



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

4.0 Introduction to Cybersecurity - Greg

Concepts (extracted from automatically generated subtitles):

First part of the course. Recent conflicts. Civilian populations. Technical aspects. Private companies. International humanitarian law. Second part of the mooc. Humanitarian operations. First section. Advantage of the training. Third state. Power plants. Unprecedented consequences. Digitally innovative ways. Criminal activities.



[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/>

UNDERSTANDING THE DIGITAL SUPPLY CHAIN AND ITS STAKES FOR HUMANITARIAN ACTORS

EPFL
EssentialTech
Centre



EPFL
**Center for
Digital Trust**

...

notes

summary

0m 0s





Welcome back to our MOOC.

notes

summary

0m 6s





We will now explore the global digital ecosystem from a different angle, cybersecurity. Why is it important? Well, first, cyberspace is nowadays referred to as the fifth military domain.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

0m 13s





The first four being sea, air, land, and space.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

0m 25s





This basically means that warring parties integrate cyberspace in their military strategies,

notes

summary

0m 28s





often through so-called hybrid warfare, which combine cyber and kinetic attacks. In recent conflicts, warring parties, third state and private companies compete in cyberspace and operate in digitally innovative ways,

notes

summary

0m 37s





generating unprecedented consequences for civilian populations, as well as new challenges for international humanitarian law and humanitarian operations. Beyond the military, this space also became a new land of opportunities

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....





for illegal and criminal activities, with more cyberattacks being perpetrated with criminal intent. Civilians might suffer from cyberattacks on critical infrastructures

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

1m 1s





like hospitals, power plants, or dams, humanitarian organisations might become targets of direct cyberattacks, putting at stake the continuity of their operations,

notes

summary

1m 13s





but also the data of the people they serve. Virtualization of resources in the cloud represents another risk for humanitarian organisations, which could become the collateral damage

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

1m 25s



.....

.....



of a cyberattack on a public cloud, for instance. In a nutshell, the digital supply chain plays a key role in how cyberattacks can be perpetrated. As we saw in the first part of the course,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

1m 37s





this digital supply chain is potentially vulnerable to attacks and needs to be protected.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

1m 49s



.....

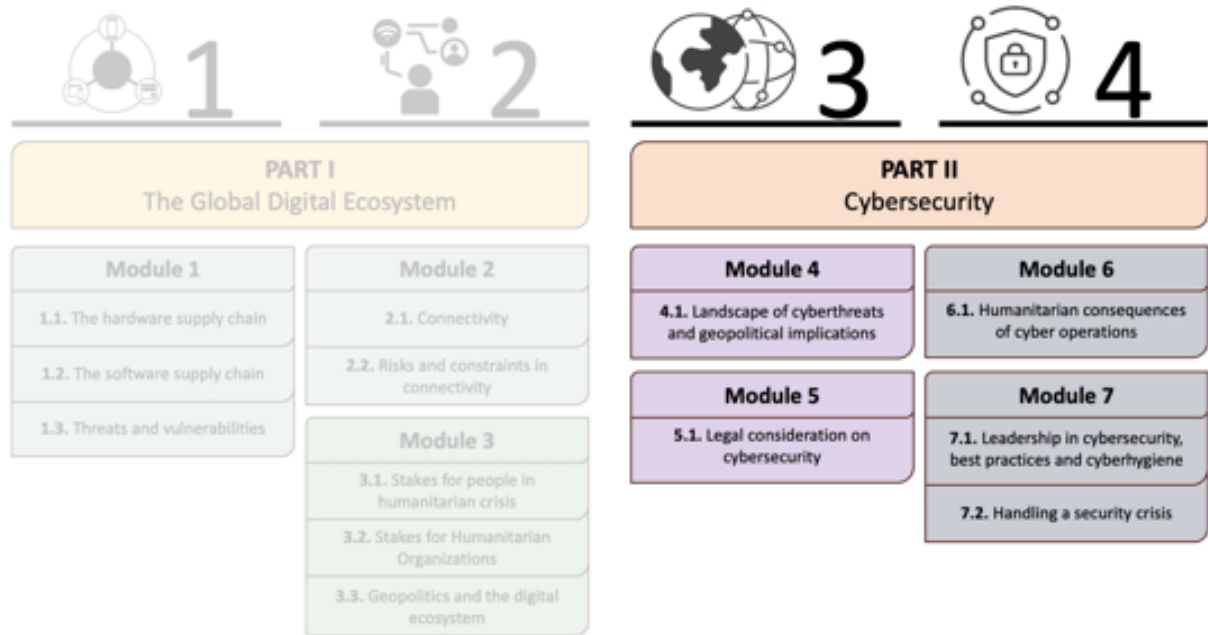
.....

.....

.....

.....

WEEKS



During the second part of the MOOC, you will investigate cybersecurity from various perspectives.

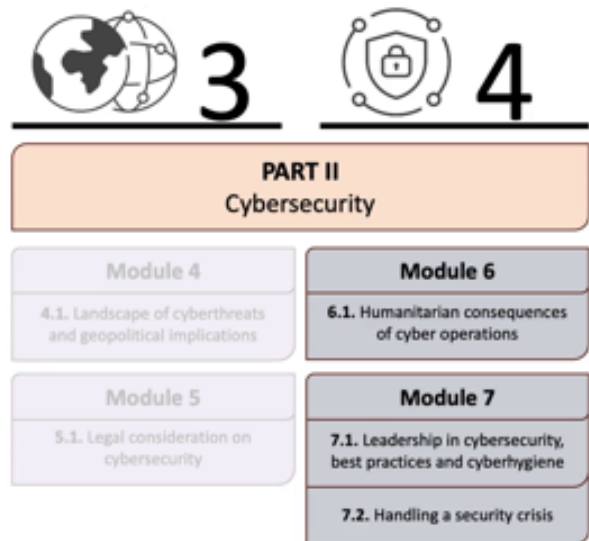
notes

summary

1m 53s



WEEKS



We divided it into two sections and four modules. In the first section, you will explore the geopolitical and legal considerations on cybersecurity. In the second, you will learn about cyber resilience,

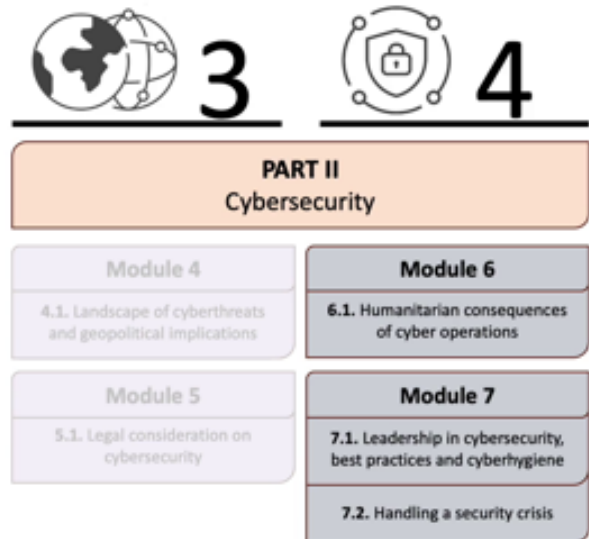
notes

summary

2m 1s



WEEKS



first by investigating humanitarian consequences of cyber operations, and then by discussing leadership, best practices, and crisis management of cyberattacks.

notes

summary

2m 13s





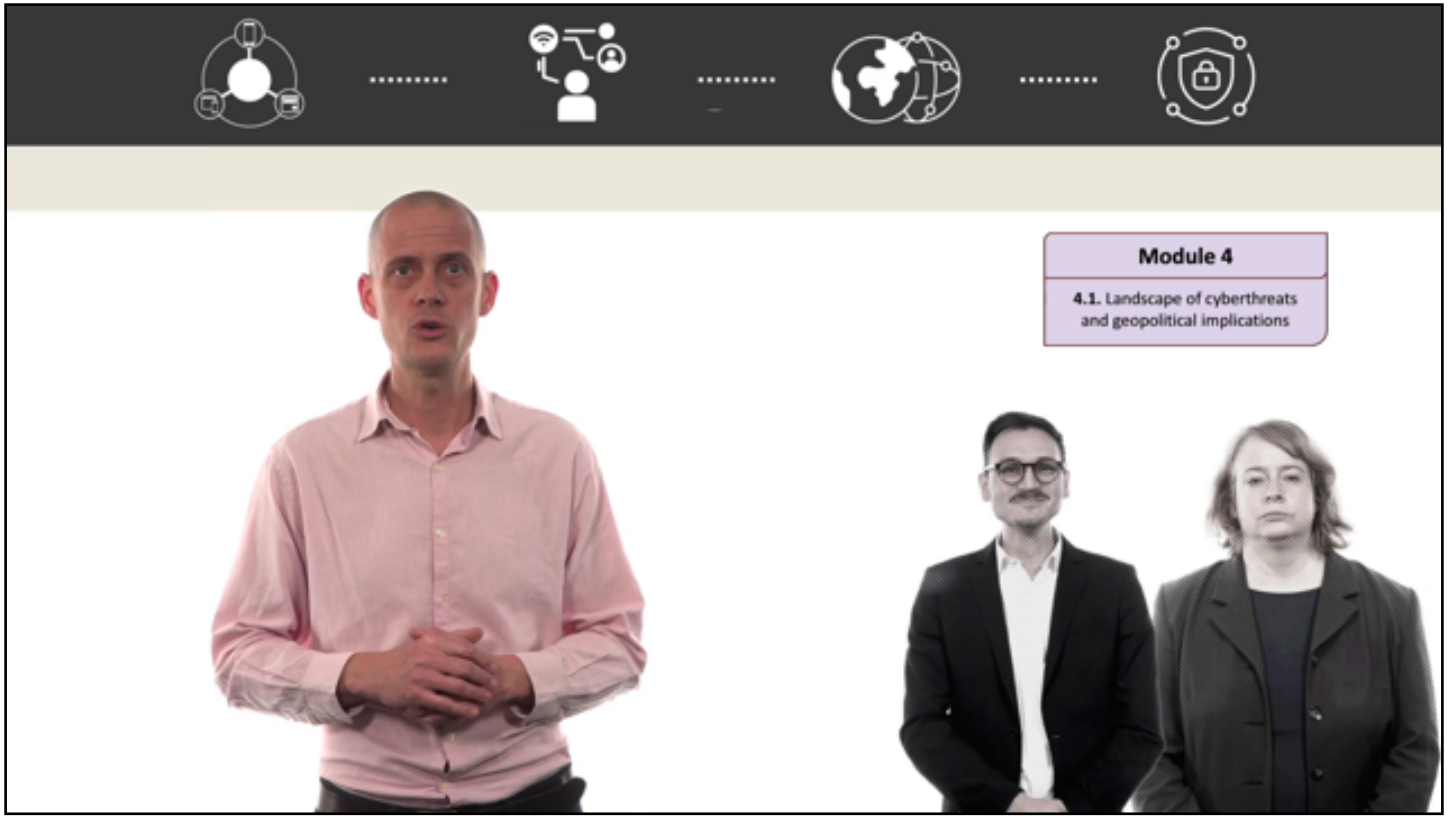
Let's now focus on the next two modules.

notes

summary

2m 22s





In Module 4, a geopolitical perspective on cybersecurity will be shared, together with the definition of the types and origins of threats. This module is given by Dr. Myriam Dunn and Sean Cordey

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

2m 25s





5.1. Legal consideration on cybersecurity

notes

2m 37s





from the ICRC Cyber Delegation in Luxembourg. Altogether, after following the second part of the MOOC, you will benefit from a solid understanding of cybersecurity,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

2m 49s





allowing you to critically assess humanitarian, organisational, and geopolitical stakes related to cybersecurity. Enjoy. Remember, if you feel like there are some technical aspects you are lacking to fully take advantage of the training, then please check our first MOOC on Humanitarian Action in the Digital Age.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

3m 1s



.....

.....

.....

.....

.....