/notice/serval:BIB_9AFC465B2EED

- Meyer Pauline/Pangrazzi Sara/Sarrasin Delphine, Ransomware Payments: On Regulatory Incentives to Limit Them, PJA 2023/10

Merci pour votre attention !

pauline.meyer.3@unil.ch

Parldigi MasterClass

Grand Conseil de la République et Canton de Genève

prochain événement: **1er mars 2024**

Transition numérique et démocratie

Prof. Tommaso Venturini,
Medialab, Université de Genève

Prof. Alexandre Bovet,
Membre de la Digital Society Initiative, Université de Zurich

---

Un événement organisé par:

Universität Zürich[UZH]
Digital Society Initiative

Parldigi

UNIVERSITÉ DE GENÈVE
CENTRE UNIVERSITAIRE D'INFORMATIQUE

Partenaire:

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

Soutenu par:

Stiftung Mercator Schweiz