



Course material

Course:

## Understanding the digital supply chain and its stakes for humanitarian actors

Video:

### 4.3 Humanitarian considerations on cyber conflict

Concepts (extracted from automatically generated subtitles):

**Cyber policy. Humanitarian settings. Cyber operations. Harm civilians. Cyber threat actors. Cyber conflicts. Sensitive data. Specific civilian infrastructure. Destructive effects. Digital threats. Humanitarian considerations. Hacktivist groups. Humanitarian crisis. Important actors. Vulnerable populations.**



[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/>



# CYBERSECURITY

LANDSCAPE OF CYBERTHREATS AND  
GEOPOLITICAL IMPLICATIONS

## Humanitarian considerations on cyberconflicts

**Sean Cordey**  
Senior Researcher at Center for Security Studies, ETH Zürich / ICRC



...

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....


.....

summary

.....

.....

0m 0s



# Humanitarian Considerations on Cyberconflicts



Welcome. I am Shaun Cordy, a senior researcher at the Centre for Security Studies at ETH Zurich, working on digital threats in humanitarian settings,

notes

---

---

---

---

---

---

---

---

---

---

summary

0m 2s



---

---

---

---

---

## You Will Learn



**Cyberthreats in  
Humanitarian Crises**



**The Humanitarian  
Implications of CyberThreats**



**CyberThreats to Humanitarian  
Actors and Action**

and have previously worked for the ICRC on cyber policy and protection in the digital sphere. In this module, we will focus on humanitarian considerations in cyber conflicts and of cyber operations. We will first look at the cyber threat landscape in humanitarian crisis. Then we will focus on how these threats might impact and harm civilians, as well as look at key humanitarian concerns. Finally, we will address how these cyber threats

notes

summary

0m 13s





# You Will Learn



**Cyberthreats in Humanitarian Crises**



**The Humanitarian Implications of CyberThreats**



**CyberThreats to Humanitarian Actors and Action**

might affect humanitarian organisations themselves

notes

summary

0m 36s



# Humanitarian Considerations on Cyberconflicts



and their ability to operate and assist people in need. With the rise of digitalisation and connectivity across the world, humanitarian crisis today increasingly have a cyber dimension.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

0m 37s



---

---

---

---

---





Increasing number of states have offensive capabilities, that can be used alongside kinetic attacks.

capabilities that are and can be used during armed conflicts and other situations of violence, sometimes in support to in parallel or coordinated with kinetic attacks.

notes

## summary

1m 12s





# Three Key Dynamics of Cyber Threats and Humanitarian Crisis

## State Cyber Capabilities

Increasing number of states have offensive capabilities, that can be used alongside kinetic attacks.

## Opportunistic Actors

APTs and criminals exploit crises.

## Non-State Actors

Hacktivists, companies and cyber mercenaries are increasingly getting involved, further blurring the lines of distinction.

The second dynamic is that opportunistic actors

notes

summary

1m 21s





Increasing number of states have offensive capabilities, that can be used alongside kinetic attacks.

APT's and criminals exploit crises.

leverage humanitarian crisis to advance their interests. APTs are often active and target specific civilian infrastructure, civilians themselves, or even humanitarian organisations. So have cyber criminals, which use the reigning confusion

notes

## summary

1m 25s





# Three Key Dynamics of Cyber Threats and Humanitarian Crisis

## State Cyber Capabilities

Increasing number of states have offensive capabilities, that can be used alongside kinetic attacks.

## Opportunistic Actors

APTs and criminals exploit crises.

## Non-State Actors

Hacktivists, companies and cyber mercenaries are increasingly getting involved, further blurring the lines of distinction.

and information asymmetries to make money. The third dynamic is that non-state actors are becoming important actors in these contexts.

notes

summary

1m 37s







## Three Key Dynamics of Cyber Threats and Humanitarian Crisis

### State Cyber Capabilities

Increasing number of states have offensive capabilities, that can be used alongside kinetic attacks.

### Opportunistic Actors

APTs and criminals exploit crises.

### Non-State Actors

Hacktivists, companies and cyber mercenaries are increasingly getting involved, further blurring the lines of distinction.

Hacktivist groups, for instance, are increasingly taking sides and conducting cyber operations against belligerents or civilian infrastructure. Private companies and cyber mercenaries are also getting involved.

notes

summary

1m 49s





# Types of Cyberthreats in Humanitarian Crises



## Destructive Effects

Example - Wiper malware targeting industrial control systems in critical infrastructure, causing physical damage and disruption to essential services.

## Disruptive Effects

Example - Distributed Denial of Service (DDoS) attacks against financial institutions, hampering access to vital economic resources during crises.

## Influence Effects

Example - Hacking of news broadcasts to spread disinformation, manipulating public opinion and exacerbating social tensions in affected areas.

## Data Weaponization

Example - Deployment of spyware to intercept sensitive information, potentially leading to targeted arrests or persecution of vulnerable individuals.

As per the type of cyber threats observed in these contexts, they can generally be divided into four broad categories those with destructive effects, such as wipers against energy infrastructure,

## notes

## summary

2m 0s



# Types of Cyberthreats in Humanitarian Crises



## Destructive Effects

Example - Wiper malware targeting industrial control systems in critical infrastructure, causing physical damage and disruption to essential services.

## Disruptive Effects

Example - Distributed Denial of Service (DDoS) attacks against financial institutions, hampering access to vital economic resources during crises.

## Influence Effects

Example - Hacking of news broadcasts to spread disinformation, manipulating public opinion and exacerbating social tensions in affected areas.

## Data Weaponization

Example - Deployment of spyware to intercept sensitive information, potentially leading to targeted arrests or persecution of vulnerable individuals.

or those with disruptive effects such as DDoS attacks

notes

summary

2m 12s



# Types of Cyberthreats in Humanitarian Crises



## Destructive Effects

Example - Wiper malware targeting industrial control systems in critical infrastructure, causing physical damage and disruption to essential services.

## Disruptive Effects

Example - Distributed Denial of Service (DDoS) attacks against financial institutions, hampering access to vital economic resources during crises.

## Influence Effects

Example - Hacking of news broadcasts to spread disinformation, manipulating public opinion and exacerbating social tensions in affected areas.

## Data Weaponization

Example - Deployment of spyware to intercept sensitive information, potentially leading to targeted arrests or persecution of vulnerable individuals.

against a banking service. Those with influence effects, such as the hacking of a news broadcast to spread some disinformation or misinformation,

notes

summary

2m 16s





## The Humanitarian Impact of Cyberthreats



Cyber operations can have detrimental effects on the safety, dignity and resilience of people.



May create or exacerbate vulnerabilities and needs.



Wide range of possible harms: physical, psychological, economic, social, cultural, and societal.

and those that collect and weaponize data, such as spyware that intercept sensitive data that can then be used to arrest or target a specific individual. One important point I want to convey is that cyber operations can have detrimental effects on the safety, dignity and resilience of people affected by conflicts and other humanitarian crises.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

2m 25s



---

---

---

---

---



## The Humanitarian Impact of Cyberthreats



Cyber operations can have detrimental effects on the safety, dignity and resilience of people.



May create or exacerbate vulnerabilities and needs.



Wide range of possible harms: physical, psychological, economic, social, cultural, and societal.

They can cause various forms of harms and exacerbate the vulnerabilities, the insecurities and the humanitarian needs of affected populations. For instance, cyber operations have the potential to disable or physically damage

notes

summary

2m 46s





## The Humanitarian Impact of Cyberthreats



Cyber operations can have detrimental effects on the safety, dignity and resilience of people.



May create or exacerbate vulnerabilities and needs.



Wide range of possible harms: physical, psychological, economic, social, cultural, and societal.

a state critical infrastructure in ways that could directly or indirectly cause physical harm, injury, or death to civilians. They can also manipulate the information environment,

notes

summary

2m 58s





## The Humanitarian Impact of Cyberthreats



Cyber operations can have detrimental effects on the safety, dignity and resilience of people.



May create or exacerbate vulnerabilities and needs.



Wide range of possible harms: physical, psychological, economic, social, cultural, and societal.

further fuelling violence or the conflict, as well as cause psychological harm,

notes

summary

3m 10s







## The Humanitarian Impact of Cyberthreats



Cyber operations can have detrimental effects on the safety, dignity and resilience of people.



May create or exacerbate vulnerabilities and needs.



Wide range of possible harms: physical, psychological, economic, social, cultural, and societal.

including fear, anxiety, guilt or anger. Or they can affect the social fabric of societies, undermine the trust and civil institutions, or even create economic disruption and financial harm

notes

summary

3m 14s







notes

summary

3m 25s





notes

3m 37s

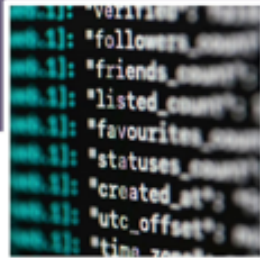


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



There are few specific issues that humanitarians are concerned about, some of which will be developed in more details in the models on humanitarian consequences of cyberattacks.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

3m 41s



---

---

---

---

---

---

---

---

---

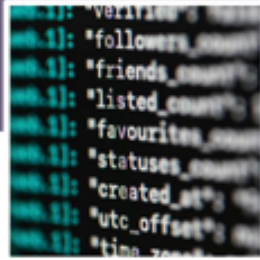
---

# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



Firstly, various actors have developed and showed their ability and willingness to disrupt the provision of essential services to the population,

## notes

## summary

3m 52s

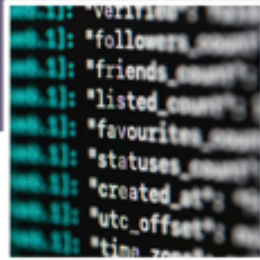


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



including medical, electrical, telecom, water and sanitation facilities. This disruption might impede affected populations ability to access vital information or essential services crucial to their survival during humanitarian crisis. Secondly, personal and humanitarian data can and have been intercepted via cyber

## notes

## summary

4m 2s

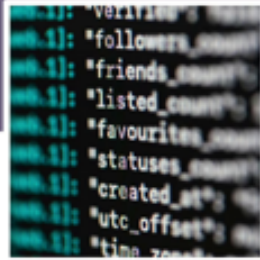


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



and other digital surveillance means. These data can be misused by malicious actors

notes

summary

4m 20s

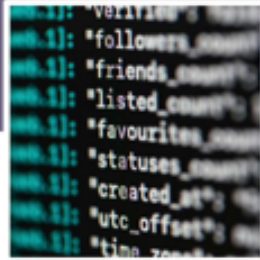


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



to cause or enable other forms of harms and threaten fundamental rights. For instance, arbitrary arrest or targeting, persecutions, detentions, torture or other ill-treatment.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

4m 25s



---

---

---

---

---

---

---

---

---

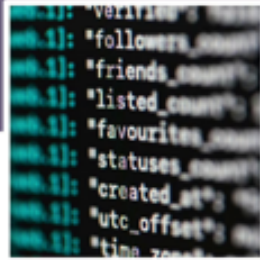
---

# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



Based on this intercepted data,

notes

summary

4m 37s



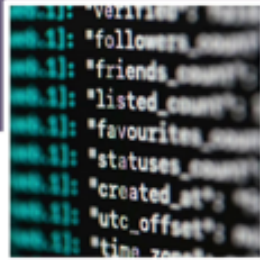


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



## Cyber exploitation and crime

E.g., Online scams in particularly vulnerable contexts can lead to or amplify economic and financial insecurity.



some individuals may also be discriminated against or denied access to essential or humanitarian services. Thirdly, cybercrime can and have targeted vulnerable populations, with scams either targeting them directly or by pretending to be humanitarian organisations.

## notes

## summary

4m 40s

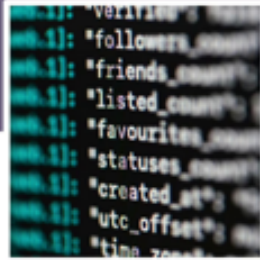


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



## Cyber exploitation and crime

E.g., Online scams in particularly vulnerable contexts can lead to or amplify economic and financial insecurity.



They also target humanitarian actors to defraud them, ransom them or sell their data. These practises can severely affect the livelihood and economic security of vulnerable population,

## notes

## summary

4m 56s



# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



## Cyber exploitation and crime

E.g., Online scams in particularly vulnerable contexts can lead to or amplify economic and financial insecurity.



## Civilian cyber involvement

E.g., Participation in cyber operations can lead to a loss of protection and exposure to different forms of retaliation.

while further affecting the limited resources of humanitarian organisations.

notes

summary

5m 6s

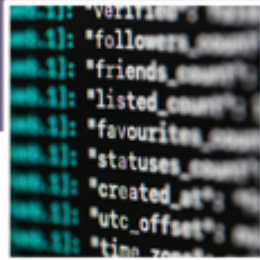


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



## Cyber exploitation and crime

E.g., Online scams in particularly vulnerable contexts can lead to or amplify economic and financial insecurity.



## Civilian cyber involvement

E.g., Participation in cyber operations can lead to a loss of protection and exposure to different forms of retaliation.

Lastly, civilians and private actors across geographical spaces are increasingly getting involved during armed conflicts and other situations of violence via digital tools, whether by providing digital infrastructure services or intelligence to conflict actors,

## notes

## summary

5m 13s

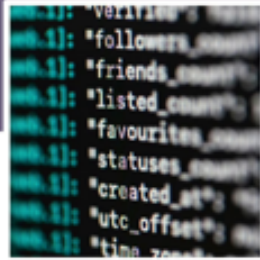


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



## Cyber exploitation and crime

E.g., Online scams in particularly vulnerable contexts can lead to or amplify economic and financial insecurity.



## Civilian cyber involvement

E.g., Participation in cyber operations can lead to a loss of protection and exposure to different forms of retaliation.

either engage in hacktivism. These practises further blur the line between civilians and combatants to the detriment of civilians.

## notes

## summary

5m 25s

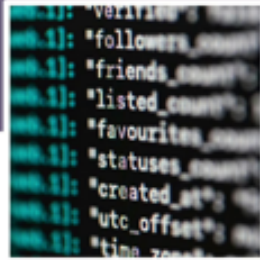


# Specific Humanitarian Concerns



## Disrupting essential and protected infrastructure and services

E.g., Targeting hospitals, telecommunication, energy providers, water systems, financial services can exacerbate/cause significant harm.



## Data misuse and interception

E.g., Compromising sensitive and personal data can enable further malicious targeting, exploitation, and discrimination.



## Cyber exploitation and crime

E.g., Online scams in particularly vulnerable contexts can lead to or amplify economic and financial insecurity.



## Civilian cyber involvement

E.g., Participation in cyber operations can lead to a loss of protection and exposure to different forms of retaliation.

They risk having civilian infrastructure targeted or bring civilians themselves closer to the conduct of military operations, making them at risk of being exposed, targeted, having their property seized or destroyed, be detained or even killed.

## notes

## summary

5m 32s



# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

Finally, humanitarian actors leverage an increasing number of digital tools

notes

summary

5m 48s





# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

and techniques to support and enhance their delivery of their mandate. From data analysis to social media to simple coordination and communication means. They also develop and use digital tools to engage with and support affected populations,

## notes

## summary

5m 52s





# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

such as with digital cash vouchers or chatbots.

notes

summary

6m 10s



# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

But at the same time, this digitalisation and expanded digital presence and service also means that humanitarian organisations and their infrastructure and wider operations can be vulnerable to cyber operations,

### notes

### summary

6m 13s



# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

which can notably affect the confidentiality of their data and work but also affect the availability of the services they provide.

notes

summary

6m 25s



# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

Cyber operations can have reputational and financial repercussions,

notes

summary

6m 34s



# Cyber Threats to Humanitarian Actors and Action



## Humanitarians as Cyber Stakeholder

- Increase reliance on digital infrastructure and data heavy solution for operations.
- Digital proximity and services: engagement with affected people with or via digital means.



## Disrupting Humanitarian Operations

- Compromise ability to deliver humanitarian assistance and protection.
- Affect access, accountability, and communication with communities.



## Compromising Principled Humanitarian Action

- Erode trust in humanitarian actors.
- Impede a Neutral, Impartial, and Independent delivery of Humanitarian action.
- Can enable other forms of harms.

but also impact humanitarian organisations are perceived, trusted and accepted by communities, but also conflict actors. It can affect their access to vulnerable populations and compromise their ability to deliver assistance as well as endanger those they seek to help, but also humanitarian workers themselves.

## notes

## summary

6m 38s





To conclude, questions on how humanitarian organisations should protect themselves against cyber operations will be covered in the module on Leadership in cybersecurity given by Paul Humes.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

6m 54s

