



Course material

Course:

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

Video:

### 6.4 Response Strategies

Concepts (extracted from automatically generated subtitles):

**Humanitarian consequences of cyber operations. Civil society organisations. Digital risks. Last video of a module. Effective data protection policies. Sensitive data. Digital emblem. Potential risks. Next module. Cyber operations. Data protection. Essential services. Important work. Cyber threats. Colleague andrea.**



[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/>

page 1/17

# Key Takeaways



- Critical infrastructure is vulnerable to cyber threats, both outside of conflict zones and during conflicts.
- Cyber attacks on essential services can have wide-ranging and potentially devastating impacts, especially on public health.
- Cyber attacks on humanitarian organizations are increasing, often targeting sensitive data with serious consequences.

Welcome back. In this last video of a module, we'll wrap up our discussion on some of the humanitarian consequences of cyber operations. To start, let's go over some key takeaways from our discussions with Michael and Felipe.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

0m 0s



---

---

---

---

---

# Key Takeaways



- **Critical infrastructure is vulnerable to cyber threats, both outside of conflict zones and during conflicts.**
- Cyber attacks on essential services can have wide-ranging and potentially devastating impacts, especially on public health.
- Cyber attacks on humanitarian organizations are increasing, often targeting sensitive data with serious consequences.

First, although there have been few examples so far of highly sophisticated cyber operations, against essential services in conflict settings. As we heard from Michael, critical civilian infrastructure can be quite vulnerable to cyber threats.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

0m 21s



---

---

---

---

---

# Key Takeaways



- **Critical infrastructure is vulnerable to cyber threats, both outside of conflict zones and during conflicts.**
- **Cyber attacks on essential services can have wide-ranging and potentially devastating impacts, especially on public health.**
- Cyber attacks on humanitarian organizations are increasing, often targeting sensitive data with serious consequences.

In addition, the interdependence of many essential services and the scale of services provided means that the impact of the cyber operation could potentially be devastating, particularly on public health. Outside of conflict zones, essential services are frequently the victims of cyber operations such as ransomware and intrusions. It remains to be seen whether these trends will be replicated at scale in the context of humanitarian crises.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

0m 37s



---

---

---

---

---

---

---

---

---

---

# Key Takeaways



- **Critical infrastructure is vulnerable to cyber threats, both outside of conflict zones and during conflicts.**
- **Cyber attacks on essential services can have wide-ranging and potentially devastating impacts, especially on public health.**
- **Cyber attacks on humanitarian organizations are increasing, often targeting sensitive data with serious consequences.**

Cyber operations against humanitarian and civil society organisations are increasing, and they often target the sensitive data that these organisations hold. With potentially severe consequences for the individuals or communities

notes

summary

1m 9s





# Key Cybersecurity Considerations

**Safety by Design:**  
Prioritize safety by design and strong cybersecurity for critical infrastructure and humanitarian organizations.

**Leadership in Cybersecurity:**  
Humanitarian organizations must better navigate the cyber threat landscape.

**Data Protection:**  
Implement data protection policies to reduce the impact of cyber incidents and ensure proper response.

that the data belongs to. What can humanitarian organisations do to prevent such operations or mitigate their impact? Ideally, of course, the response should be multifaceted and transversal. It's also important to act preemptively whenever possible and try to anticipate potential risks and build resilience within organisations and impacted communities. We've already got some hints in the previous videos about potential responses.

## notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

## summary

.....

.....

.....

.....

.....

1m 25s





## Key Cybersecurity Considerations

**Safety by Design:**  
Prioritize safety by design and strong cybersecurity for critical infrastructure and humanitarian organizations.

**Leadership in Cybersecurity:**  
Humanitarian organizations must better navigate the cyber threat landscape.

**Data Protection:**  
Implement data protection policies to reduce the impact of cyber incidents and ensure proper response.

Michael talked about the importance of safety by design for critical infrastructure, and of course about improved cybersecurity. This also applies to humanitarian organisations themselves.

notes

summary

1m 58s





# Key Cybersecurity Considerations

**Safety by Design:**  
Prioritize safety by design and strong cybersecurity for critical infrastructure and humanitarian organizations.

**Leadership in Cybersecurity:**  
Humanitarian organizations must better navigate the cyber threat landscape.

**Data Protection:**  
Implement data protection policies to reduce the impact of cyber incidents and ensure proper response.

In the next module, my colleague, Paul Hume, will talk in more details about how humanitarian organisations can show leadership in cybersecurity and better understand and navigate the threat landscape that they operate in.

## notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

## summary

.....

.....

.....

.....

.....

2m 10s







# Key Cybersecurity Considerations

**Safety by Design:**  
Prioritize safety by design and strong cybersecurity for critical infrastructure and humanitarian organizations.

**Leadership in Cybersecurity:**  
Humanitarian organizations must better navigate the cyber threat landscape.

**Data Protection:**  
Implement data protection policies to reduce the impact of cyber incidents and ensure proper response.

As my colleague Andrea already mentioned in her module on legal considerations on cybersecurity, another key aspect is for organisations to put in place clear and effective data protection policies and practises, as it's often data that is targeted when cyber operations are directed at humanitarian organisations.

notes

summary

2m 26s



# Addressing Cyber Risks in Humanitarian Operations



While data protection may not defend against cyber operations, it can mitigate their impact by helping ensure that only necessary data is collected and that procedures are in place to identify, investigate, and respond to incidents, including how and when to notify people whose data has been affected so that they can take steps to protect themselves, as you heard from Felipe earlier on. Humanitarian organisations should also look at how cyber threats are integrated in their analyses and response across the range of their programming to better account for and address their potential consequences.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

2m 47s



---

---

---

---

---



## Addressing Cyber Risks in Humanitarian Operations

**Cyber Risks in Programming:**  
Integrate cyber threat considerations into all programming and responses.

**Protection Work:**  
Assess and address cyber risks in protection work, engaging relevant actors to mitigate harm.

**Innovative Solutions:**  
Explore new approaches like the ICRC's digital emblem to reduce cyber risks.

You heard Michael talk about the role humanitarians can play in conducting risk analyses for critical infrastructure and in anticipating potential cyber operations by building in redundancies when providing support.

notes

summary

3m 28s





## Addressing Cyber Risks in Humanitarian Operations

**Cyber Risks in Programming:**  
Integrate cyber threat considerations into all programming and responses.

**Protection Work:**  
Assess and address cyber risks in protection work, engaging relevant actors to mitigate harm.

**Innovative Solutions:**  
Explore new approaches like the ICRC's digital emblem to reduce cyber risks.

Similarly, protection actors should also integrate cyber risks in their assessments, documentation, and analyses, and when appropriate, raise these issues with relevant duty bearers, whether militaries, governments, or non-state actors, in order to influence their behaviour and help prevent or mitigate harm to civilian populations. You can read more about what to take into account in a protection response to cyber and digital risks in the fourth edition of the professional standards for protection work that we've linked in the additional reading section.

### notes

### summary

3m 44s





## Addressing Cyber Risks in Humanitarian Operations

**Cyber Risks in Programming:**  
Integrate cyber threat considerations into all programming and responses.

**Protection Work:**  
Assess and address cyber risks in protection work, engaging relevant actors to mitigate harm.

**Innovative Solutions:**  
Explore new approaches like the ICRC's digital emblem to reduce cyber risks.

Finally, humanitarian organisations can also explore new and innovative ways to prevent cyber operations or reduce their humanitarian consequences. One example is the ICRC's initiative to explore the possibility of developing a digital emblem, which would be a digital equivalent to the red cross and red crescent emblems used in the physical world. Here's a short video explaining the initiative.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

4m 23s



---

---

---

---

---

---

---

---

---

---



**military operators must verify  
that they do not target protected objects.**

In response to the growing number of harmful cyber operations against medical facilities and humanitarian organisations, the ICRC is proposing the development of a digital emblem. Like the Red Cross, Red Crescent, and red crystal emblems in the physical world, a digital emblem signals that the marked entities must not be attacked. How would a digital emblem work? As part of their legal obligations, military operators must verify

#### notes

---

---

---

---

---

---

---

---

---

---

#### summary

4m 51s



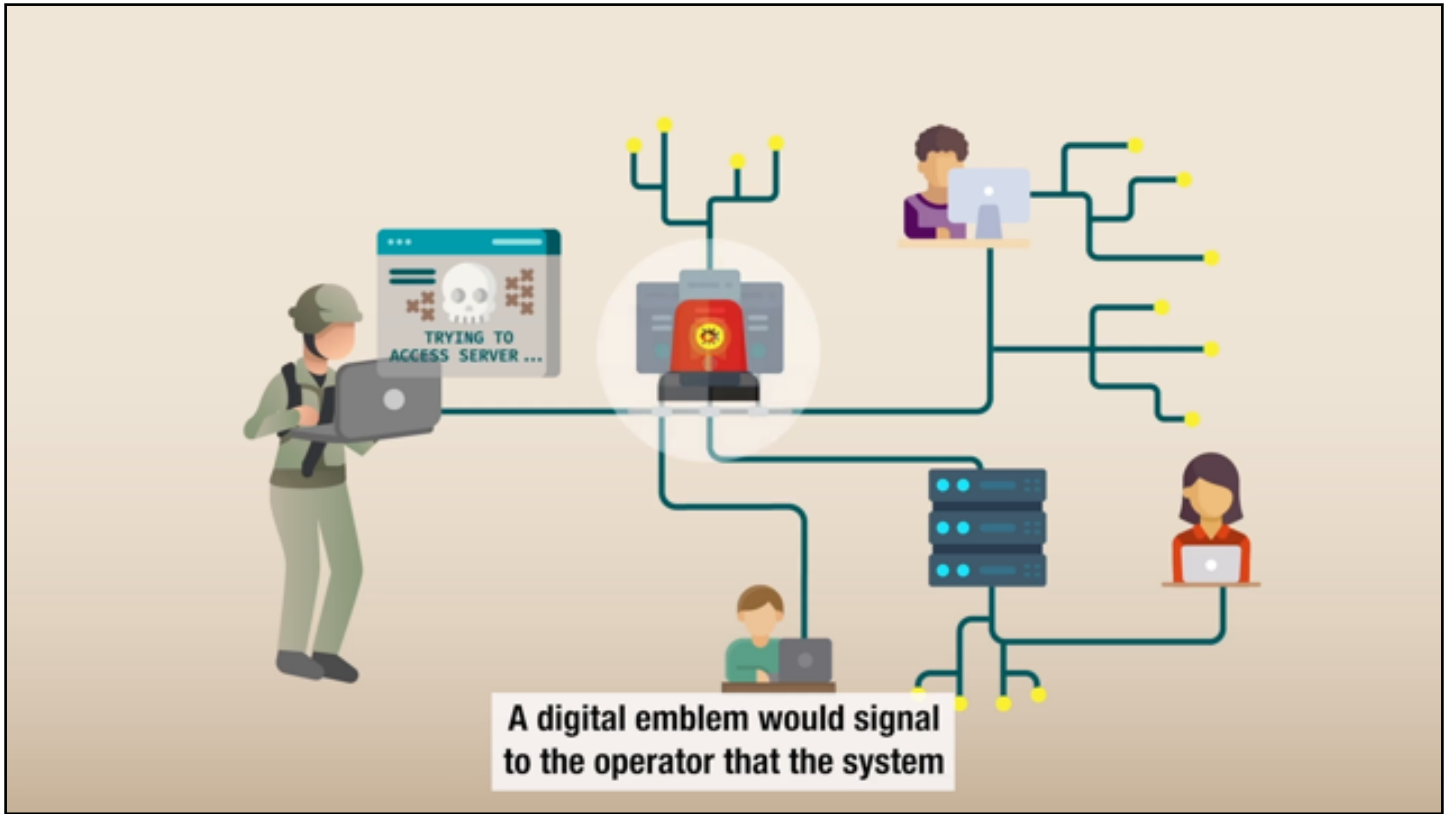
---

---

---

---

---



that they do not target protected objects. A digital emblem would signal to the operator that the system

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

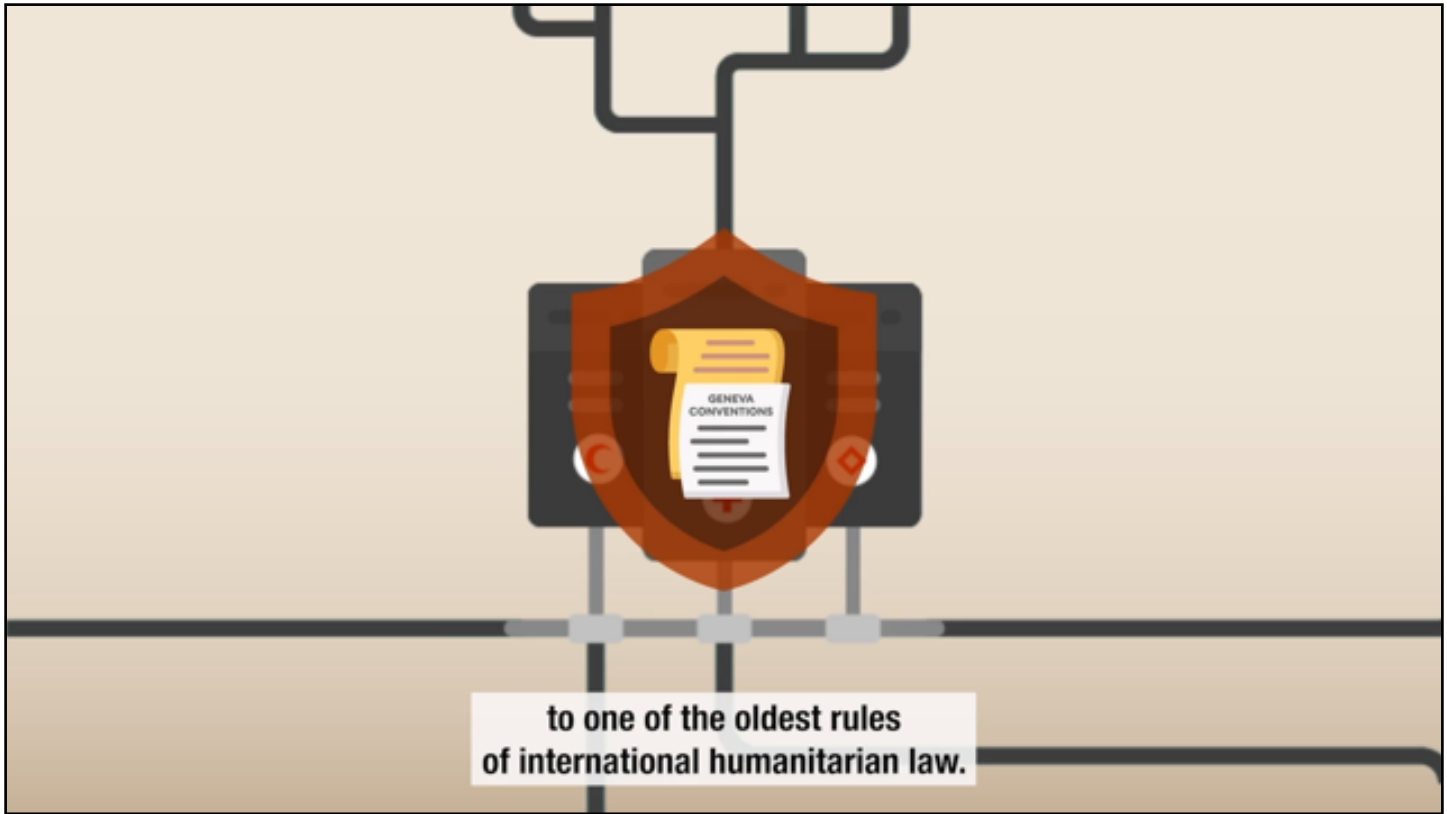
.....

.....

.....

5m 20s





they are about to attack is actually protected the same way the emblem does in the physical world. A digital emblem gives a digital expression to one of the oldest rules of international humanitarian law.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

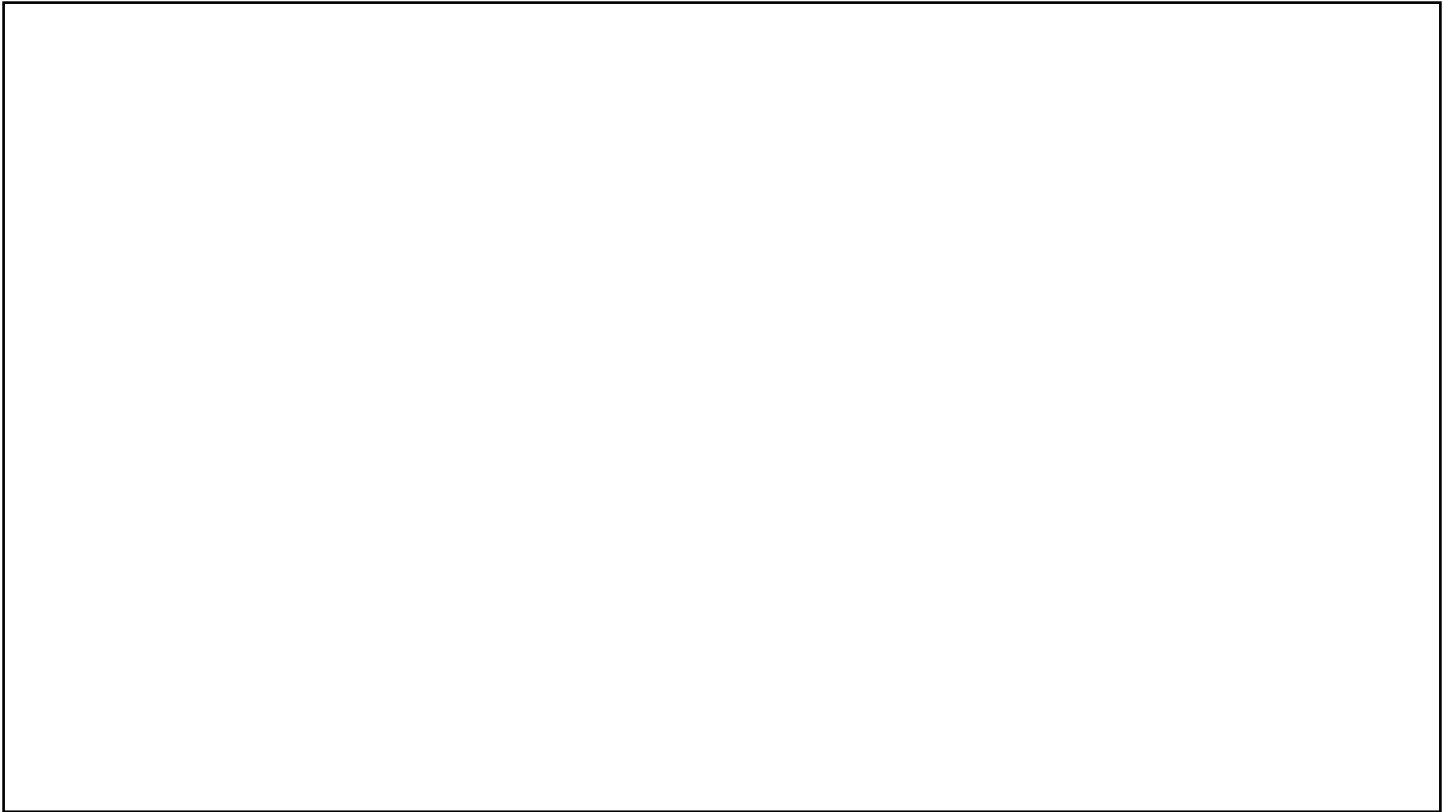
.....

.....

.....







It signals protection, It is not a cybersecurity measure like an antivirus programme. It cannot prevent or stop an attack, just like a Red Cross or Red Crescent cannot block a missile. It relies on the protections of international law, those same protections that have guaranteed the important work of medical and humanitarian workers and their assets all over the world. As you've seen, there are many ways in which organisations can respond to cyber threats in conflicts and humanitarian crises. We hope this module can help you better understand the potential consequences of these threats and provide some inspiration for exploring new avenues to respond to these risks.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

