

Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

3.1.1 Digital Risks as Protection Risks to Civilians in Conflict

Concepts (extracted from automatically generated subtitles):

Digital risk advisor. Protection risks. Digital risks. Digitalisation of other situations of violence. Armed actors. Different ways. Use of icts. Situations of armed conflict. Protection work today. Digital tools. Using such tools. Harmful effects. Spread of harmful information. Actors' behaviour. Cyber operations.



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

STAKES FOR PEOPLE IN HUMANITARIANS CRISES

Digital Risks as Protection Risks to Civilians in Conflict

Joelle Rizk

Digital Risk Adviser

International Committee of the Red Cross (ICRC)

...

notes

summary

0m 0s



STAKES FOR PEOPLE IN HUMANITARIANS CRISES

Digital Risks as Protection Risks to Civilians in Conflict

Joelle Rizk

Digital Risk Adviser

International Committee of the Red Cross (ICRC)



Hello, my name is Joelle Rizk.

notes

summary

0m 10s



Digital Risks as Protection Risks to Civilians in Conflict



Joelle Rizk

Digital Risk Adviser

International Committee of the Red Cross (ICRC)



I am the Digital Risk Adviser at the International Committee of the Red Cross. Today, I will be with you for Module 3 to introduce digital risks as protection risks to civilians in situations of armed conflict.

notes

summary

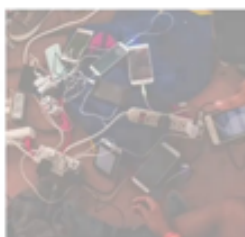
0m 13s



The Emergence of Digital Risks



Digitalization of
armed conflict and
other situations of
violence.



Connectedness of
affected populations.



The digital
transformation of
humanitarian action.

What are protection risks and digital risks to civilians affected by situations of armed conflict? There are a few factors that we need to understand when thinking of digital risks to civilians.

notes

summary

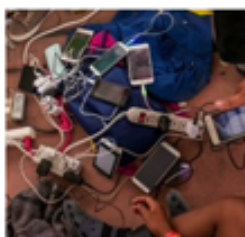
0m 29s



The Emergence of Digital Risks



Digitalization of
armed conflict and
other situations of
violence.



Connectedness of
affected populations.



The digital
transformation of
humanitarian action.

Primarily, it's the digitalisation of armed conflicts in today's digital age and the digitalisation of other situations of violence. In other words, it's also about the use of ICTs by states and non-state armed actors and other stakeholders in situations of conflict or other situations of violence. A second factor to keep in mind is that people affected by armed conflict and other situations of violence are also themselves relying on connectivity and connectedness to different forms of ICTs for accessing essential services and for the functioning of society.

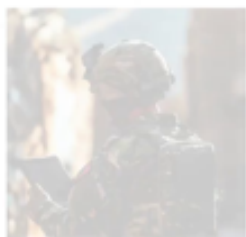
notes

summary

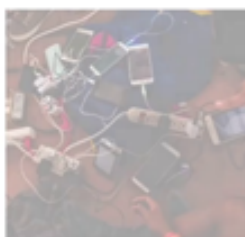
0m 45s



The Emergence of Digital Risks



Digitalization of
armed conflict and
other situations of
violence.



Connectedness of
affected populations.



The digital
transformation of
humanitarian action.

The third factor to keep in mind and that is the delivery of humanitarian

notes

summary

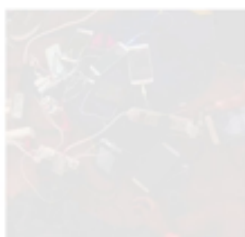
1m 24s



The Emergence of Digital Risks



Digitalization of
armed conflict and
other situations of
violence.



Connectedness of
affected populations.



The digital
transformation of
humanitarian action.

and protection work today is either mediated or assisted through digital tools or by digital tools. These three factors combined change the landscape in which protection work is delivered. They are to keep in mind as we go through this module.

notes

summary

1m 25s



Protection Work in the Digital Age

Protecting the rights of people when they are restricted or affected in the digital sphere, or because of actors' behaviors in that space and their use of ICT in conflict.

When we speak of protection in the digital age or protection work in the digital age, we are speaking of protecting the rights of people when they are restricted or affected in the digital sphere, or because of actors' behaviour in that space

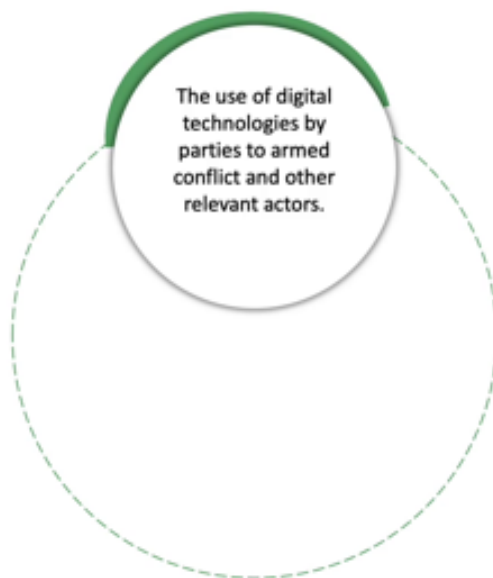
notes

summary

1m 47s



How these Risks are Enabled



and their use of ICTs in conflict. Protection digital risks are usually enabled in 3 different ways. First, the use of digital technologies or ICTs by states and non-state actors in situations of armed conflict or violence in ways that may lead to harmful effects on civilians.

notes

summary

2m 7s



How these Risks are Enabled



That includes the behaviour of states and non-state actors and other stakeholders.

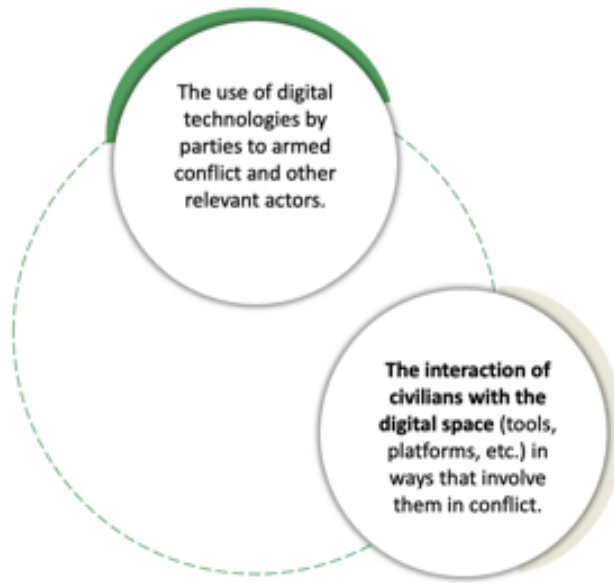
notes

summary

2m 30s



How these Risks are Enabled



Second, it's in the way in which civilians themselves are interacting with the digital space through tools that they use or rely on to access services or assistance or through the platforms that they use: digital platforms, applications, messaging apps, etc. Civilians may end up using such tools or such digital tools in ways that involve them in conflict or bring them closer to the digital front lines of conflict either through the spread of harmful information, through information gathering or through cyber operations in being involved or becoming part of the delivery of cyber operations or other examples.

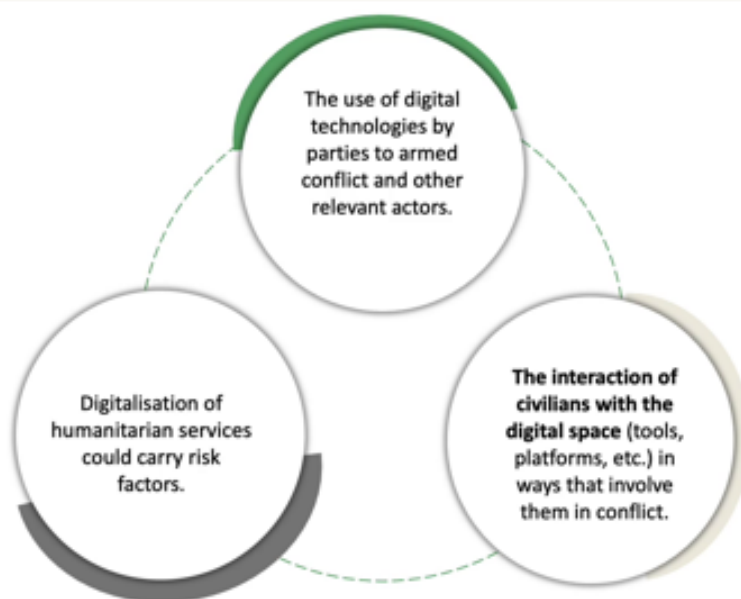
notes

summary

2m 38s



How these Risks are Enabled



Third, it is also about the use of digital technologies or ICTs by humanitarian actors themselves in ways that may amplify risk factors and vulnerabilities of people.

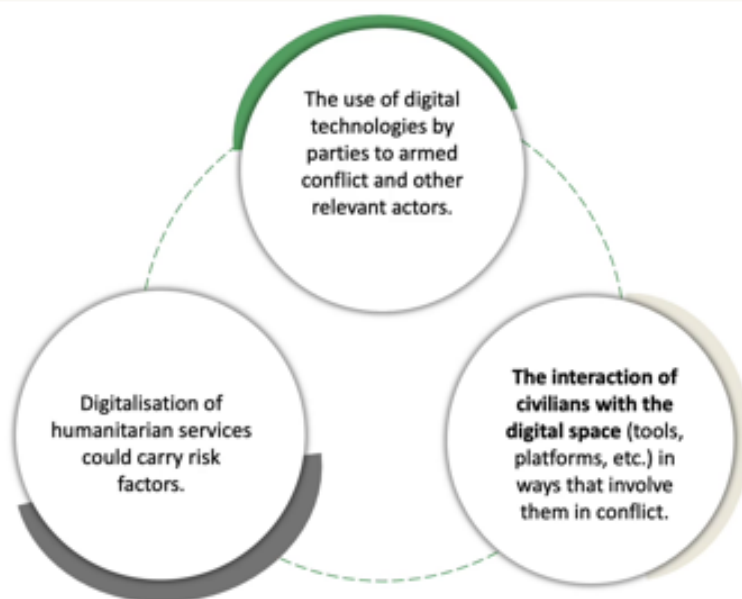
notes

summary

3m 21s



How these Risks are Enabled



In other words, in situations where protection

notes

summary

3m 36s



Examples



The use of digital interception tools to monitor communication might lead to harmful acts.



The spread of harmful information online may encourage violence against certain populations, may lead to persecution, violence, or extrajudicial killing.



Connectivity restrictions may prevent people from connecting with their loved ones or from obtaining information necessary for their safety.



The disruption of critical infrastructure with a cyber operation may lead to physical harm or economic hardship.

and humanitarian actors may become themselves the vectors of harm towards civilians. To be more concrete, I'll give you a couple of examples.

notes

summary

3m 37s



Examples



The use of digital interception tools to monitor communication might lead to harmful acts.



The spread of harmful information online may encourage violence against certain populations, may lead to persecution, violence, or extrajudicial killing.



Connectivity restrictions may prevent people from connecting with their loved ones or from obtaining information necessary for their safety.



The disruption of critical infrastructure with a cyber operation may lead to physical harm or economic hardship.

For example, the use of digital interception tools

notes

summary

3m 49s



Examples



The use of digital interception tools to monitor communication might lead to harmful acts.



The spread of harmful information online may encourage violence against certain populations, may lead to persecution, violence, or extrajudicial killing.



Connectivity restrictions may prevent people from connecting with their loved ones or from obtaining information necessary for their safety.



The disruption of critical infrastructure with a cyber operation may lead to physical harm or economic hardship.

to monitor digital communication of affected people in ways that enable harmful acts such as arbitrary arrests, disappearances, targeted killing, etc. Another example.

notes

summary

3m 50s



Examples



The use of digital interception tools to monitor communication might lead to harmful acts.



The spread of harmful information online may encourage violence against certain populations, may lead to persecution, violence, or extrajudicial killing.



Connectivity restrictions may prevent people from connecting with their loved ones or from obtaining information necessary for their safety.



The disruption of critical infrastructure with a cyber operation may lead to physical harm or economic hardship.

The disruption of critical infrastructure or essential infrastructure with cyber operations or through cyber operations that may lead to physical harm or economic harm of people. We will hear more about this in Module 6: Humanitarian consequences of cyber operations.

notes

summary

4m 7s



Examples



The use of digital interception tools to monitor communication might lead to harmful acts.



The spread of harmful information online may encourage violence against certain populations, may lead to persecution, violence, or extrajudicial killing.



Connectivity restrictions may prevent people from connecting with their loved ones or from obtaining information necessary for their safety.



The disruption of critical infrastructure with a cyber operation may lead to physical harm or economic hardship.

Another example is the spread of hate speech or other forms of harmful information online calling for violence against certain populations, for example, such as minority groups in ways that may lead to persecution, violence or extrajudicial killing or the incitement or encouragement of committing violations of international humanitarian law.

notes

summary

4m 28s



Examples



The use of digital interception tools to monitor communication might lead to harmful acts.



The spread of harmful information online may encourage violence against certain populations, may lead to persecution, violence, or extrajudicial killing.



Connectivity restrictions may prevent people from connecting with their loved ones or from obtaining information necessary for their safety.



The disruption of critical infrastructure with a cyber operation may lead to physical harm or economic hardship.

We will hear more about this in the next video on harmful information following this session. A final example is restrictions on connectivity and telecommunication, such as internet shutdowns and communication blackouts in ways that may amplify family separation or other safety concerns of those that are unable to verify information, for example, about safe zones or humanitarian corridors.

notes

summary

4m 49s



Risks to Civilians



We see that digital risks to civilians could be a combination of information-related risks, cyber-related risks and data-related risks.

notes

summary

5m 16s



Different Types of Risks to Civilians



Information related

- Misinformation.
- Disinformation.
- Malinformation.
- Hate Speech.
- Other form of harmful information online.
- Denial of connectivity, shutdowns, blackout.

More concretely, examples of information-related risks include the spread of misinformation, disinformation, malinformation, hate speech, or other forms of harmful information online. At the same time, restrictions on connectivity such as shutdowns or communication blackouts.

notes

summary

5m 29s



Different Types of Risks to Civilians



Information related

- Misinformation.
- Disinformation.
- Malinformation.
- Hate Speech.
- Other form of harmful information online.
- Denial of connectivity, shutdowns, blackout.



Cyber related

- Cyber attacks targeting civilians.
- Cyber attacks targeting infrastructure.
- Cyber attacks targeting humanitarian organizations.

Examples of cyber-related risks may include cyberattacks that target civilians or infrastructure important for the functioning of society

notes

summary

5m 49s



Different Types of Risks to Civilians



Information related

- Misinformation.
- Disinformation.
- Malinformation.
- Hate Speech.
- Other form of harmful information online.
- Denial of connectivity, shutdowns, blackout.



Cyber related

- Cyber attacks targeting civilians.
- Cyber attacks targeting infrastructure.
- Cyber attacks targeting humanitarian organizations.



Data related

- Data misuse/mishandling.
- Digital surveillance.
- Harmful effects of AI/Automation.

or cyberattacks targeting humanitarian organisations. Examples of data-related risks may include different forms of data misuse or mishandling and digital surveillance.

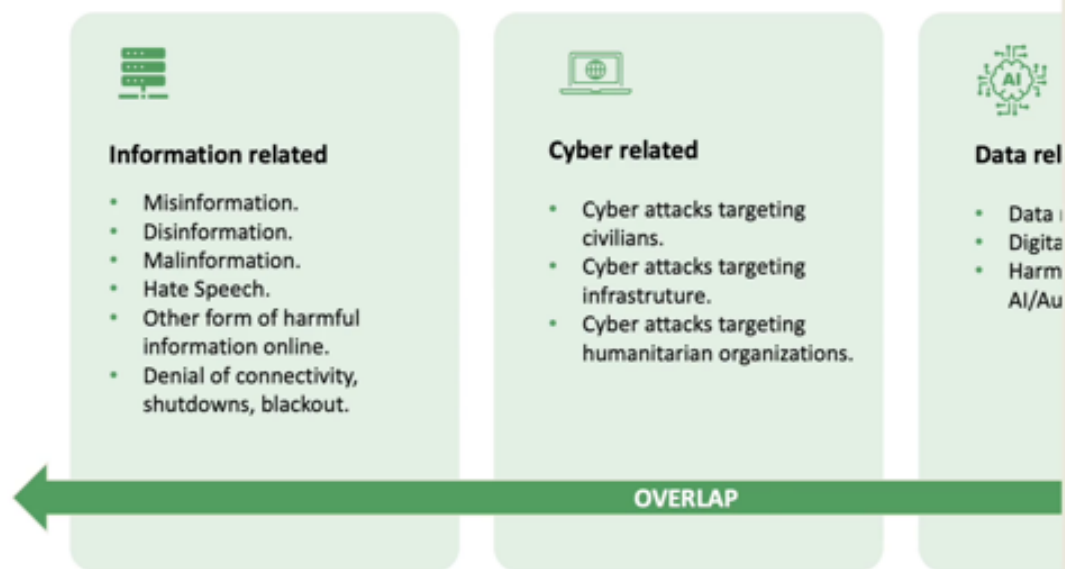
notes

summary

6m 1s



Different Types of Risks to Civilians



In reality, all 3 sources of risks, whether information-related, cyber-related or data-related, may overlap.

notes

summary

6m 13s



Digital Risks as Protection Risks



Protection risks that are enabled by the use of digital technologies and might have consequences for the rights, safety and dignity of affected populations in situations of armed conflict and other situations of violence.

When speaking of protection risks, protection actors understand risk as a combination of a threat and its interaction with the vulnerability of affected people and their capacity to address or mitigate that threat and its impact. When aiming at reducing a risk, protection actors will try to reduce the threat and/or reduce the vulnerability of affected people and improve their capacity for self-protection, or mitigating the impact of that threat. This applies as well to digital risks that are enabled by digital technologies and might have consequences for the rights, safety and dignity of affected populations.

notes

summary

6m 21s



Digital Risks as Protection Risks



Protection response to digital risks

- Identify and understand digital risks.
- Integrate digital risks in protection strategies.
- Address the capacity of duty bearers to meet their obligations.

Protection risks that are enabled by the use of digital technologies and might have consequences for the rights, safety and dignity of affected populations in situations of armed conflict and other situations of violence.

- Prevent foreseeable negative impacts and encourage preventive or protective measures.
- Reinforce self protection capacities and resilience of affected individuals and communities.

Keeping that in mind, what are protection responses?

notes


summary

.....

.....

.....

7m 12s





Protection response to digital risks

- **Identify and understand digital risks.**
- **Integrate digital risks in protection strategies.**
- **Address the capacity of duty bearers to meet their obligations.**
- **Prevent foreseeable negative impacts and encourage preventive or protective measures.**
- **Reinforce self protection capacities and resilience of affected individuals and communities.**

What should protection actor keep in mind when delivering protection responses to digital risks? We've established already that the use of digital technologies and the use of ICTs by states and non-state actors can, in fact, lead to harmful effects for people affected by armed conflict and violence. Protection action, as we have just seen, should therefore be informed and be relevant and adequate to the right threat or the risk and to identify the vulnerability of people and their capacity. To recap, protection workers

notes

summary

7m 13s





Protection response to digital risks

- **Identify and understand digital risks.**
- **Integrate digital risks in protection strategies.**
- Address the capacity of duty bearers to meet their obligations.
- Prevent foreseeable negative impacts and encourage preventive or protective measures.
- Reinforce self protection capacities and resilience of affected individuals and communities.

must therefore identify and understand digital risks and integrate digital dimensions in their documentation and protection analysis to guide their protection strategies.

notes

summary

7m 55s





Protection response to digital risks

- **Identify and understand digital risks.**
- **Integrate digital risks in protection strategies.**
- **Address the capacity of duty bearers to meet their obligations.**
- Prevent foreseeable negative impacts and encourage preventive or protective measures.
- Reinforce self protection capacities and resilience of affected individuals and communities.

For example, protection actors may work to address the capacity of duty bearers to meet their obligations while achieving other protection outcomes.

notes

summary

8m 9s





Protection response to digital risks

- Identify and understand digital risks.
- Integrate digital risks in protection strategies.
- Address the capacity of duty bearers to meet their obligations.
- Prevent foreseeable negative impacts and encourage preventive or protective measures.
- Reinforce self protection capacities and resilience of affected individuals and communities.

Other activities could aim at preventing foreseeable negative impact or encourage preventive measures by duty bearers. On another front, protection actors should reinforce the self-protection capacities and resilience of affected individuals and communities

notes

summary

8m 18s



Challenges

Difficulty to understand the behaviors and specific acts that may cause harm.

How to meaningfully document and gather evidence to inform protection strategies?

How to properly attribute acts and understand the responsibility of actors?

in relation to digital risks. To do so effectively, there remains a lot of challenges.

notes

summary

8m 37s



Challenges

Difficulty to understand the behaviors and specific acts that may cause harm.

How to meaningfully document and gather evidence to inform protection strategies?

How to properly attribute acts and understand the responsibility of actors?

To name a few challenges, first, understanding of the risk and the behaviour and defining specific acts that may cause harm remains a challenge for protection actors and more work is still needed to better understand how these behaviours or what are the specific acts in the digital space or by using ICTs and digital technologies that may have harmful effects on people affected by armed conflict and other situations of violence.

notes

summary

8m 49s



Challenges

Difficulty to understand the behaviors and specific acts that may cause harm.

How to meaningfully document and gather evidence to inform protection strategies?

How to properly attribute acts and understand the responsibility of actors?

Second, the documentation of such events and incidents in ways that provide

notes

summary

9m 17s



Challenges

Difficulty to understand the behaviors and specific acts that may cause harm.

How to meaningfully document and gather evidence to inform protection strategies?

How to properly attribute acts and understand the responsibility of actors?

relevant evidence and preserve such evidence even outside accountability, even for the purpose of informing protection action and informing protection strategies.

notes

summary

9m 26s



Image Reference



In order of appearance

PICTURE1 : robin-worrall-FPT10LXK0cg-unsplash
PICTURE2 : World humanitarian by xartproduction from Adobe Stock
ICON1 : Created by Sharon Showalter from Noum Project
ICON2 : Created by Chalwat Kinkaew from Noum Project
ICON3 : Created by IconField from Noum Project
ICON4 : Created by Good Wife from Noum Project
PICTURE3 : Civilians from Adobe Stock
PICTURE4 : By Mvproductions from Adobe Stock
PICTURE5 : Photo provided by ICRC
PICTURE6 : Photo provided by ICRC
ICON1 : Created by Icons Field from Noum Project
ICON2 : Created by M. Faisal from Noum Project
ICON3 : Created by Adrien Coquet Pumomo from Noum Project
ICON4 : Created by Atif Arshad from Noum Project
PICTURE7 : Photo provided by ICRC
PICTURE8 : Risk Management by janews094 from Adobe Stock
PICTURE9 : bussiness prevent falling by Passion from Adobe Stock

A third challenge to keep in mind is attribution of acts and understanding the responsibility of actors for the purpose of designing relevant protection action remains a challenge. We hope that this was a good introduction to identifying digital risk that may be harmful to people affected by conflict and other situations of violence.

notes

summary

9m 37s