Responsible data management training cycle

Session 5
Stakes of the day, and how they apply to you

Introduction to the final session

And now...

1/ The different dimensions of responsible data management

2/ Focus on data protection

3/ The concepts of responsible data management in action- part 1

4/ The concepts of responsible data management in action- part 2

5/ Discover how current stakes apply to you

cartong

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Session 5 agenda

- Introduction to today's session
- Pitch on 4 stakes

- Group work on the stakes
- Wrapping up the training
  - Group work on learnings
  - Satisfaction survey
  - Next steps / Conclusion

The development of this training material is supported by the French Ministry of Europe and Foreign Affairs (MEAE-CDCS). Nevertheless, the ideas and opinions presented in this training do not necessarily represent those of MEAE-CDCS.

The 4 stakes

Introducing our speakers

CyberPeace Institute

Alexandru Lazar – Program Officer for the CyberPeace Builders program
Zacharia Okere - Non-Profit Cybersecurity Specialist, based in Nairobi

The CyberPeace Institute is a Geneva based organization protecting the most vulnerable in cyberspace. Independent and neutral, the Institute investigates and analyzes the human impact of systemic cyber threats, delivers free cybersecurity assistance, tracks the enforcement of international laws and norms and forecasts threats to Cyberpeace

The Engine room

Quito Tsui – Associate, Reasearch and Learning Team
Helen Kilbey – Editorial Manager

The Engine room is a non-profit organisation with a distributed global team of experienced and committed activists, researchers, technologists and community organisers. It's a committed team that strengthens the fight for social justice by supporting civil society to use technology and data in strategic, effective and responsible ways

Quiz

Cybersecurity


cyber
peace
builders.
CyberPeace
Institute
ASSISTANCE | ANALYSIS | ADVANCEMENT

cartong


CyberPeace
Institute
UNDERSTANDING CYBER
THREATS FACED BY NGOS
cyber
peace
builders

SECURITY AWARENESS: FOCUS ON THE HUMAN FACTOR

HTTPS://WWW.YOUTUBE.COM/WATCH?V=UD-5LPULDNM

CyberPeace Institute

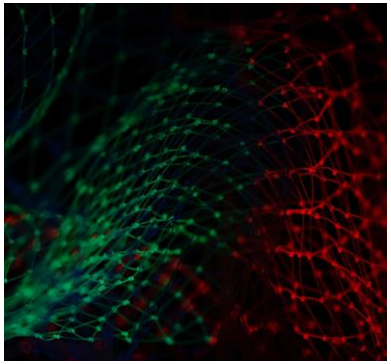
DIFFERENT ACTORS AND THEIR INTERESTS

Hacktivists

- ✓ World-famous organisations can be seen as a trophy
- ✓ Attacks can be carried out by chance or by mistake

Criminal groups

- ✓ International organization, high profile organization may appear rich…
- ➢ Financial gain



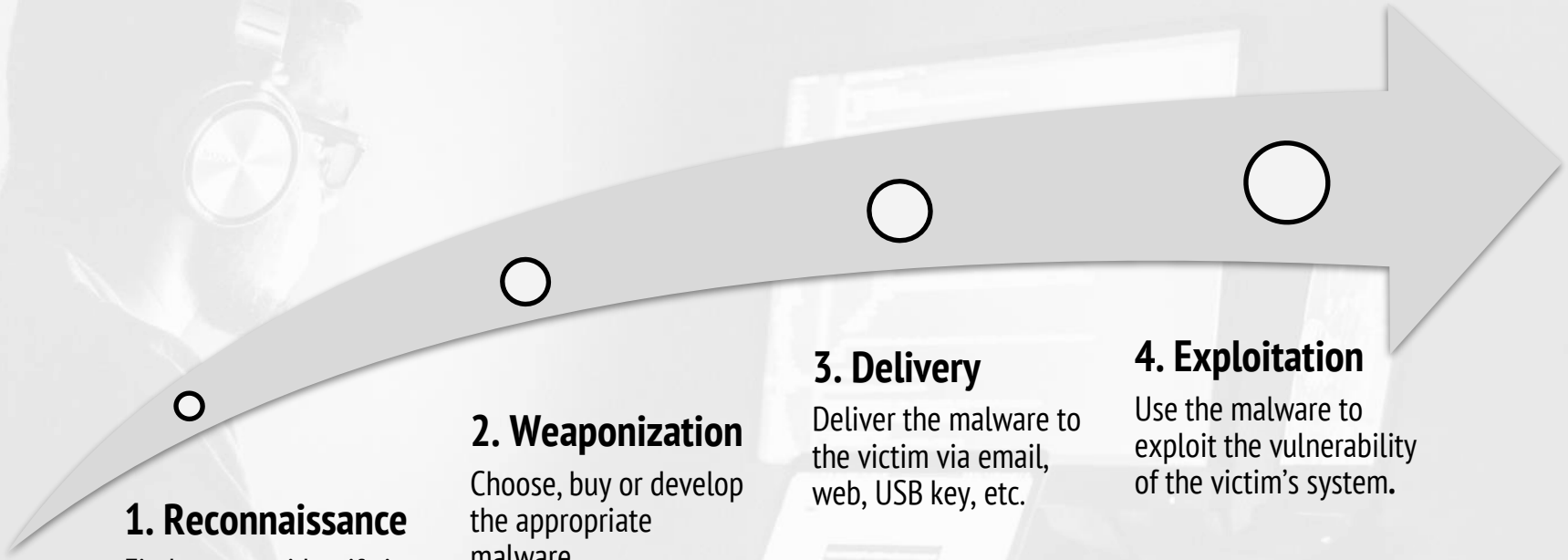
States & State-sponsored groups

- ✓ Organizations or individuals own sensitive information
- ✓ Activities could be considered as disturbing
- ➢ Espionage, sabotage

cyber peace builders.

cartong

CYBER THREATS - THE CYBER KILL CHAIN SIMPLIFIED



1. Reconnaissance

Find a target, identify its weak spot and plan the attack, maybe using social engineering.

2. Weaponization

Choose, buy or develop the appropriate malware.

3. Delivery

Deliver the malware to the victim via email, web, USB key, etc.

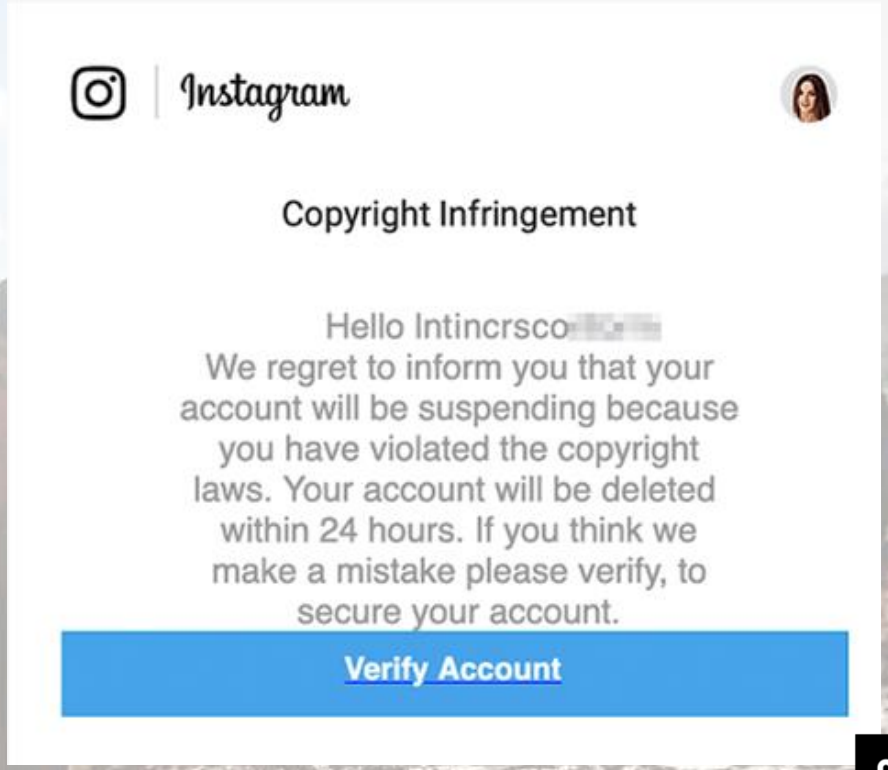
4. Exploitation

Use the malware to exploit the vulnerability of the victim's system.

CyberPeace Institute

SOCIAL MEDIA

What happens when you lose access to one of your organization's social media account?



More information:
https://cyberpeaceinstitute.org/news/testimonial-uicc/

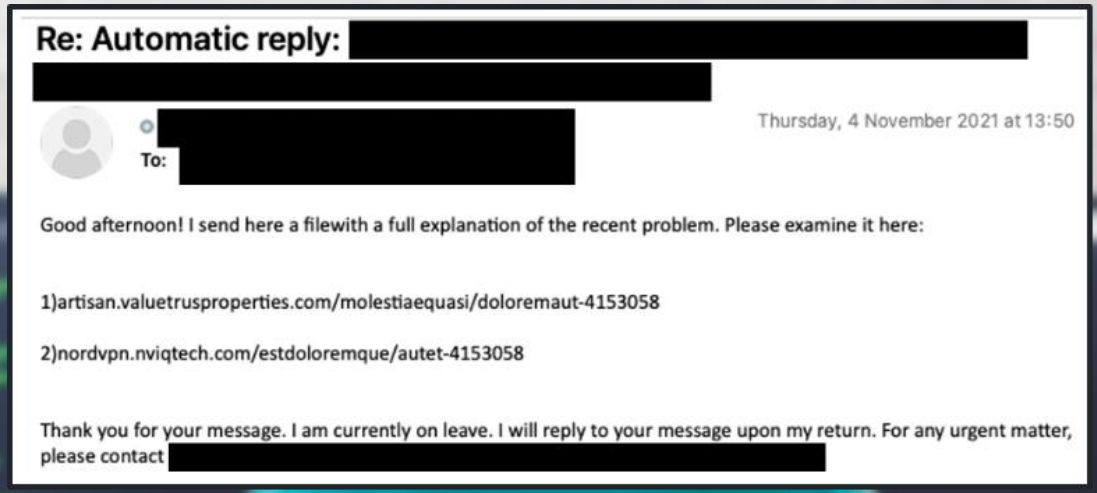
cyber peace builders

cartong

CyberPeace Institute

COMPROMISED EMAILS

And if your partners no longer trust you?



More information:
https://cyberpeaceinstitute.org/news/ngos-caught-in-the-net/

cyber peace builders.

cartong

CyberPeace Institute

HELPING NGOS UNDERSTAND CYBER RISKS

85%

of NGO think that their staff pose an important risk in terms of cybersecurity, yet only **55 %** of them deliver regular cybersecurity awareness sessions

1. Start by a standard cybersecurity assessment
2. Identify your critical functions
3. Determine who could pose a threat to your NGO
4. Identify your vulnerabilities

cyber peace builders.

cartong

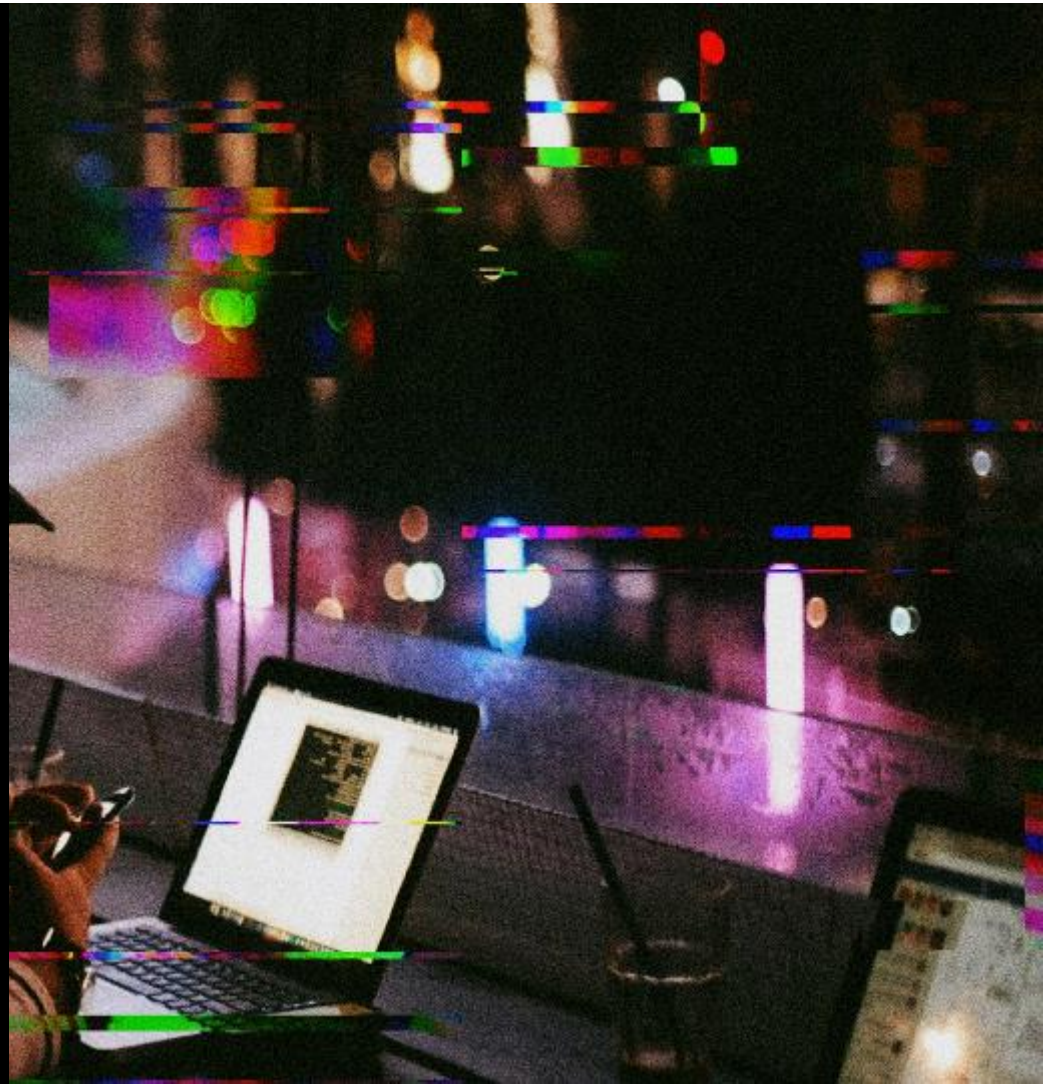
CyberPeace Institute

cyber peace builders.

THANK YOU

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

CyberpeaceInstitute
@CyberpeaceInst
The CyberPeace Institute



Disinformation / Misinformation

Disinformation / Misinformation

What it is:

These phenomena are information relaying perceptions that don't reflect reality - substantial and cross-cutting impacts.

Misinformation refers to false information that is not intended to cause harm
Whereas *disinformation* refers to false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction
Hate speech 'contributes directly or indirectly to endangering civilian populations' safety or dignity' (ICRC)

The stakes:

- **Accelerating phenomena** due to massive spread via technologies
- Misinformation **spreads faster than the truth**
- Can entail **loss of confidence of communities**, exacerbated in situations of fear and uncertainty
- Impact on **capacities of NGOs** to deploy activities
- It is harmful for people: increasing « risks and vulnerabilities » (ICRC)

Further reading:

- ICRC: Q&A on misinformation, disinformation and hate speech consequences in the humanitarian sector & podcast on misinformation and humanitarian action
- Cyberpeace Institute: ChatGPT and the health crisis related to Covid 19
- Canadian centre for cybersecurity: how to identify misinformation, disinformation and malinformation
- Internews: managing misinformation in a humanitarian context report
- ICTworks: 7 recommendations & How to Address Disinformation in Eastern and Central Europe
- The Newsguard: Article on massive disinformation
- Manchesterhive: article on 'Humanitarian Communication in a Post-Truth World'
- Oxfam and the Engine Room: Example on misinformation spreading within camps

An example: ICRC in Burkina Faso

An independent journalistic consortium revealed in February 2023 that the **ICRC** had been the target of a **disinformation campaign** in Burkina Faso : false information, fabricated by a specialized private company, which had been used on behalf of politicians.

Consequences:

- the **"neutrality"** of the ICRC was criticized
- Violent comments raised **fears for the safety** of the local team
- ICRC had to issue **a statement to contradict the information**.

Source: the voice of Africa


How misinformation and disinformation harm ICRC's humanitarian work in 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: the ICRC

What can you do to tackle these phenomena?

Recommandations, when possible:

- For the comm's teams to **invest time & research** about how your NGO is perceived and what the disinformation trends are
- To **build trustful relations** with the communities you are working with and key stakeholders
- To have **quality program data**, shared and accepted by the communities: responsibility of MEAL teams To « commit to **accurate reporting and campaigning** » and include it into your communication strategy

  These 2 last points refer to the **transparency and accountability** principles

Source: ICRC - manchesterhive

Biometrics

THE ENGINE ROOM

Biometrics

A closer look at risks and benefits

How are biometrics used?

- Identification and verification purposes as part of humanitarian operations
- Foundational and functional systems
- Biometric technologies capture key aspects of a biometric sample in a biometric template

Why is biometric information sensitive?

- ❏ Uniqueness and immutability
- ❏ Richness of information
- ❏ Flexibility of use

A closer look at benefits

- Anticipated benefits associated with biometric systems have not changed significantly since 2018.
- Potential benefits include: improving the process of aid distribution due to greater registration efficiency; traceability, de-duplication and fraud control; increased accuracy of data and as an anti-corruption tool, economic benefits to individuals and humanitarian organisations
- However, evidence for these benefits often comes from case studies outside the humanitarian sector, and do not fully account for potential context specific limitations

A closer look at harms

+ New evidence of biometric systems as both the cause and amplifier of risk and harm.
+ Risks spanning the entire lifecycle of biometric systems include the challenges of risk mitigation, concerns about data security and harm to impacted communities, surveillance and the misuse of data as well as the possibility of function creep
+ Biometrics amplifies broader data sharing concerns regarding vendor lock-in, third-party differences in data governance, technical limitations regarding data protection, and opaquely governed data sharing

Case studies of harm

Case study: Non-consensual data sharing of Rohingya refugees in Bangladesh
Refugees in Bangladesh had their biometric information processed through a joint verification exercise between the Bangladeshi Government and the UNHCR as part of a process intended to preserve their right to voluntary return and furnish them with an individual identity document. Biometric data in the form of thumbprints on paper documents were then shared by the Bangladeshi government with the Myanmar authorities as part of right to return efforts. Many refugees, however, did not know that this information would be shared by the Bangladeshi government with Myanmar authorities to potentially facilitate repatriation.

Case study: Double registration in Kenya
Double registration of Somali Kenyan nationals in both refugee and national databases led to double registered Somali Kenyans being unable to access their citizenship rights.The estimated 40,000 Kenyan citizens registered in the refugee database – the majority of whom are below the age of 40, many having had their data captured when they were children – were rendered de facto stateless.

Case study: WFP and Houthi standoff in Yemen
Following allegations that Houthi operatives had been interfering in the delivery of food aid, the WFP sought to introduce a biometric system. However the Houthi leadership sought access to this biometric information as a condition of implementation. Disagreement over access led to a partial aid suspension in June 2019, before coming to an agreement with the Houthis a few months later. The deal emphasised the need for total transparency in aid beneficiary registration and included a biometric database, with the information stored on a joint server housed in Yemen that is not connected to the internet.

Charting a path to responsible biometric policies

1. Continued interrogation of the necessity of biometrics

+ How do we think about necessity in the context of biometrics?
+ Are biometric technologies the only option for addressing a given challenge?
+ How can humanitarian practitioners create space for alternative solutions?
+ How do we resist path dependency?
+ What steps can be codified to ensure that real need drives the adoption of biometrics?

2. More nuanced policy design and implementation

+ Who is considered in the policy design and implementation process?
+ Are our policies accessible?
+ Can our policies be implemented?
+ How do we create space for feedback and engage with criticism?
+ In what ways do staffing processes e.g high turnover, short-term contracts, impact how we design and implement policies?

3. Establishing community-centred standards of practice

+ Are similar and/or partnered organisations operating on a shared framework of understanding?
+ How do we create coherency in the sector with regards to the use of biometrics?

4. Strengthening practices around Data Protection Impact Assessments (DPIAs)

+ How do we ensure that DPIAs are understood by all stakeholders?
+ How do we develop sufficiently detailed DPIAs?
+ How do we maintain DPIAs and mitigate new risks after the initial assessment and during a project's lifecycle?

5. More sophisticated ecosystem-wide analysis of technology

- What ways of thinking are driving decision-making?
- How do we acknowledge the resource constrained environments of humanitarian contexts, while avoiding an over reliance on technological solutions?
- What is the appropriate role of private sector actors that do not explicitly adhere to humanitarian principles?

Artificial intelligence

Artificial Intelligence

What is it?

"Artificial intelligence (AI) refers to the **series of techniques which allow a machine to simulate human learning**, namely to learn, predict, make decisions and perceive its surroundings. In the case of a computing system, artificial intelligence is applied to digital data."
(Montreal Declaration)

Machine Learning: An extension to AI. Capability for **prediction or decision** based on data.

Generative AI is a type of AI system **capable of generating text, images or other media** in response to prompts.

There is no such thing a « global AI » but rather a **diversity of specialised AI**

Further reading:

- 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
- AI ethics: 5 considerations for nonprofits: https://nethope.org/articles/ai-ethics-5-reasons-why-nonprofit-engagement-is-key/

Artificial Intelligence

Topics of interest

- Medical diagnosis
- Predictive crisis analysis
- Predicting population movement
- Context evolution analysis
- Data processing and analysis
- (internal) Fraud detections
- Detecting threat
- Remote sensing technology
- Agricultural productivity
- Analytics for food and food security
- Translation or production or synthesis of documents

Artificial Intelligence

The more things change, the more they stay the same

- The “Do not harm” principle must prevail above all
- Responsible Data Management principles remain relevant
- Data is rarely neutral, and prejudice is omnipresent
- There is a need and responsibility for risk assessment
- Focus on people and skills rather than tools, systems and the latest 'innovations' and gadgets
- Over-reliance on AI systems could contribute to the reproduction of structural inequalities and inequalities embedded in datasets.
- Big Tech is the main force shaping the trajectory of research and the political and popular conversation around AI.

Artificial Intelligence: Keep in mind

AI Ethical Principles

(ICT works)

- Fairness
- Human agency and oversight
- Privacy and security
- Safety and robustness
- Transparency and explainability
- Accountability
- Environmental impact

Inevitability does not mean we have accept as is. Humanitarians must adapt and participate to the discussions and debates on the direction that AI may take in the sector by influencing current developments.

The regulations around AI remain vague, insufficient and fragmented.

It is important to continue to raise awareness on data protection (which is already difficult topic to grasp).

Focus first on the problem you need to address and solve, then on the data and AI tools you need to help you change what you do in the field

- What assumptions need to be verified?
- How can we determine responsibility when errors occur?
- How can we make these tools our own and adapt them to the local context?
- What are the needs and issues in the field?

Let's get down to group work!

Group discussion !

You will be expected for the case study you are on to **list the challenges,and measures to take/that you should have taken**

Group numbers:

- 1/ Cybersecurity
- 2/ Disinformation & misinformation
- 3/ Biometrics
- 4/ Artificial intelligence

Restitution

Questions & Answers

Do you have questions for our speakers? Or testimonies you would like to share?

Break

Wrapping up

What did you learn from the training and what will you do with it? Group work

Satisfaction survey: please take 5-10 minutes to fill it!

If you need further support...

Want extra support?

If you are **interested in a consultancy with CartONG** to support you in

- capacity building (trainings, coaching, hotline – you name it)
- implementing tools and approaches related to program data

… here's our portfolio

Get in touch with your focal points (as we have partnership agreements with many of your organisations and/or Maeve (m_defrance@cartong.org) if you **want to discuss further**!

And remember- the go-to resources

Available on https://www.im-portal.org/learning-corner

The responsible data resource list we compiled for you!

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://merl	2022
CMS - GDPR Fines		GDPR Enforcement Tracker	Tutorial / Tips / Tool	https://www	
OXFAM		Biometric and Foundational Identity Policy	Policy	https://oxfa	2021
Responsible Data		Responsible Data website	Website	https://resp	
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 Series (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

Homework

- Make sure you **practice everything you have learned** sooner rather than later

- Continue **discussing and sharing experiences** with your colleagues

- Let's try and **be the new responsible data in action community**!

Thank you for your attention!

info@cartong.org

www.cartong.org