Cycle de formation à la gestion responsable des données

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Session 5
Les enjeux actuels, et comment ils s'appliquent à vous

Introduction de la dernière session

Et maintenant…

1/ Les différentes dimensions de la gestion responsable des données

2/ Focus sur la protection des données

3/ Les concepts de la gestion responsable des données en action- partie 1

4/ Les concepts de la gestion responsable des données en action- partie 2

5/ Découvrir comment les enjeux actuels s'appliquent à vous

Agenda de la session 5

- Introduction à la session d'aujourd'hui
- Focus sur 4 enjeux

- Travail de groupe sur les enjeux
- Clôture de la formation
  - Quels apprentissages?
  - Enquête de satisfaction
  - Conclusion

L'élaboration de ce matériel de formation est soutenue par le Ministère français de l'Europe et des Affaires étrangères (MEAE-CDCS). Néanmoins, les idées et opinions présentées dans cette formation ne représentent pas nécessairement celles du MEAE-CDCS.

Les 4 enjeux

Présentation de nos intervenants

CyberPeace Institute
Alexandru Lazar - Responsable du programme CyberPeace Builders
Zacharia Okere - Spécialiste de la cybersécurité pour les organisations à but non lucratif, based in Nairobi

Le CyberPeace Institute est une organisation basée à Genève qui protège les plus vulnérables dans le cyberespace. Indépendant et neutre, l'Institut étudie et analyse l'impact humain des cybermenaces systémiques, fournit une assistance gratuite en matière de cybersécurité, suit l'application des lois et des normes internationales et prévoit les menaces qui pèsent sur la cyberpaix.

The Engine room
Quito Tsui - Associé, équipe de recherche et d'apprentissage
Helen Kilbey - Responsable éditoriale

The Engine room est une organisation à but non lucratif composée d'une équipe mondiale répartie de militants, de chercheurs, de technologues et d'organisateurs communautaires expérimentés et engagés. Cette équipe engagée renforce la lutte pour la justice sociale en aidant la société civile à utiliser la technologie et les données de manière stratégique, efficace et responsable.

Quiz

Cybersécurité


cyber
peace
builders.
CyberPeace
Institute
ASSISTANCE | ANALYSIS | ADVANCEMENT


CyberPeace
Institute
COMPRENDRE LES CYBER RISQUES DANS LE MONDE DES ONG
cyber peace builders


Je vois une maison à vendre.

CyberPeace Institute

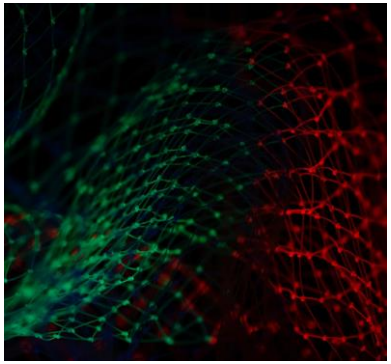
LES ACTEURS MALVEILLANTS ET LEURS INTÉRÊTS

Hacktivists

- ✓ Les organisations connues mondialement peuvent être vues comme un trophée
- ✓ Les attaques peuvent être menées par hasard voir par erreur
- ➢ Divertissement

Groupes criminels

- ✓ Les organisations internationales, les organisations reconnues peuvent sembler riche
- ➢ Gain financier



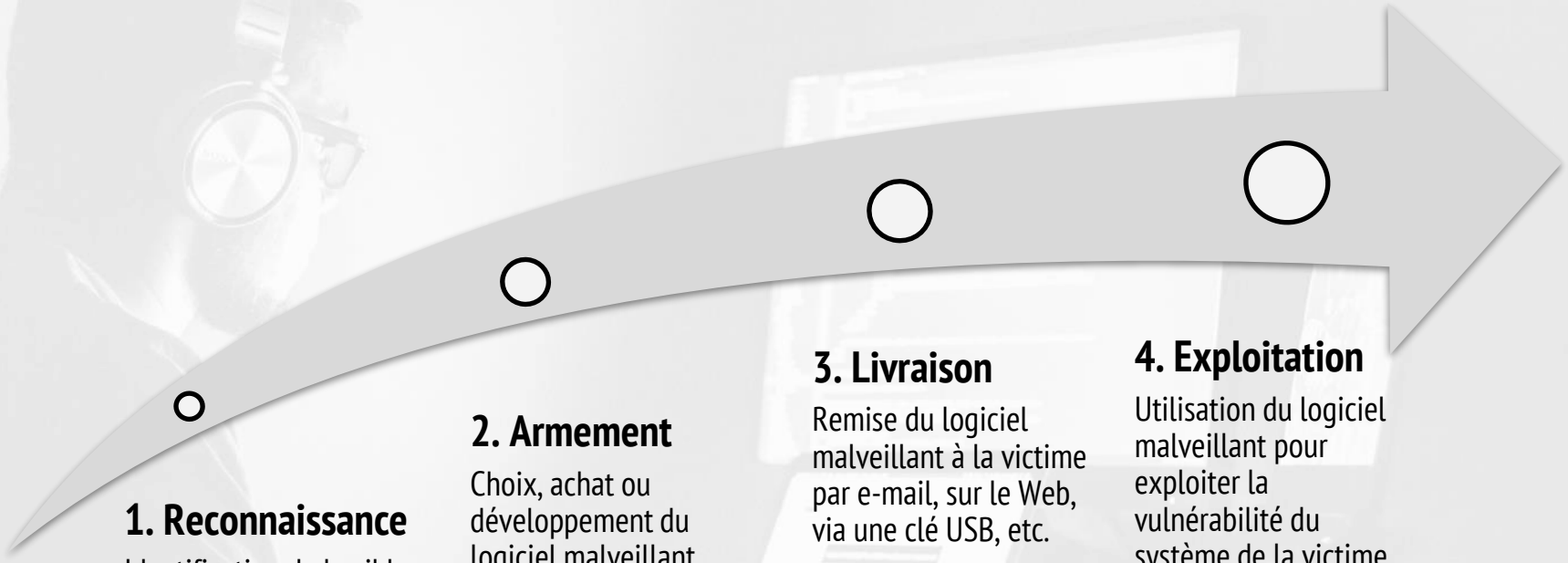
États et groupes soutenus par des États

- ✓ Les organisations ou les individus détiennent des informations sensibles
- ✓ Les activités peuvent être considérées comme dérangeantes
- ➢ Espionnage, sabotage

cyber peace builders.

cartong

LA “CYBER KILL CHAIN” SIMPLIFIÉE



1. Reconnaissance

Identification de la cible et de ses points faibles et planification de l’attaque, éventuellement par ingénierie sociale

2. Armement

Choix, achat ou développement du logiciel malveillant approprié

3. Livraison

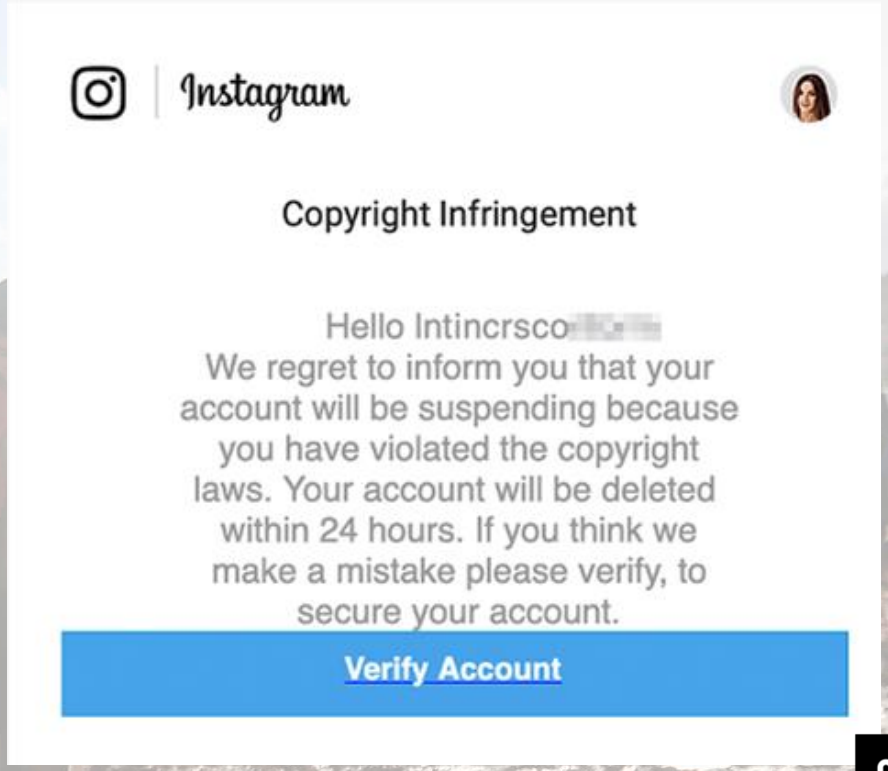
Remise du logiciel malveillant à la victime par e-mail, sur le Web, via une clé USB, etc.

4. Exploitation

Utilisation du logiciel malveillant pour exploiter la vulnérabilité du système de la victime

RÉSEAUX SOCIAUX

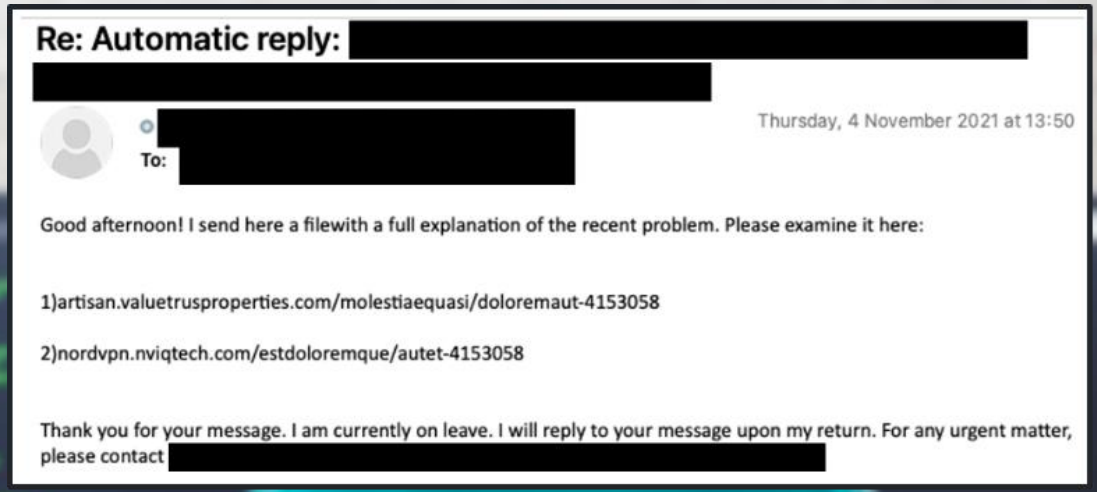
Que se passe-t-il sous vous perdez vos accès aux comptes de réseaux sociaux?



Plus d'information: https://cyberpeaceinstitute.org/news/testimonial-uicc/

E-MAIL COMPROMIS

Et si vos partenaires ne vous font plus confiance?



Plus d'information: https://cyberpeaceinstitute.org/news/ngos-caught-in-the-net/

AIDER LES ONG À COMPRENDRE LE RISQUE CYBER

85%

Des ONG pensent que leur personnel représente un risque important en termes de cybersécurité, mais seulement **55 %** d'entre elles organisent régulièrement des formations de sensibilisation à la cybersécurité.

1. Commencer par une évaluation des risques
2. Identifier vos actifs critiques et leur emplacement
3. Déterminer qui peut représenter une menace pour votre organisation
4. Identifier vos vulnérabilités


cyber
peace
builders.
Experts en cybersécurité, tous métiers confondus,
employés par des entreprises locales et internationales.
Aidant gratuitement les ONG à travers le monde

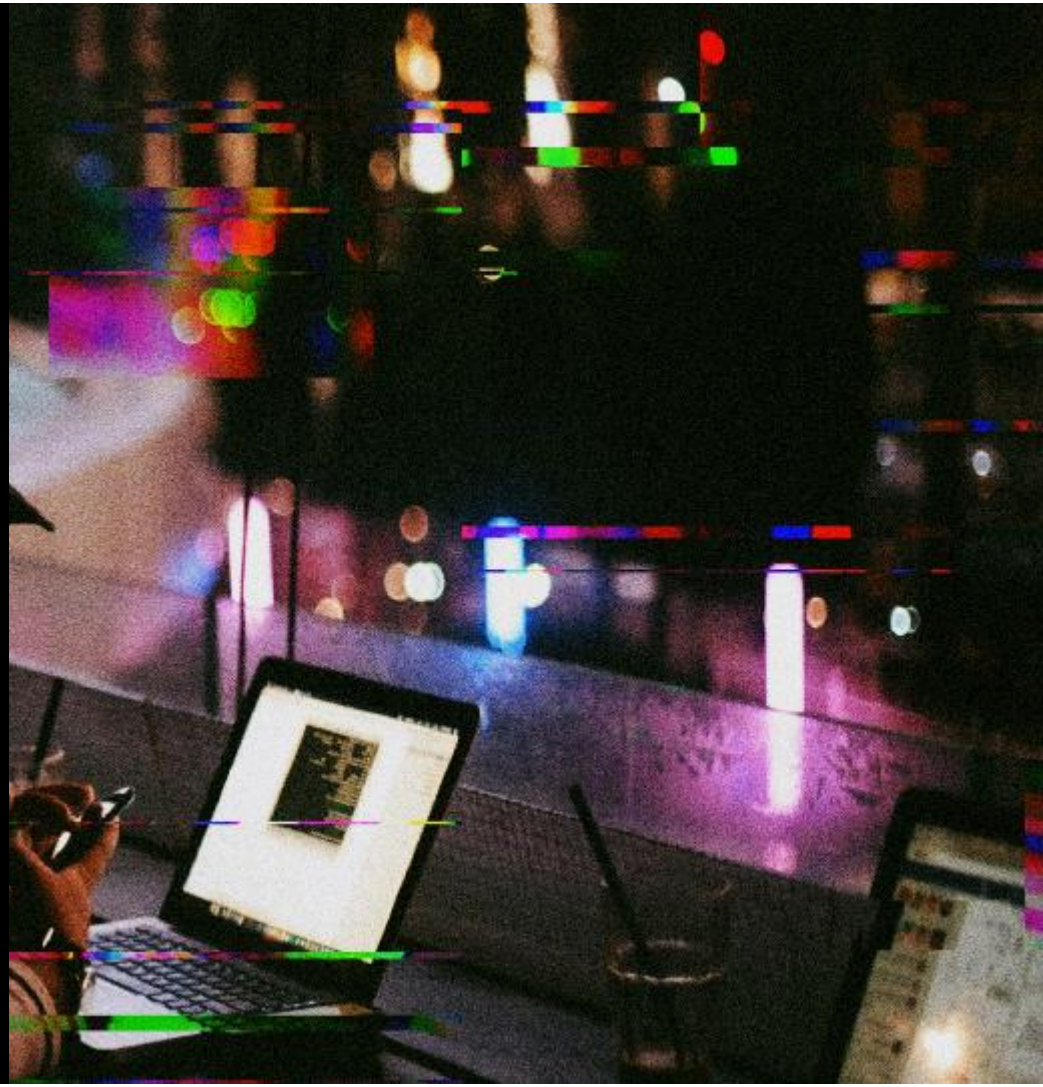
CyberPeace Institute

cyber peace builders.

THANK YOU

assistance@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

CyberpeaceInstitute
@CyberpeaceInst
The CyberPeace Institute



Désinformation / Mésinformation

Désinformation / Mauvaise information

Ce que c'est :

Ces phénomènes sont des perceptions relayées par l'information qui ne reflètent pas la réalité - des impacts substantiels et transversaux.

La désinformation fait référence à de fausses informations qui n'ont pas pour but de causer des préjudices.
Considérant que la *désinformation* fait référence à de fausses informations destinées à manipuler, à causer des dommages ou à orienter les personnes, les organisations et les pays dans la mauvaise direction

Les discours de haine "contribuent directement ou indirectement à mettre en danger la sécurité ou la dignité des populations civiles" (CICR).

Les enjeux :

- **Phénomènes d'accélération** dus à la diffusion massive des technologies
- La désinformation **se répand plus vite que la vérité**
- Peut entraîner une **perte de confiance des communautés**, exacerbée dans les situations de peur et d'incertitude.
- Impact sur les **capacités des ONG** à déployer des activités
- Elle est préjudiciable aux personnes : elle augmente les "risques et les vulnérabilités" (CICR).

Pour en savoir plus :

- CICR : Q&R sur les conséquences de la désinformation, de la désinformation et du discours de haine dans le secteur humanitaire & podcast sur la désinformation et l'action humanitaire.
- Institut Cyberpeace : ChatGPT et la crise sanitaire liée à Covid 19
- Centre canadien pour la cybersécurité : comment identifier la désinformation, la désinformation et la malinformation ?
- Internews : rapport sur la gestion de la désinformation dans un contexte humanitaire
- ICTworks : 7 recommandations et comment lutter contre la désinformation en Europe centrale et orientale
- The Newsguard : Article sur la désinformation massive
- Manchesterhive : article sur "La communication humanitaire dans un monde post-vérité".
- Oxfam et la salle des machines : Exemple de désinformation dans les camps

Un exemple : Le CICR au Burkina Faso

Un consortium journalistique indépendant a révélé en février 2023 que le **CICR** avait été la cible d'une **campagne de désinformation** au Burkina Faso : de fausses informations, fabriquées par une société privée spécialisée, qui avaient été utilisées pour le compte d'hommes politiques.

Conséquences :

- la **"neutralité"** du CICR a été critiquée
- Des commentaires violents ont suscité des **craintes pour la sécurité de** l'équipe locale.
- Le CICR a dû publier **une déclaration pour contredire ces informations.**

Source : la voix de l'Afrique

How misinformation and disinformation harm ICRC's humanitarian work in Burkina Faso

ARTICLE | 17 FEBRUARY 2023 | BURKINA FASO

An independent investigation by a consortium of news organizations resulted in the publication of stories on 16 February 2023 about a disinformation campaign targeting the International Committee of the Red Cross (ICRC) in Burkina Faso. The ICRC is sharing more information about the incident to further clarify the work we do to help victims of conflict and other situations of violence.

Source : le CICR

Que pouvez-vous faire pour lutter contre ces phénomènes ?

Recommandations, dans la mesure du possible :

- Les équipes de communication doivent **consacrer du temps et des recherches** à la manière dont votre ONG est perçue et aux tendances en matière de désinformation.
- **Établir des relations de confiance** avec les communautés avec lesquelles vous travaillez et les principales parties prenantes.
- Disposer de **données de programmes de qualité**, partagées et acceptées par les communautés : responsabilité des équipes de SERA S'engager à **produire des rapports et des campagnes précis** et les inclure dans la stratégie de communication.

These Les deux derniers points font référence aux principes de **transparence et de redevabilité.**

Source : CICR - manchesterhive

Biométrique

THE ENGINE ROOM

Biométrique

Un examen plus approfondi des risques et des avantages

Comment le biométrique est-il utilisé ?

- Identification et vérification dans le cadre d'opérations humanitaires
- Systèmes généraux et fonctionnels
- Les technologies biométriques capturent les aspects clés d'un échantillon biométrique dans un gabarit biométrique

Pourquoi les informations biométriques sont-elles sensibles ?

- ❏ Unicité et immuabilité
- ❏ Richesse de l'information
- ❏ Flexibilité d'utilisation

Un examen plus approfondi des avantages

+ Les avantages anticipés associés aux systèmes de biométrie n'ont pas changé de manière significative depuis 2018.
+ Les avantages potentiels sont les suivants : amélioration du processus de distribution de l'aide grâce à une plus grande efficacité de l'enregistrement ; traçabilité, déduplication et contrôle de la fraude ; précision accrue des données et, en tant qu'outil de lutte contre la corruption, avantages économiques pour les particuliers et les organisations humanitaires.
+ Toutefois, les preuves de ces avantages proviennent souvent d'études de cas réalisées en dehors du secteur humanitaire et ne tiennent pas pleinement compte des éventuelles limitations propres au contexte

Un examen plus approfondi des préjudices

+ De nouvelles preuves que les systèmes de biométrie sont à la fois la cause et l'amplificateur de risques et de préjudices.
+ Les risques couvrant l'ensemble du cycle de vie des systèmes biométriques comprennent les défis liés à l'atténuation des risques, les préoccupations concernant la sécurité des données et les préjudices causés aux communautés impactées, la surveillance et l'utilisation abusive des données, ainsi que la possibilité d'un détournement de fonction.
+ La biométrie amplifie les préoccupations plus générales en matière de partage des données concernant le blocage des fournisseurs, les différences entre les parties prenantes en matière de gouvernance des données, les limitations techniques concernant la protection des données et le partage des données régi de manière opaque.

Études de cas de préjudice

Étude de cas : Partage non consensuel de données sur les réfugiés rohingyas au Bangladesh
Les réfugiés au Bangladesh ont vu leurs données biométriques traitées dans le cadre d'un exercice de vérification conjoint entre le gouvernement bangladais et le HCR, dans le cadre d'un processus visant à préserver leur droit au retour volontaire et à leur fournir un document d'identité individuel. Les données biométriques sous forme d'empreintes de pouce sur des documents papier ont ensuite été partagées par le gouvernement du Bangladesh avec les autorités du Myanmar dans le cadre des efforts visant à préserver le droit au retour. De nombreux réfugiés ignoraient toutefois que ces informations seraient communiquées par le gouvernement bangladais aux autorités du Myanmar afin de faciliter éventuellement leur rapatriement.

Étude de cas : Double enregistrement au Kenya
Le double enregistrement des ressortissants somaliens kényans dans les bases de données des réfugiés et dans les bases de données nationales a eu pour conséquence que les ressortissants somaliens kényans doublement enregistrés n'ont pas pu accéder à leurs droits de citoyenneté.Les quelques 40 000 citoyens kenyans enregistrés dans la base de données sur les réfugiés - dont la majorité a moins de 40 ans et dont les données ont souvent été saisies lorsqu'ils étaient enfants - se sont retrouvés de facto apatrides.

Étude de cas : Le PAM et l'impasse des Houthis au Yémen
À la suite d'allégations selon lesquelles des agents des Houthis auraient interféré dans la livraison de l'aide alimentaire, le PAM a cherché à introduire un système biométrique. Cependant, les dirigeants houthis ont demandé l'accès à ces informations biométriques comme condition de mise en œuvre. Le désaccord sur l'accès a conduit à une suspension partielle de l'aide en juin 2019, avant de parvenir à un accord avec les Houthis quelques mois plus tard. L'accord souligne la nécessité d'une transparence totale dans l'enregistrement des bénéficiaires de l'aide et inclut une base de données biométriques, les informations étant stockées sur un serveur commun hébergé au Yémen et non connecté à internet.

Tracer la voie vers des politiques responsables en matière de biométrie

1. Poursuite de l'interrogation sur la nécessité du biométrique

+ Comment concevoir la nécessité dans le contexte du biométrique?
+ Les technologies biométriques sont-elles la seule option pour relever un défi donné ?
+ Comment les praticiens de l'humanitaire peuvent-ils créer un espace pour des solutions alternatives ?
+ Comment résister à la dépendance de trajectoire ?
+ Quelles étapes peuvent-elles être codifiées pour s'assurer que l'adoption du biométrique est motivée par un besoin réel ?

2. Une conception et une mise en œuvre plus nuancées des politiques

+ Qui est pris en compte dans le processus d'élaboration et de mise en œuvre des politiques ?
+ Nos politiques sont-elles accessibles ?
+ Nos politiques peuvent-elles être mises en œuvre ?
+ Comment créer un espace pour les retours (feedback) et pour échanger en lien avec les critiques potentielles ?
+ De quelle manière les processus de recrutement, par exemple la rotation élevée du personnel, les contrats à court terme, influencent-ils la manière dont nous concevons et mettons en œuvre les politiques ?

3. Établir des normes de pratique centrées sur la communauté

+ Les organisations similaires et/ou partenaires fonctionnent-elles sur la base d'un cadre de compréhension commun ?
+ Comment créer une cohérence dans le secteur en ce qui concerne l'utilisation du biométrique?

4. Renforcer les pratiques relatives aux analyses d'impact sur la protection des données (DPIA)

+ Comment s'assurer que les DPIA sont compris par toutes les parties prenantes ?
+ Comment élaborer des DPIA suffisamment détaillés ?
+ Comment maintenir les DPIA et atténuer les nouveaux risques après l'évaluation initiale et pendant le cycle de vie d'un projet ?

5. Analyse plus sophistiquée des technologies à l'échelle de l'écosystème

+ Quels sont les modes de pensée qui guident la prise de décision ?
+ Comment reconnaître les environnements à ressources limitées des contextes humanitaires, tout en évitant une dépendance excessive à l'égard des solutions technologiques ?
+ Quel est le rôle approprié des acteurs du secteur privé qui n'adhèrent pas explicitement aux principes humanitaires ?

Intelligence artificielle

Intelligence Artificielle

Ce que c'est :
"L'intelligence artificielle (IA) désigne **l'ensemble des techniques qui permettent à une machine de simuler l'apprentissage humain**, c'est-à-dire d'apprendre, de prédire, de prendre des décisions et de percevoir son environnement. Dans le cas d'un système informatique, l'intelligence artificielle est appliquée aux données numériques."
(Déclaration de Montréal)

Machine Learning: Une extension de l'IA. Capacité de **prédiction ou de décision** basée sur des données.

IA générative est un type de système d'IA **capable de générer du texte, des images ou d'autres médias** en réponse à des invites (ou prompts en anglais)

Il n'existe pas une « IA globale », mais plutôt une **diversité d'IA spécialisées.**

Lectures supplémentaires:

- OECD principles: https://www.oecd.org/going-digital/ai/principles/
- ICO guidance: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
- Montreal Declaration on Responsible AI :https://www.montrealdeclaration-responsibleai.com/
- Privacy International guidance :https://www.privacyinternational.org/learning-topics/artificial-intelligence and https://www.privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf
- Ethique IA - 5 raisons pour lesquelles l'engagement des organisations à but non lucratif est essentiel: https://nethope.org/articles/ai-ethics-5-reasons-why-nonprofit-engagement-is-key/

Intelligence Artificielle

Sujets d'intérêt

- Diagnostics médicaux
- Analyse prédictive des crises
- Analyse de l'évolution du contexte
- Productivité agricole
- Traitement et analyse des données
- Détection des fraudes
- Détection des menaces
- Télédétection
- Analyse pour l'alimentation et la sécurité
- Prévision des mouvements de population
- Traduction, production ou synthèse de documents

Intelligence Artificielle

Plus les choses changent, plus elles restent les mêmes ?

- L'approche "Do no harm" (ne pas nuire) reste au premier plan
- Les principes de la gestion responsable des données s'appliquent toujours
- Les données sont rarement neutres et les préjugés sont omniprésents
- Nécessité et responsabilité d'évaluer les risques
- Privilégiez les personnes et les compétences plutôt que les outils, les systèmes et les dernières "innovations" et gadgets,
- Une confiance excessive dans les systèmes d'IA pourrait contribuer à la reproduction des inégalités structurelles et des inégalités intégrées dans les ensembles de données.
- Les « Big Tech » sont la principale force qui façonne la trajectoire de la recherche et la conversation politique et populaire autour de l'IA.

Intelligence Artificielle: Les enjeux

Principes éthiques

(source: ICT works)

- L'équité
- Autonomie et surveillance
- Vie privée et sécurité
- Sûreté et robustesse
- Transparence et explicabilité
- Responsabilité
- Impact sur l'environnement

Inéluctable ne veut pas dire subir- L'humanitaire doit **s'adapter et participer à l'orientation que peut prendre l'IA dans le secteur en influençant les développements en cours**

L'encadrement reste flou, insuffisant et fragmenté.

Il est important de **continuer d'expliquer le sujet de la protection des données** (qui est déjà difficile à appréhender)

Concentrez-vous d'abord sur le problème que vous devez aborder et résoudre, puis sur les données et outils IA dont vous avez besoin pour vous aider à changer ce que vous faites sur le terrain

- Quelles sont les hypothèses à vérifier ?
- Comment déterminer la responsabilité en cas d'erreur?
- Comment pouvons-nous nous approprier ces outils en faisant en sorte qu'ils soient adaptés dans le contexte local ?
- Quels sont les questionnements sur le terrain?

cartong

Passons au travail de groupe !

Discussion en group !

Vous pouvez **choisir le sujet qui vous intéresse le plus**
On attend de vous que chaque groupe **énumère les défis et les mesures à prendre/qu'il aurait fallu prendre sur l'étude de cas**

Numéros de groupe :

- 1/ Cybersécurité
- 2/ Désinformation et désinformation
- 3/ La biométrie
- 4/ L'intelligence artificielle

Restitution

Questions & réponses

Vous avez des questions à poser à nos intervenants ?
Ou des témoignages à partager ?

Pause

Cloture de la formation

Qu'avez-vous appris de la formation et qu'allez-vous en faire ? Travail de groupe

Enquête de satisfaction : prenez 5 à 10 minutes pour la remplir !

Et une fois cette session terminée?

Vous souhaitez un soutien supplémentaire ?

Si vous êtes **intéressé par une consultance avec CartONG** pour vous aider à

- renforcement des capacités ou montée en compétences (formations, coaching, hotline, etc.)
- la mise en œuvre d'outils et d'approches liés aux données programmes

... voici notre portefolio ☺

Contactez vos points focaux (car nous avons des accords de partenariat avec certaines de vos organisations et/ou Maeve (m_defrance@cartong.org) si vous **souhaitez en discuter davantage** !

Et n'oubliez pas : les ressources de référence

Disponible sur https://www.im-portal.org/learning-corner

La liste des ressources en gestion responsable des données que nous avons compilée pour vous !

Disponible sur https://docs.google.com/spreadsheets/d/1rqx94f8hOYqOD3wC-PhpW0ftv7Sck07wBfhqbb9KVqE/edit#gid=487823661

Organisation	Key doc ?	Title	Type	Link	Date
The Engine Room		The Engine Room website	Website	https://www	
The Engine Room		How to start your responsible data journey	Blogpost / Article	https://www	2021
National Cyber Security Centre		NCSC's cyber security training for staff	Training	https://www	2021
CartONG		Why data literacy is important in the aid sector	Blogpost / Article	https://www	2021
OHCHR		Artificial intelligence risks to privacy demand urgent action	Blogpost	https://www	2021
MERL Tech		New Guides! Responsible Data Governance for M&E in Africa	Practical handbook	https://merlt	2022
CMS - GDPR Fines		GDPR Enforcement Tracker	Tutorial / Tips / Tool	https://www	
OXFAM		Biometric and Foundational Identity Policy	Policy	https://oxfar	2021
Responsible Data		Responsible Data website	Website	https://respo	
The Engine Room		RAD planning	Tutorial / Tips / Tool	https://www	2021
ICRC - DigitHarium		Digital Dilemmas Debate #7: Biometrics - 'Overpurposed' by design?	Video	https://www	2021
ICRC		Intro to blog series on human costs of cyber operations	Blogpost / Article	https://blogs	2019
ICRC		Digital risks for populations in armed conflict: Five key gaps the humanitarian sector should address	Blogpost / Article	https://blogs	2019
GIZMODO		Authorities Claim They Accessed Encrypted Signal Chats to Charge Oath Keepers	Blogpost / Article	https://gizm	2022
The Engine Room		Responsible Data Policy	Policy	https://www	
Forbes		Can The FBI Hack Into Private Signal Messages On A Locked iPhone? Evidence Indicates Yes	Blogpost / Article	https://www	2021
ICRC - DigitHarium		Digital Dilemmas Serries (Dialogues & Debates)	Video	https://www	2021
The New Humanitarian		The UN's refugee data shame	Blogpost / Article	https://www	2021
ICRC		You can't handle the truth: misinformation and humanitarian action	Blogpost / Article	https://blogs	2021
ICRC		Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people	Blogpost / Article	https://www	2022
Politico		Suicide hotline shares data with for-profit spinoff, raising ethical questions	Blogpost / Article	https://www	2022
Access Now		Access Now website	Website	https://www	

cartong

Devoirs ☺

- Veillez à **mettre en pratique tout ce que vous avez appris** le plus tôt possible ☺
- Continuer à **discuter et à partager des expériences** avec vos collègues
- Essayons d'**être la nouvelle communauté d'action en gestion responsable des données du secteur**!

Merci de votre attention !
Des dernières questions?

info@cartong.org

www.cartong.org

cartong