



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

6.2 Cyber Ops against civilian infrastructure and services ITW with Michael

Concepts (extracted from automatically generated subtitles):

Essential services. Food production systems. Protection of essential services. Humanitarian operations. Cyber operations. Civilian infrastructure. Electricity service providers. Critical infrastructure. Delivery of such services. Supportive water. Michael talhami. Significant impact. Digital control systems. Icrc colleague. Essential civilian infrastructure.



[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 1/54



HUMANITARIAN CONSEQUENCES OF CYBER OPERATIONS

Interview with Michael Talhami

Senior program manager for critical infrastructure and essential services in the Near and Middle East, ICRC

Cléa Thouin

Protection in the Digital Age specialist, ICRC



...

notes

summary

0m 0s



Welcome



Hello again. In this video, I'll be talking to my ICRC colleague, Michael Talhami, about cyber operations against civilian infrastructure.

notes

summary

0m 4s



Welcome



Michael is a senior programme manager for critical infrastructure and essential services in the near and Middle East.

notes

summary

0m 13s



Welcome



He's advised the ICRC for 13 years on the protection of essential services. In his current role, he oversees humanitarian operations in supportive water, sanitation, and electricity service providers that aim

notes

summary

0m 25s



Definition of Critical Infrastructure and Essential Services



to strengthen their resilience to the effects of conflict and climate hazards. Michael, welcome. Thanks so much for talking to us. Thanks for having me.

notes

summary

0m 37s



Definition of Critical Infrastructure and Essential Services



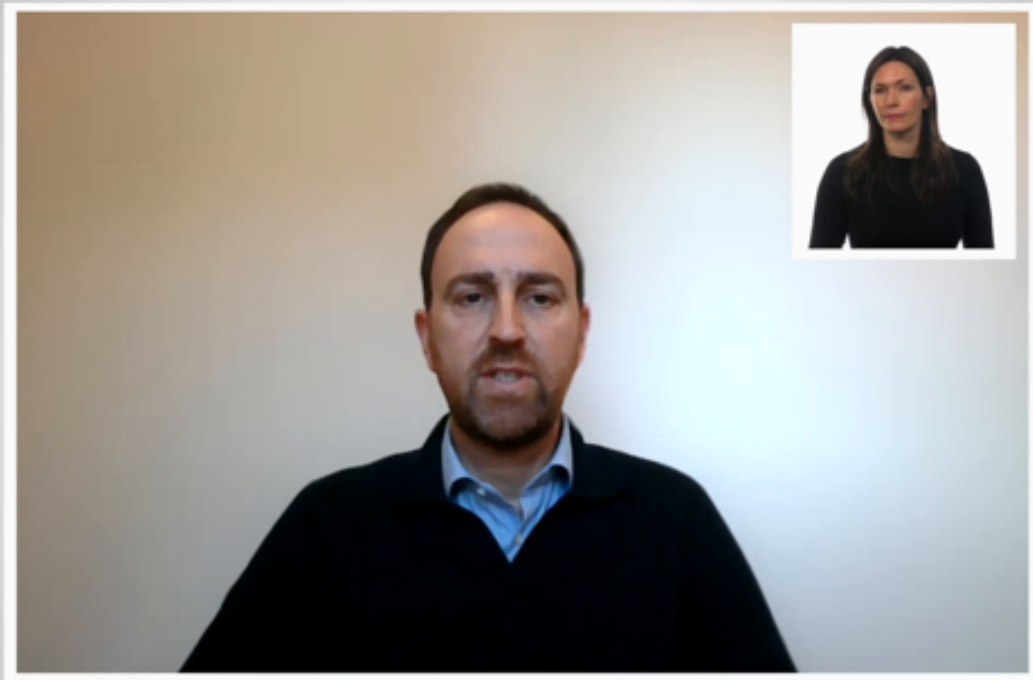
Before we get into what cyber operations against essential civilian infrastructure can look like, let's take a few steps back and talk about essential civilian infrastructure itself.

notes

summary

0m 49s





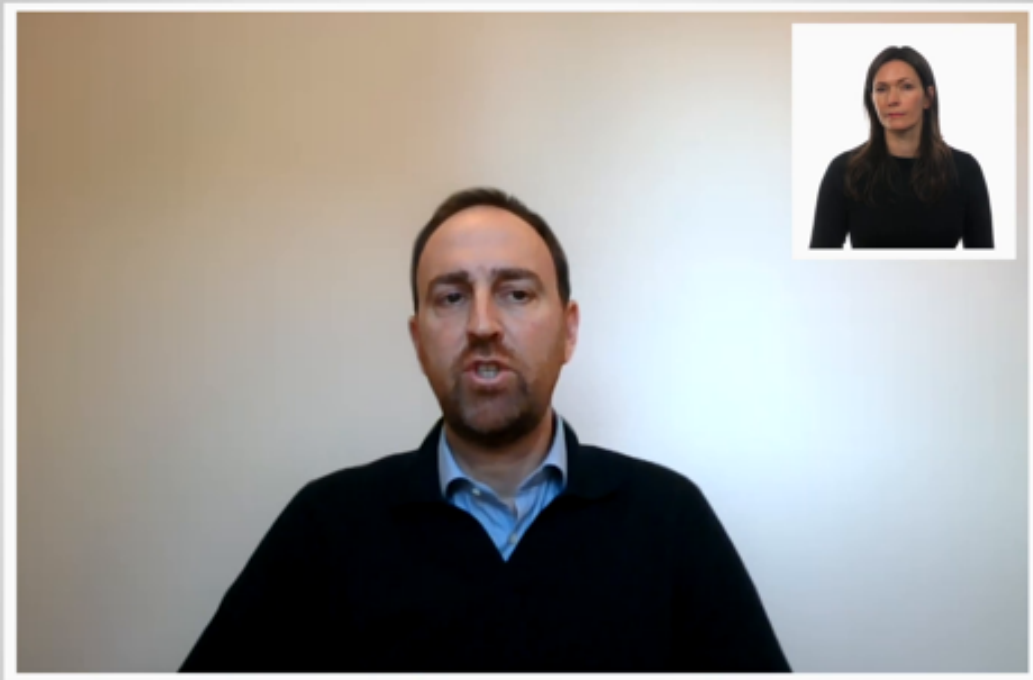
In news articles, we often see references to critical infrastructure. What do we mean when we use this term? Are those two terms the same? At the ICRC, we usually refer to essential services.

notes

summary

1m 1s





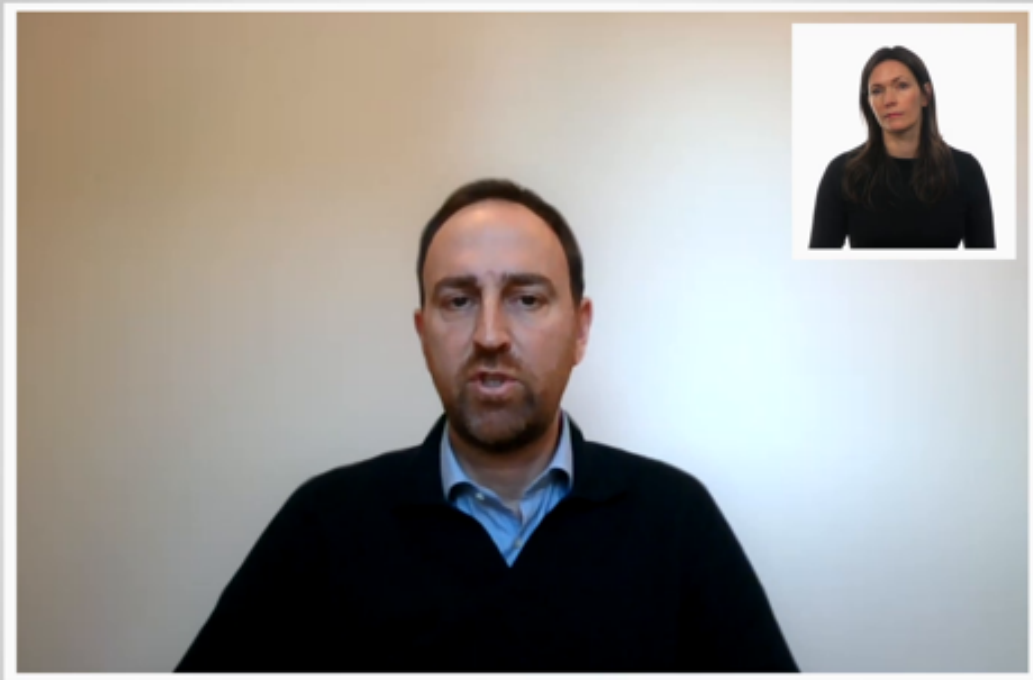
Essential services are services indispensable to the survival

notes

summary

1m 13s





of the civilian population, such as water and sanitation, electricity, health care, food production systems, and solid waste disposal. The reason we talk about essential services is that the focus needs to be on the service and not just the infrastructure. Ensuring that civilians have access to essential services requires not only

notes

summary

1m 16s



Components of Essential Services



All essential services depend on ...

... people



... hardware



... consumables



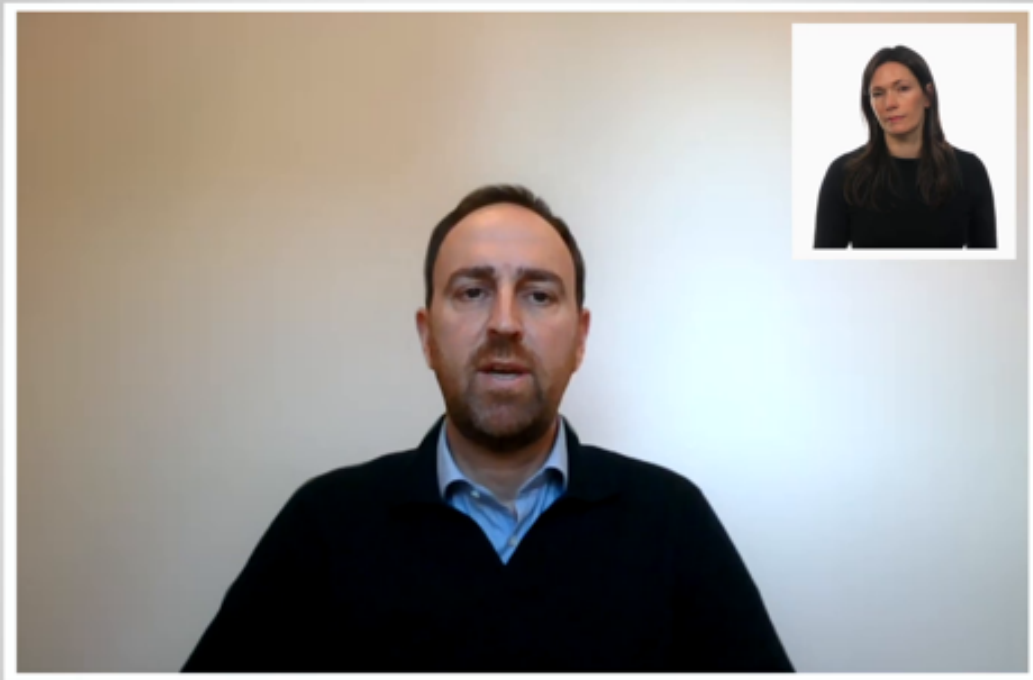
protecting civilian infrastructure, but also the service provider personnel who operate, maintain, and repair the infrastructure, as well as the necessary contingency stocks, replacement parts, and consumables.

notes

summary

1m 36s





Whereas by critical infrastructure, we mean infrastructure necessary

notes

summary

1m 47s



Critical Infrastructure



Critical infrastructure is infrastructure necessary for the functioning of an essential service and whose damage or destruction has a significant impact on the delivery of the service.

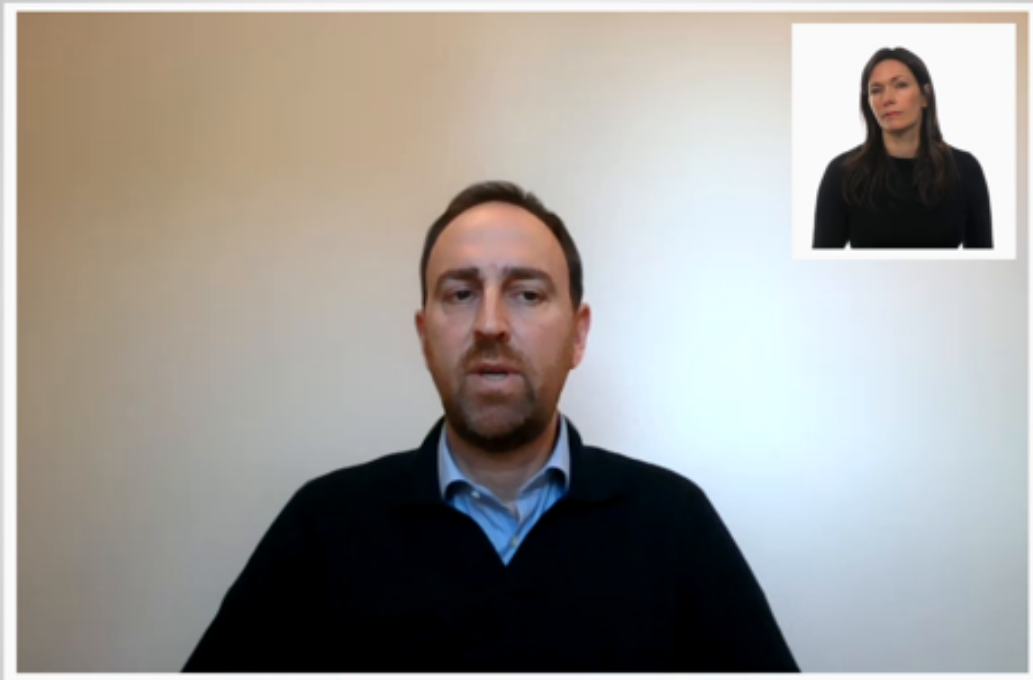
for the functioning of an essential service and whose damage or destruction has a significant impact on the delivery of the service. This said, different actors have different definitions of critical infrastructure.

notes

summary

1m 53s





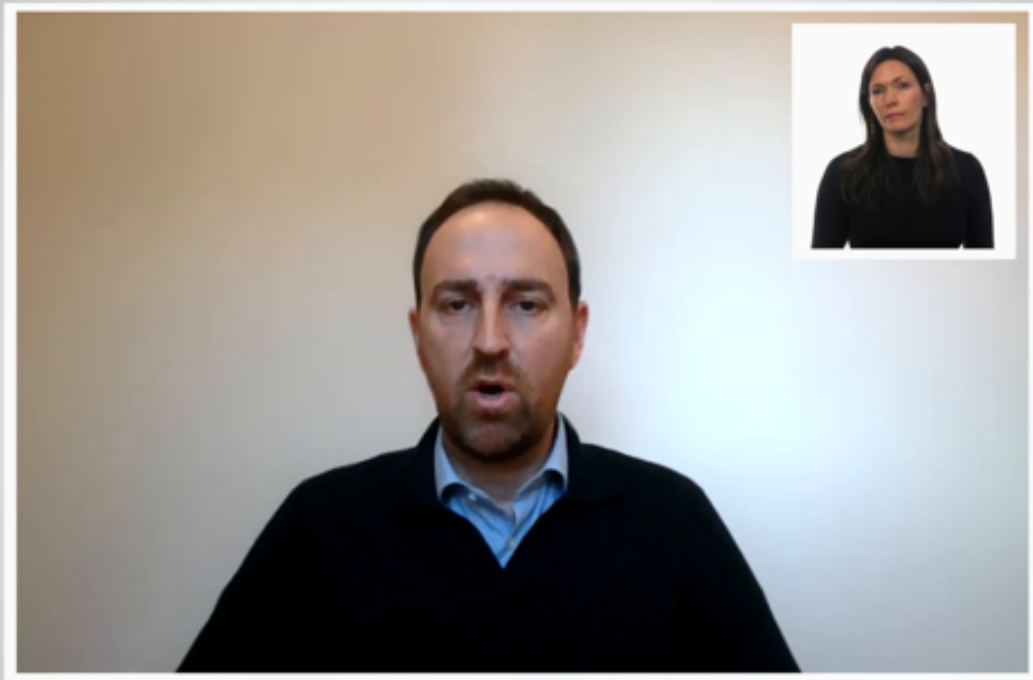
For example, states often include a broad set of critical infrastructure sectors that fall under their national security in this definition.

notes

summary

2m 4s





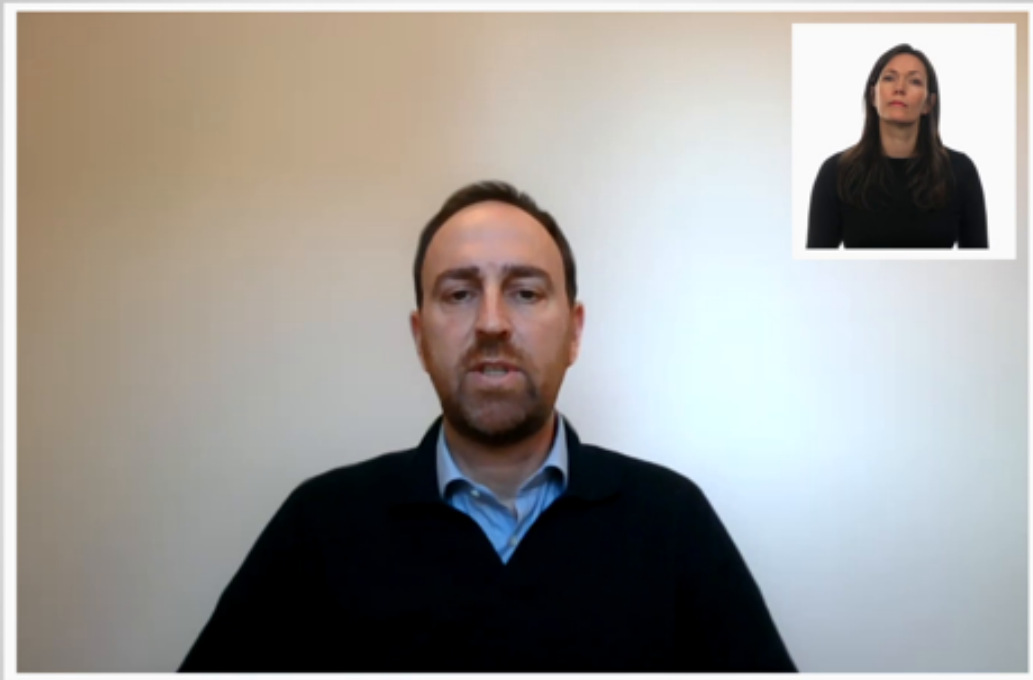
Whereas at the ICRC, we are talking exclusively about civilian infrastructure that enables the delivery of essential services. It is important to note in this regard that international humanitarian law

notes

summary

2m 13s





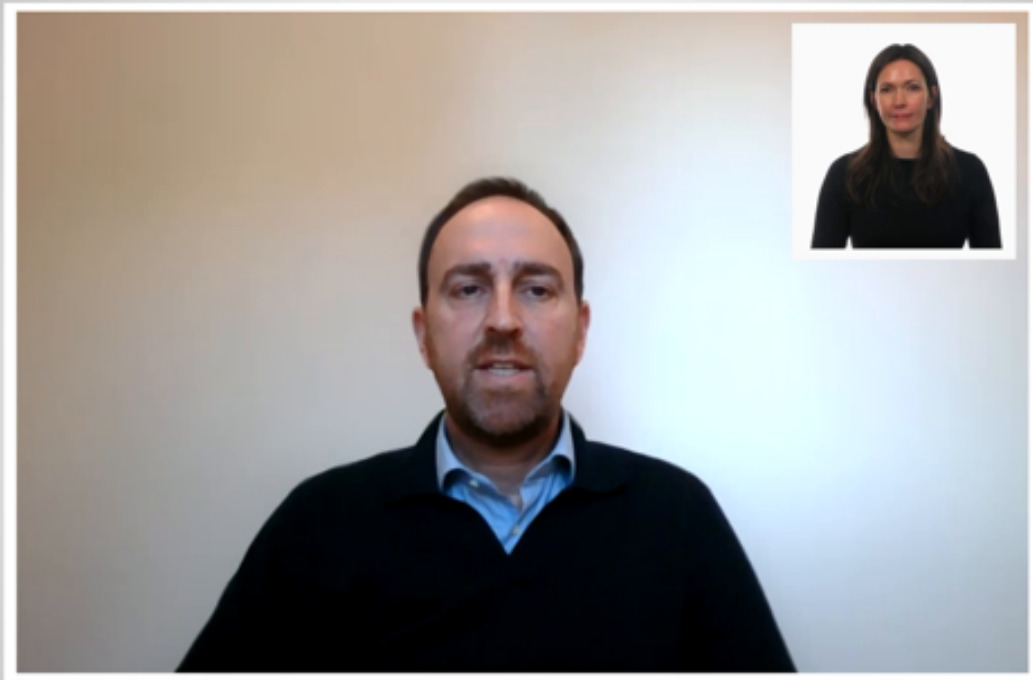
prohibits parties from attacking, destroying, removing, or rendering useless objects indispensable to the survival of the civilian population, which includes infrastructure that is

notes

summary

2m 25s





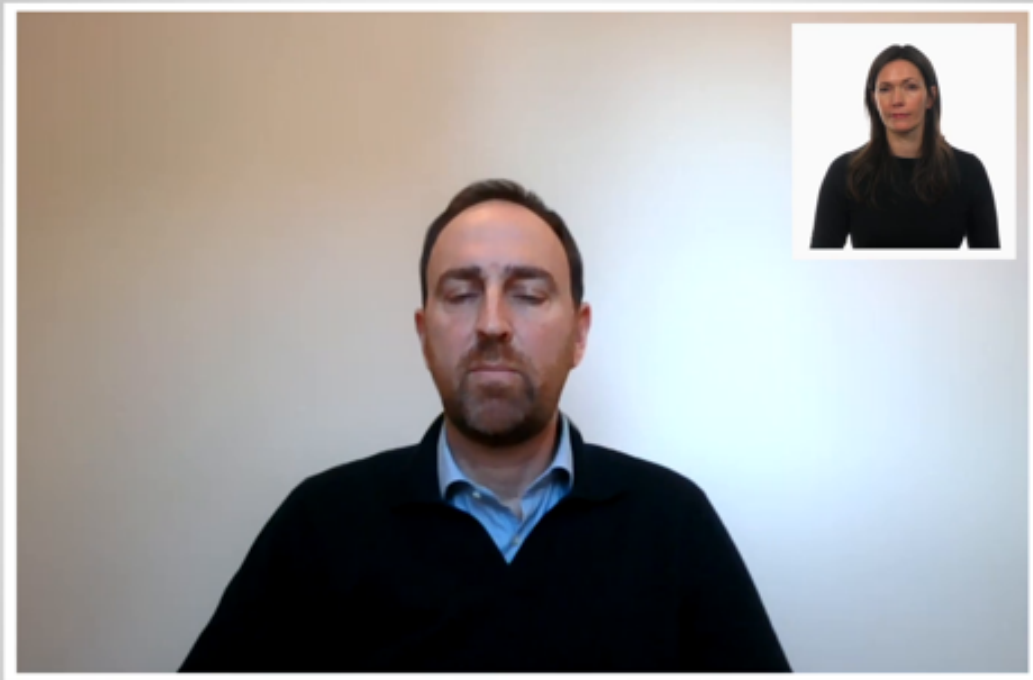
critical to the delivery of such services. Thanks for clarifying those concepts for us. So how has digitalization impacted the delivery of essential services?

notes

summary

2m 37s





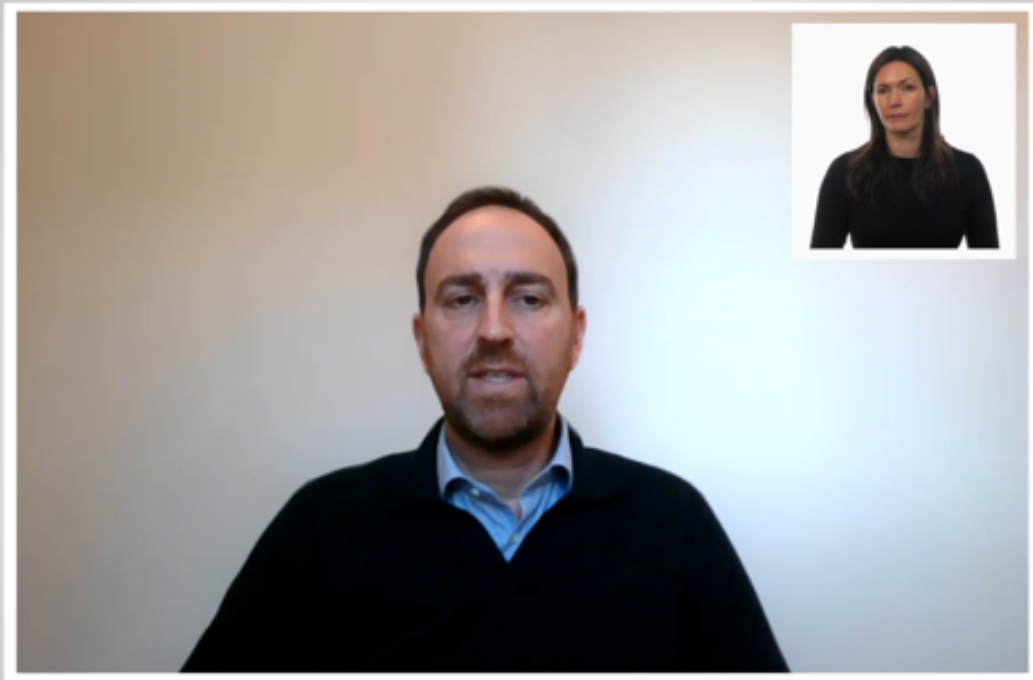
Digitalization adds another layer of complexity to the delivery of essential services. It enables the remote operation of critical infrastructure that allows for greater efficiency in the delivery of essential services to the

notes

summary

2m 49s





population in the service area. For example, a water operator can remotely control the operation of a valve to open and close it to divulge water to a different part of the city.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

3m 1s



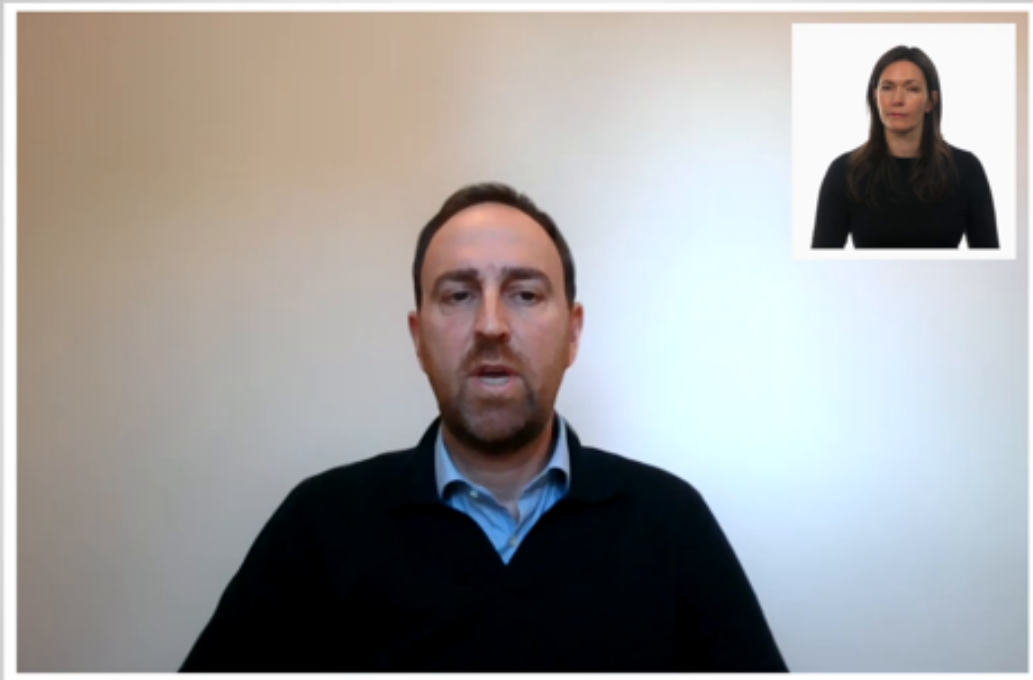
.....

.....

.....

.....

.....



Automating these systems is important for their normal operation and during hostilities that can help reduce the exposure of service provider personnel. In fact, digital control systems such as SCADA systems,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

3m 13s



.....

.....

.....

.....

Cyber Vulnerabilities of Essential Services



supervisory control and data acquisition systems have become commonplace to monitor and operate water and wastewater systems, electricity grids, and even hospitals.

notes

summary

3m 25s



Cyber Vulnerabilities of Essential Services



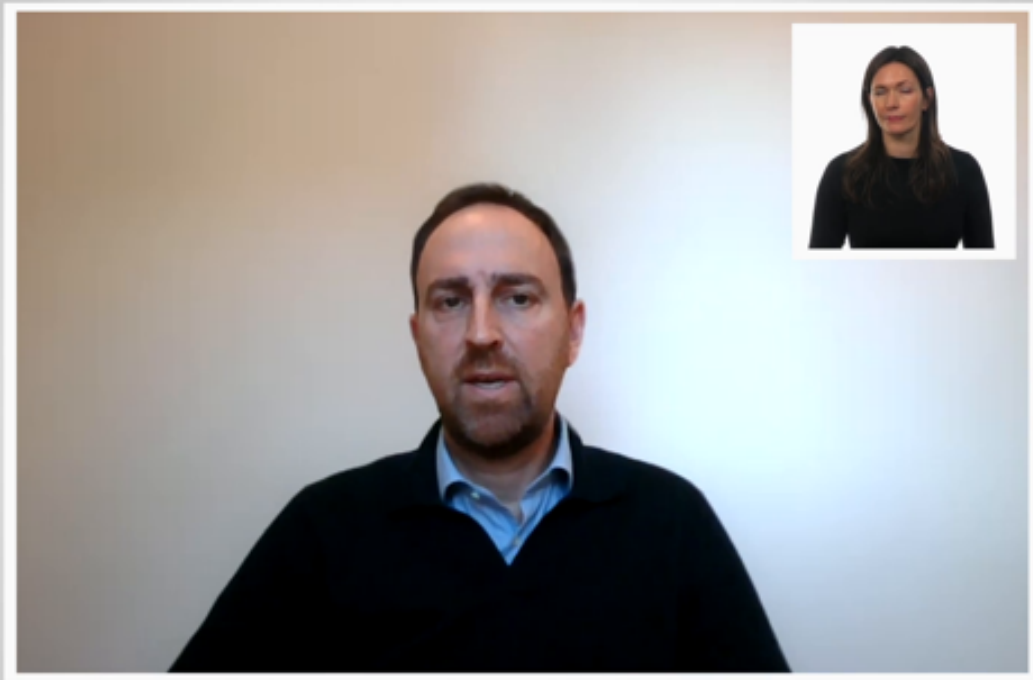
Now that we have a better understanding of what we mean by essential services and how they use digital technology, can you explain to us how they can be targeted by cyber operations?

notes

summary

3m 37s





When remote operation is introduced into essential service systems, it can create technical vulnerabilities that can be at risk from cyberattacks.

notes

summary

3m 49s



SCADA System



A SCADA system (Supervisory control and data acquisition) is a control system architecture comprising of computers, servers, data centers, networked data communications, and graphical user interfaces for high-level supervision of critical infrastructure.

For instance, a SCADA system, which is a control system architecture

notes

summary

3m 58s



SCADA System



A SCADA system (Supervisory control and data acquisition) is a control system architecture comprising of computers, servers, data centers, networked data communications, and graphical user interfaces for high-level supervision of critical infrastructure.

comprising of computers, servers, data centres, network data communications, and graphical user interfaces for high-level supervision of critical infrastructure and the delivery of an essential service,

notes

summary

4m 1s



Attack Surface Vulnerabilities



Networks
(e.g. telecom lines,
proxies, routers,
firewalls, protocols,
ports, connected
devices).

Software
(e.g. web and mobile
apps).

Humans
(e.g. errors, trusted
insider).

can be vulnerable to attack. Such attack surface vulnerabilities include networks, for example, telecom lines, proxies, and routers.

notes

summary

4m 15s



Attack Surface Vulnerabilities



Networks
(e.g. telecom lines,
proxies, routers,
firewalls, protocols,
ports, connected
devices).

Software
(e.g. web and mobile
apps).

Humans
(e.g. errors, trusted
insider).

Secondly, software such as web and mobile apps. Thirdly, humans in terms of human errors or trusted insiders. This is of a real concern, considering essential service providers

notes

summary

4m 25s



Attack Surface Vulnerabilities



Networks
(e.g. telecom lines,
proxies, routers,
firewalls, protocols,
ports, connected
devices).

Software
(e.g. web and mobile
apps).

Humans
(e.g. errors, trusted
insider).

often do not dedicate enough human and financial resources to cybersecurity. Moreover, the systems they operate often run on outdated software with systems that have been in place for years, potentially never receiving

notes

summary

4m 37s



Humanitarian Consequences of Cyber Operations



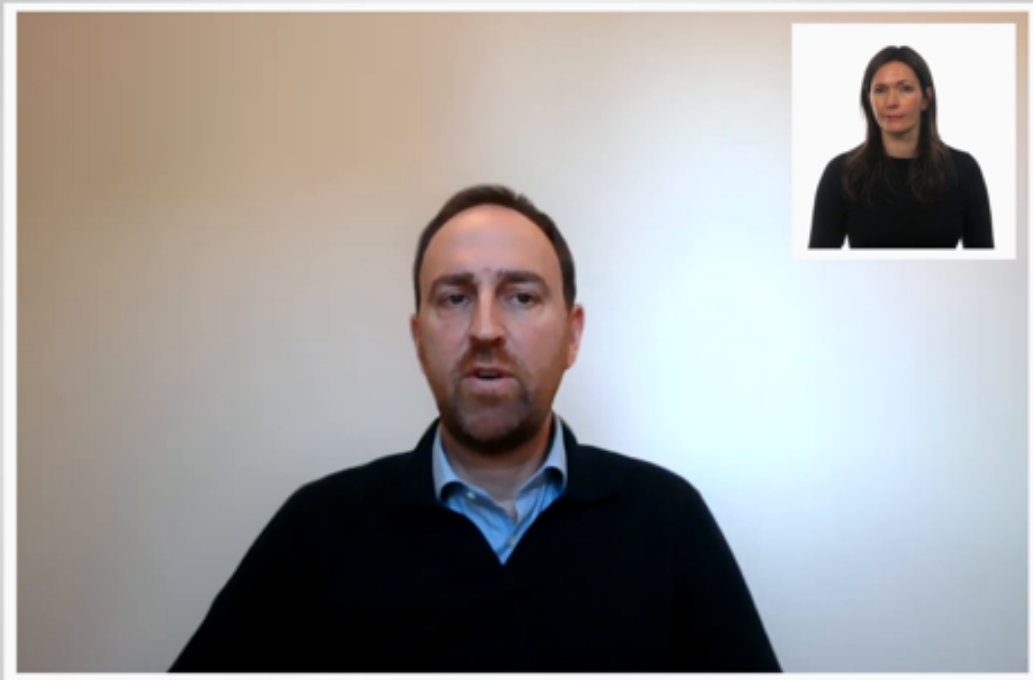
security updates. Given all of these vulnerabilities that you've mentioned, what humanitarian consequences can cyber operations against critical infrastructure have?

notes

summary

4m 49s





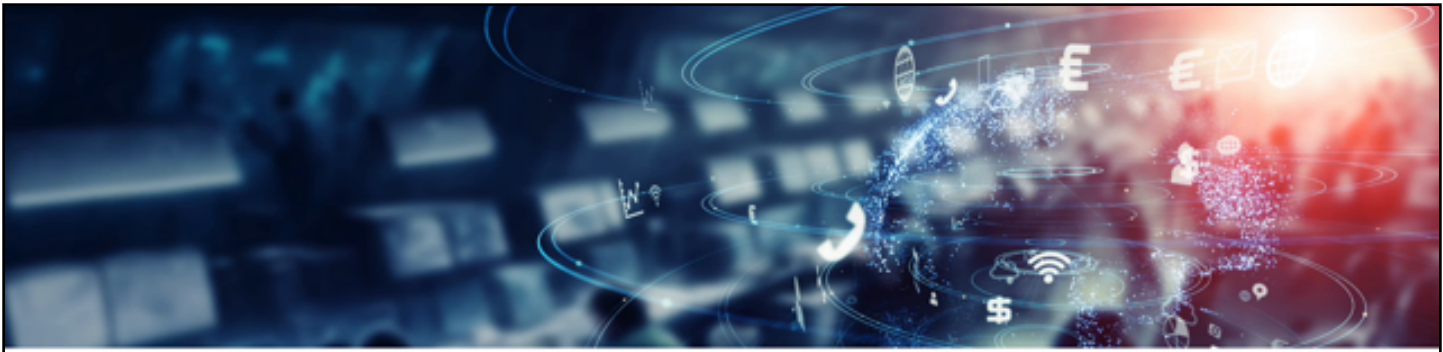
Cyberattacks destroying or tampering with the IT or SCADA systems that allow for the remote operation of critical infrastructure can render the service

notes

summary

5m 1s





Humanitarian Consequences of Cyber Operations

Cyber-attacks

Destruction or tampering of IT or SCADA systems of critical infrastructure can render the service inoperable or limit its function.

Consequences

Service deprivation in parts of coverage area, erroneous data reporting and service disruption.

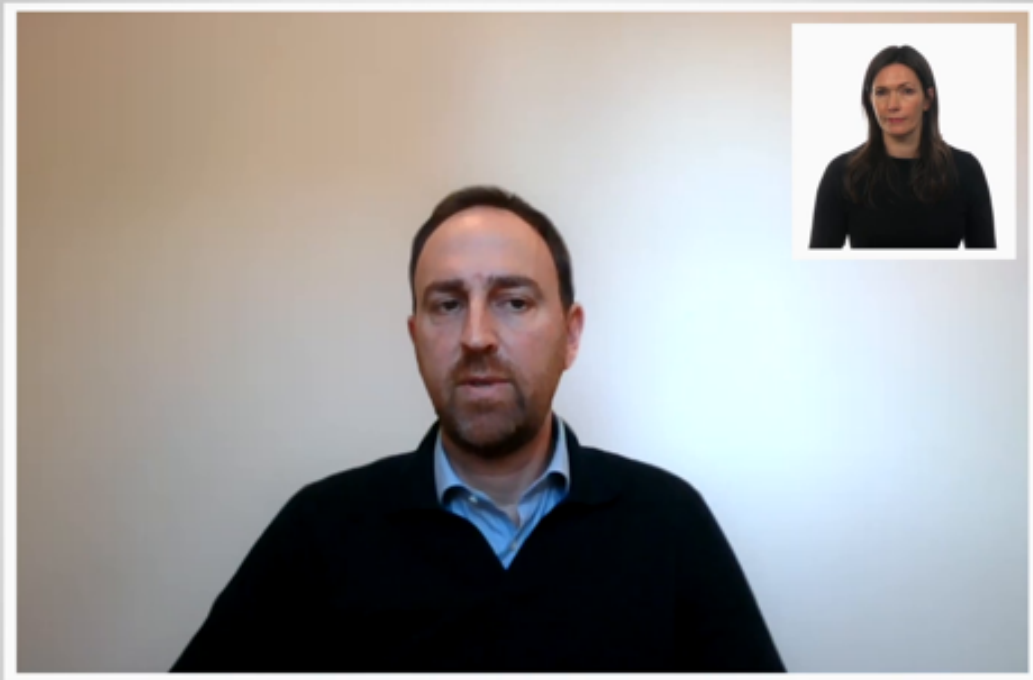
inoperable or limit its function. This in turn can deprive parts of or all of a coverage area of access to that service or report erroneous data that can lead to the disruption and access to services.

notes

summary

5m 10s





Most essential services are highly interdependent. For instance, water and wastewater services require electricity to function.

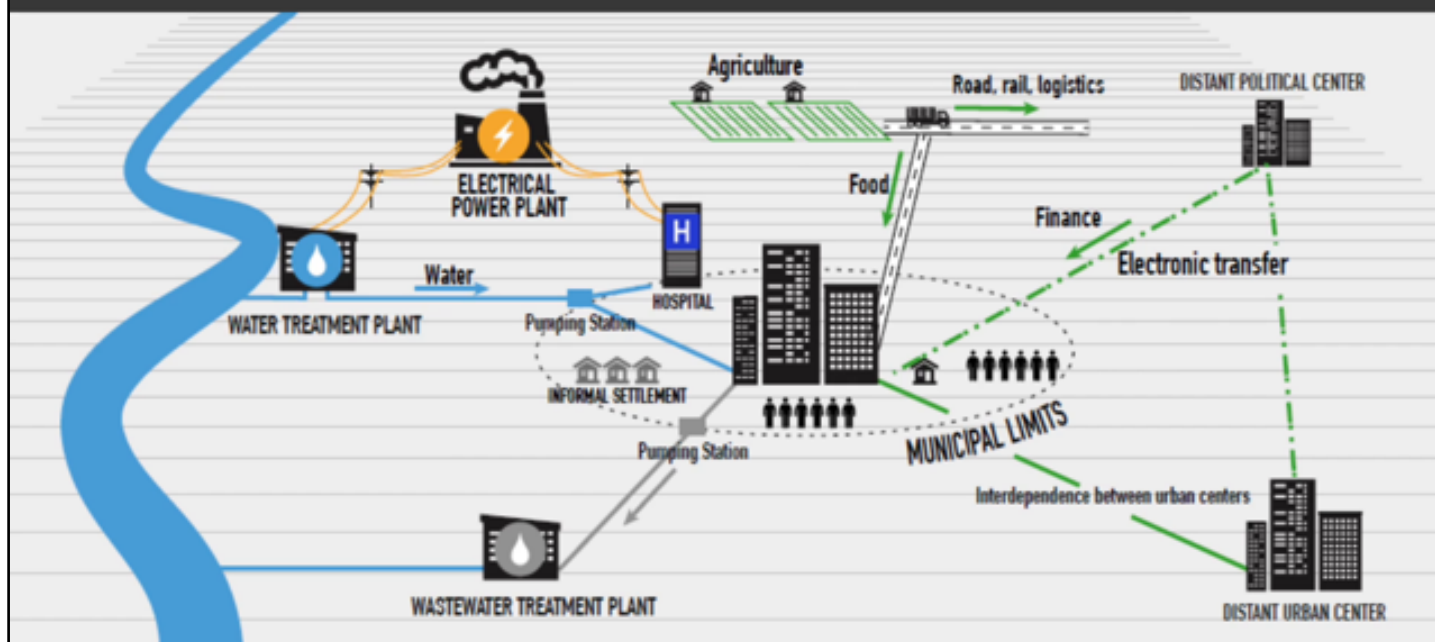
notes

summary

5m 23s



Most essential services are highly interdependent



Stand-alone essential services such as hospitals or schools rely on pipeline services, namely water, wastewater, and electricity to operate.

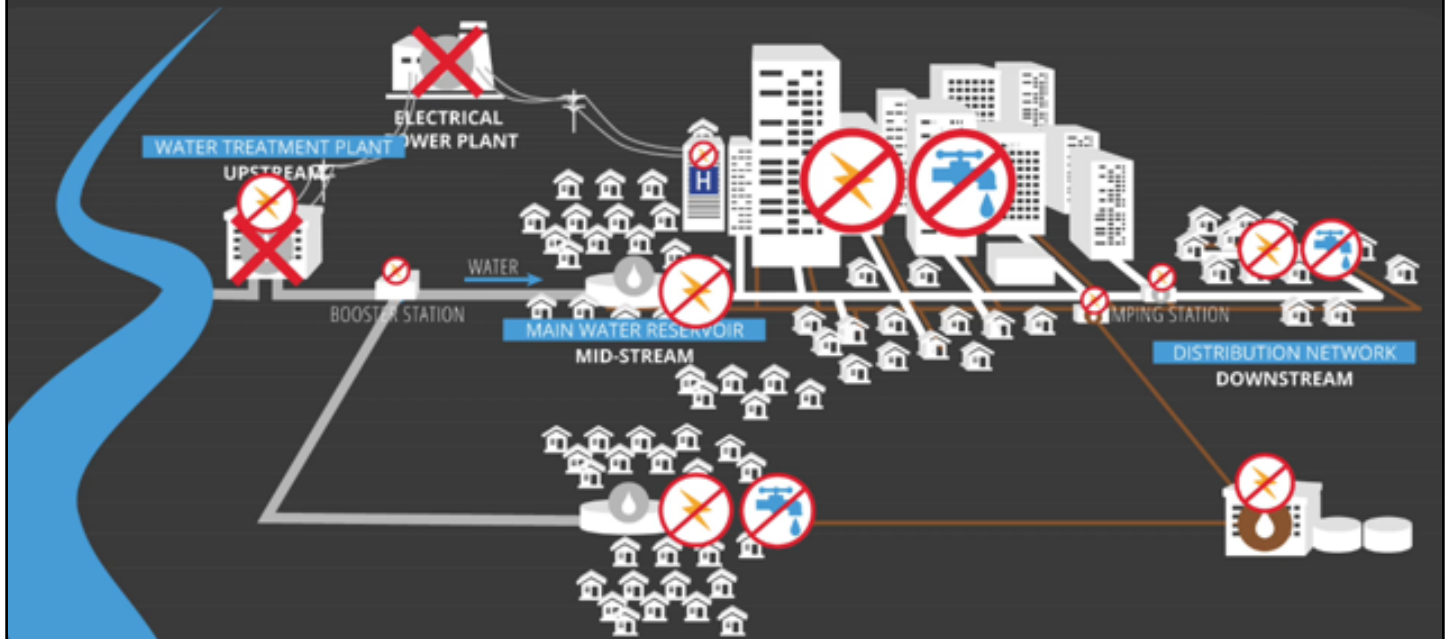
notes

summary

5m 31s



Domino Effects



The interdependence between essential services can create a vast vulnerability whereby rendering inoperable one service such as electricity can have a domino

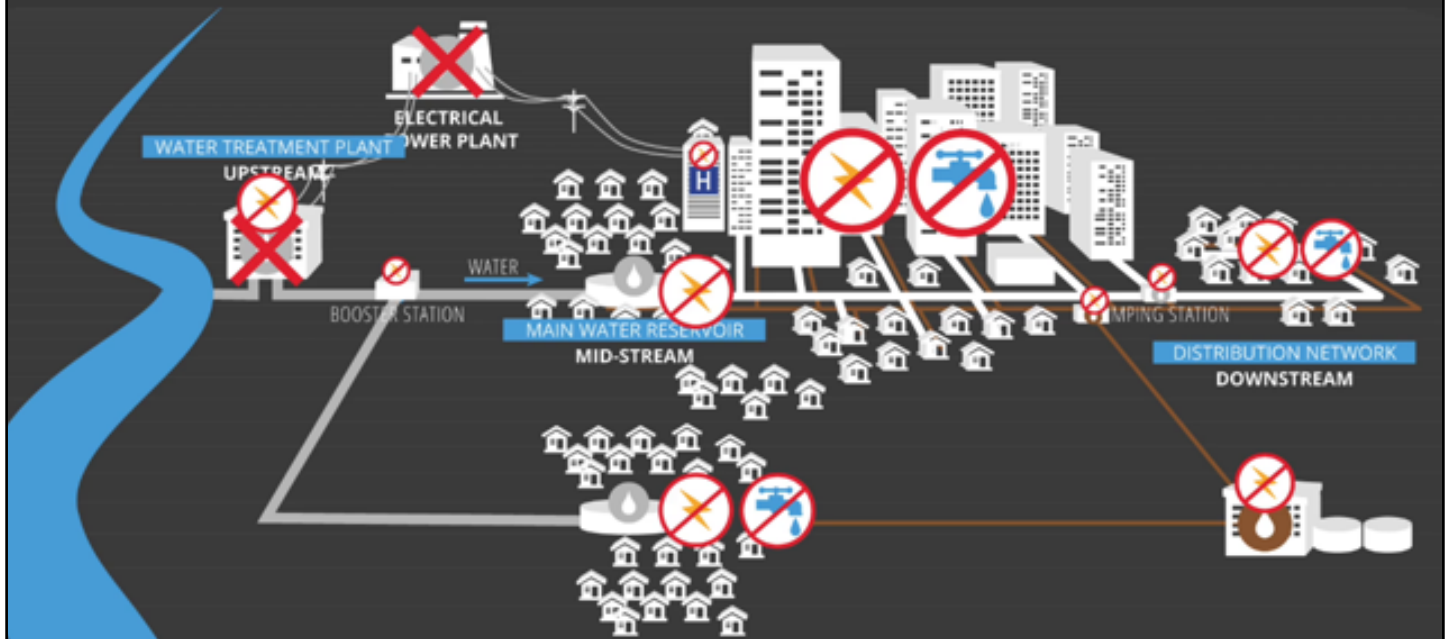
notes

summary

5m 42s



Domino Effects



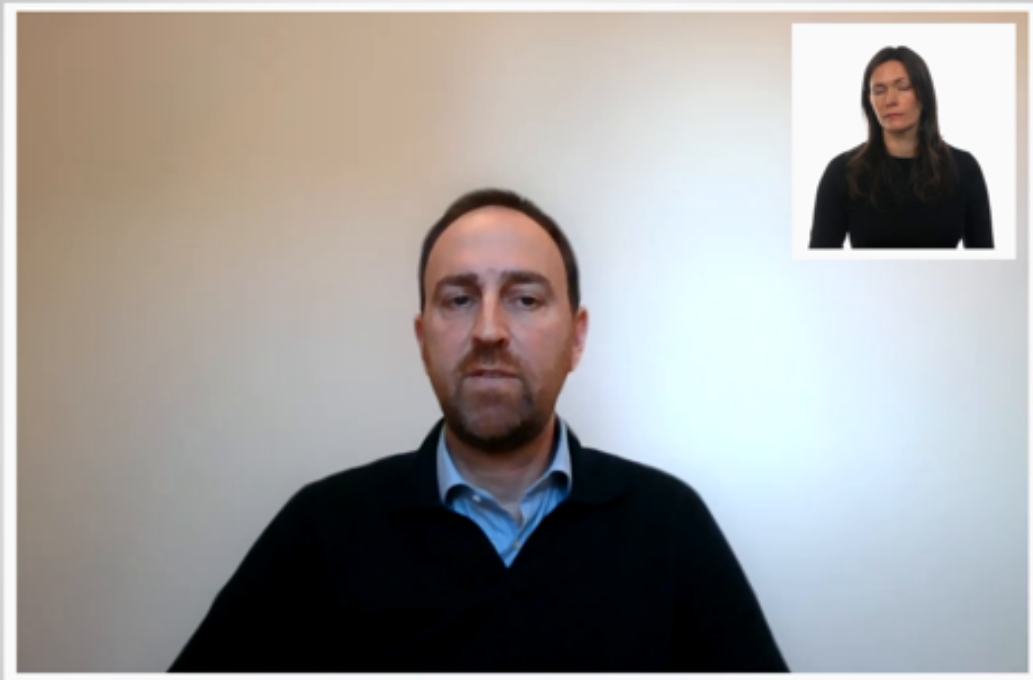
effect that disrupts the delivery of all other services that are reliant on it to function. The humanitarian consequences of such disruptions to essential services can be

notes

summary

5m 52s





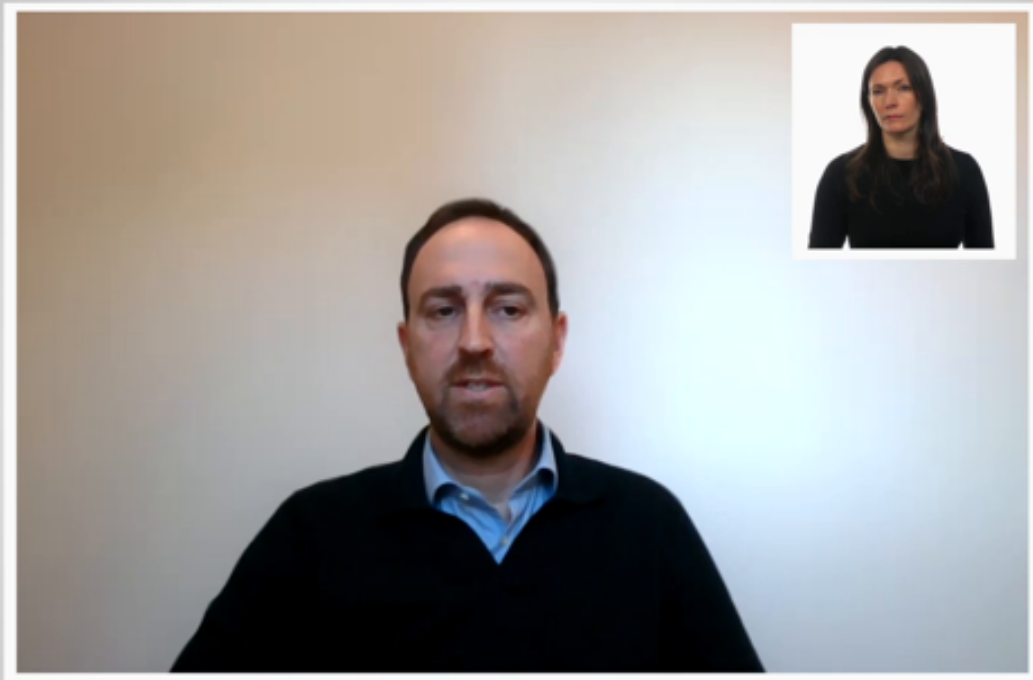
both immediate and long-term, often resulting in a degradation of public health. This can range from an immediate risk of death in extreme cases to a gradual

notes

summary

6m 1s





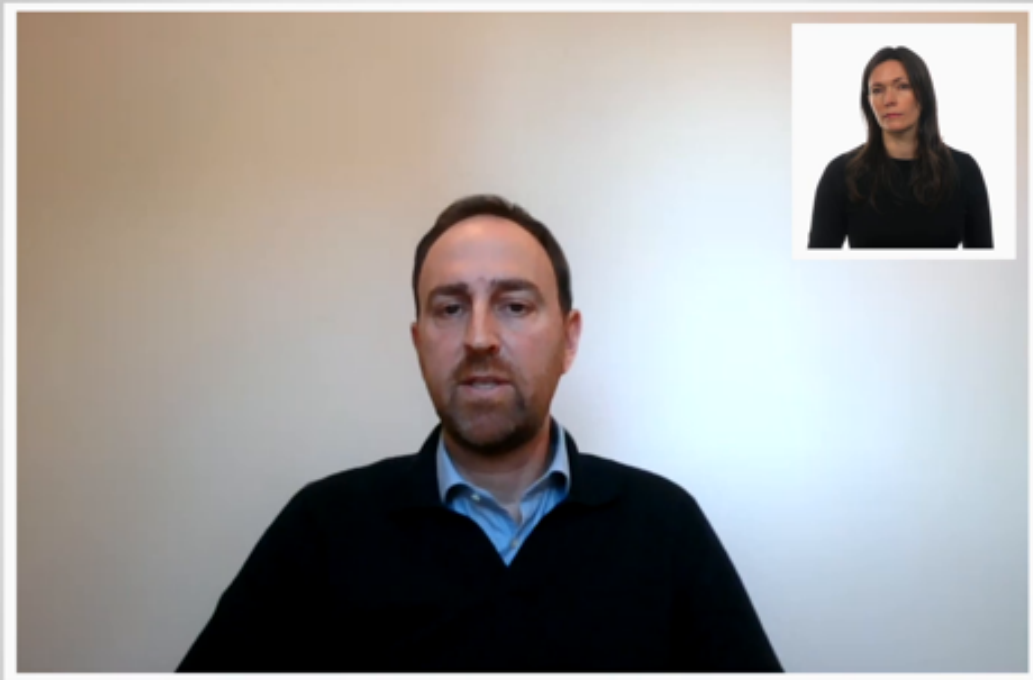
increase in mortality rates and a loss of dignified living conditions. For example, hospitals without electricity or clean water can struggle to perform safe surgeries or provide basic treatment to prevent the spread of an infectious disease.

notes

summary

6m 13s





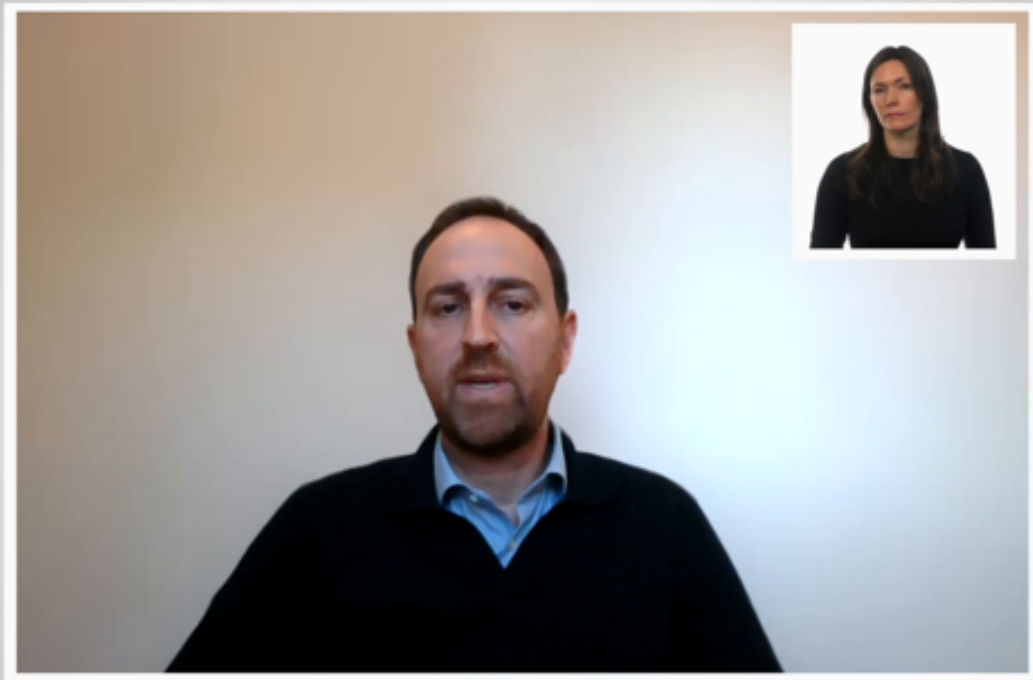
If drinking water facilities cease to function, this can create long-term risks for an outbreak and spread of infectious disease. These impacts are particularly severe in densely populated areas

notes

summary

6m 25s





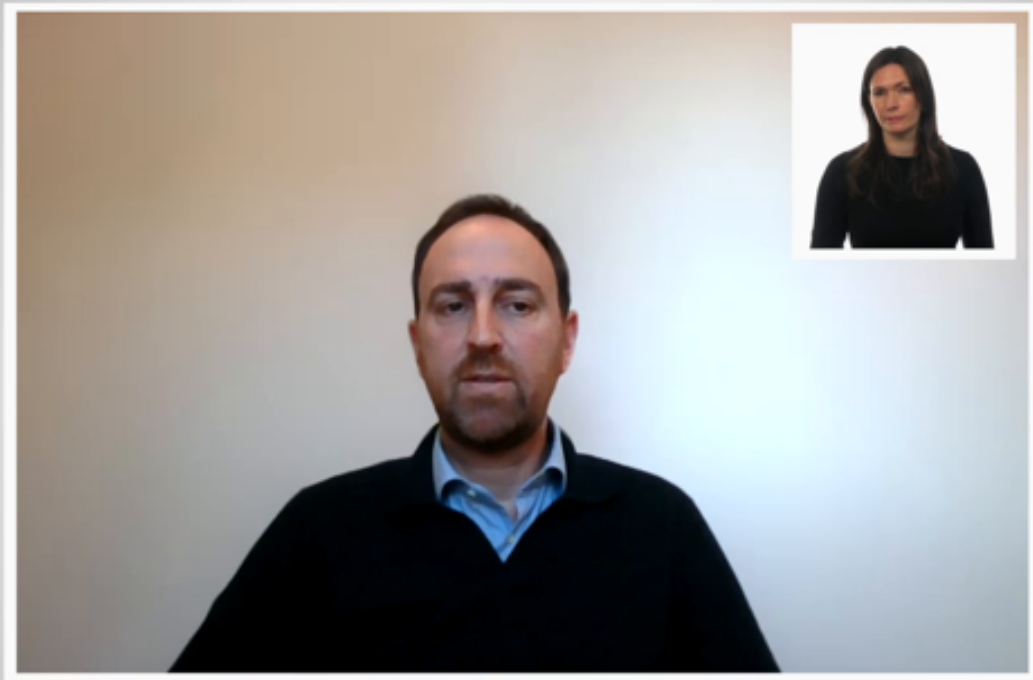
such as cities or displacement camps where people cannot escape and coping mechanisms are non-existent. It is important to note, however, that while we are preparing

notes

summary

6m 37s





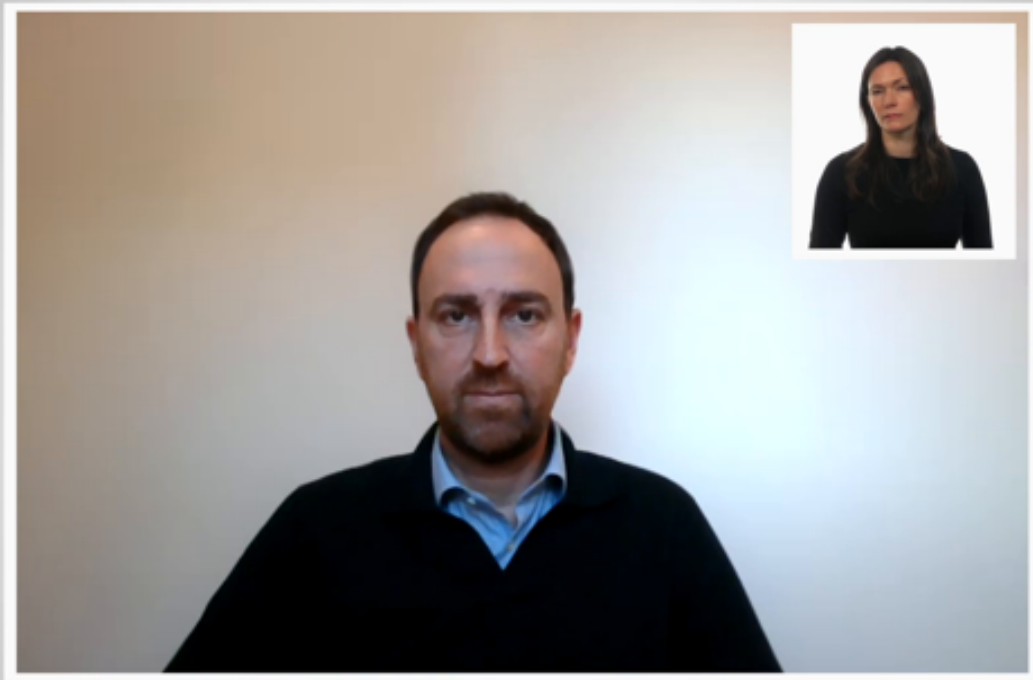
for the challenges posed by digitalization and cyber operations during armed conflict, fact, most of the devastation we witness as the ICRC continues to result from the use of conventional weapons.

notes

summary

6m 49s





Nevertheless, the threat and potential impact of cyber warfare cannot be underestimated or ignored because it is an additional source of risk for ensuring civilians continue to have access to essential services.

notes

summary

7m 1s



Protection and Resilience Strategies



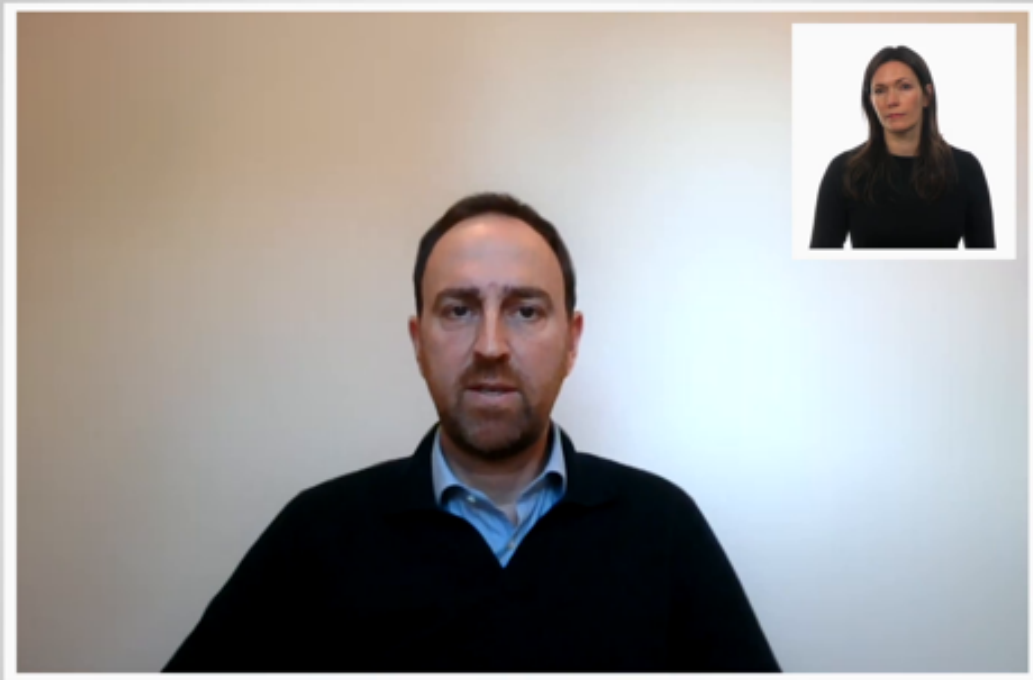
Thanks for walking us through those potential consequences. So keeping in mind everything that you've just shared, what can humanitarian

notes

summary

7m 13s





organisations that support such essential services do to protect them from cyber threats or to increase their resilience to cyber threats? First and foremost, remote operation capabilities should be installed with safety by design from the outset.

notes

summary

7m 25s





Key strategies for Essential Service Resilience

1. Remote operation capabilities should be built on safety-by-design principle.

2. Building in redundancies in systems delivering essential services.

3. Humanitarian practitioners should analyze how the conduct of hostilities impacts the delivery of essential services and assess the actions and behaviors of parties to armed conflict.

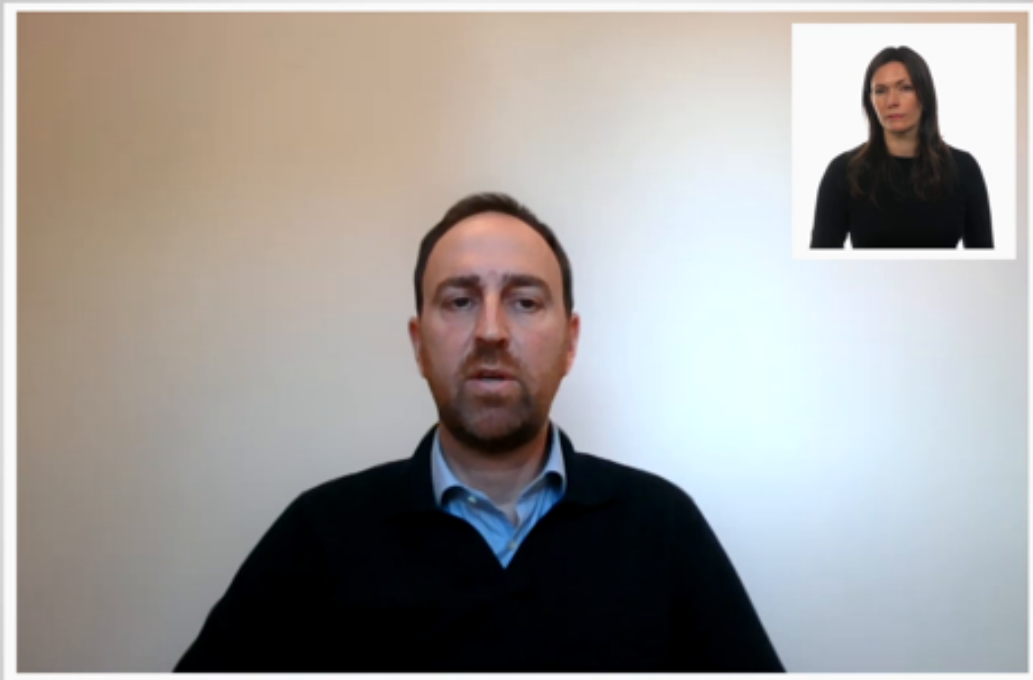
Safety by design is increasingly becoming the industry standard, but unfortunately, not the reality in most essential service systems. Once installed, regular software updates, including, but not limited to security

notes

summary

7m 37s





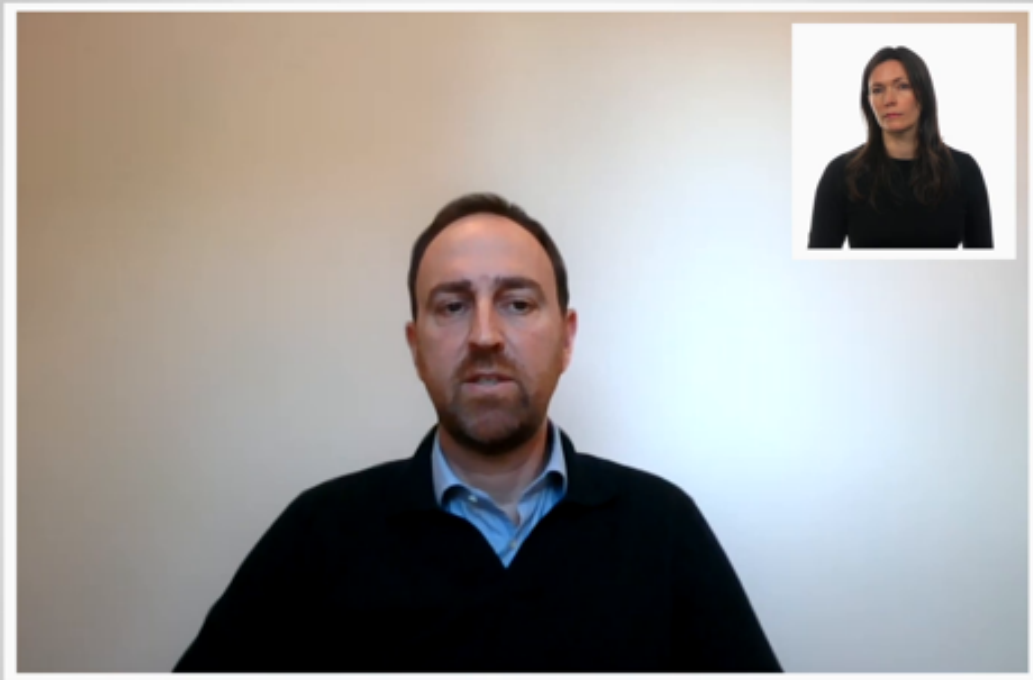
updates, should be done, and service provider personnel should receive cybersecurity training. Mitigation measures to be considered for IT and SCADA systems, in particular,

notes

summary

7m 50s





include, first being able to disconnect services from the Internet. Second, looking at ensuring an ability to operate manually, and third, engaging multidisciplinary teams made up of essential service provider personnel and cybersecurity experts to build in cybersecurity to essential service systems from the outset or during upgrades of existing systems.

notes

summary

8m 1s





Key strategies for Essential Service Resilience

1. Remote operation capabilities should be built on safety-by-design principle.

2. Building in redundancies in systems delivering essential services.

3. Humanitarian practitioners should analyze how the conduct of hostilities impacts the delivery of essential services and assess the actions and behaviors of parties to armed conflict.

Second, humanitarian organisations providing support to service providers

notes

summary

8m 24s





Key strategies for Essential Service Resilience

1. Remote operation capabilities should be built on safety-by-design principle.

2. Building in redundancies in systems delivering essential services.

3. Humanitarian practitioners should analyze how the conduct of hostilities impacts the delivery of essential services and assess the actions and behaviors of parties to armed conflict.

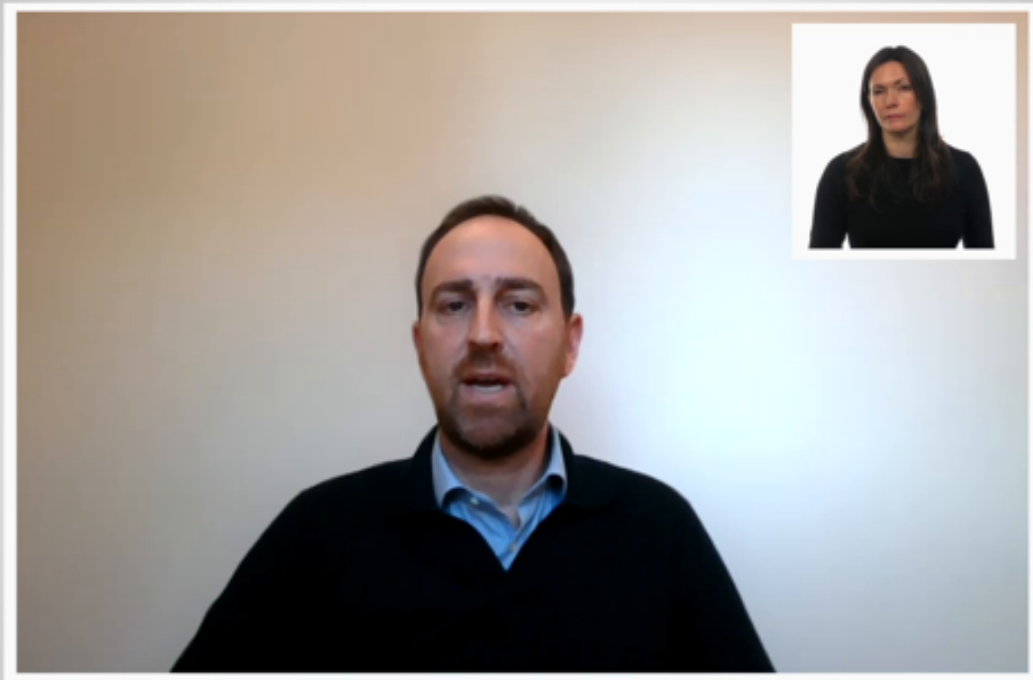
should help build in redundancies or two interdependent essential service systems.

notes

summary

8m 26s





For example, the ICRC often supports the installation of second power supply lines for critical water, wastewater, and health care-related infrastructure

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

8m 37s



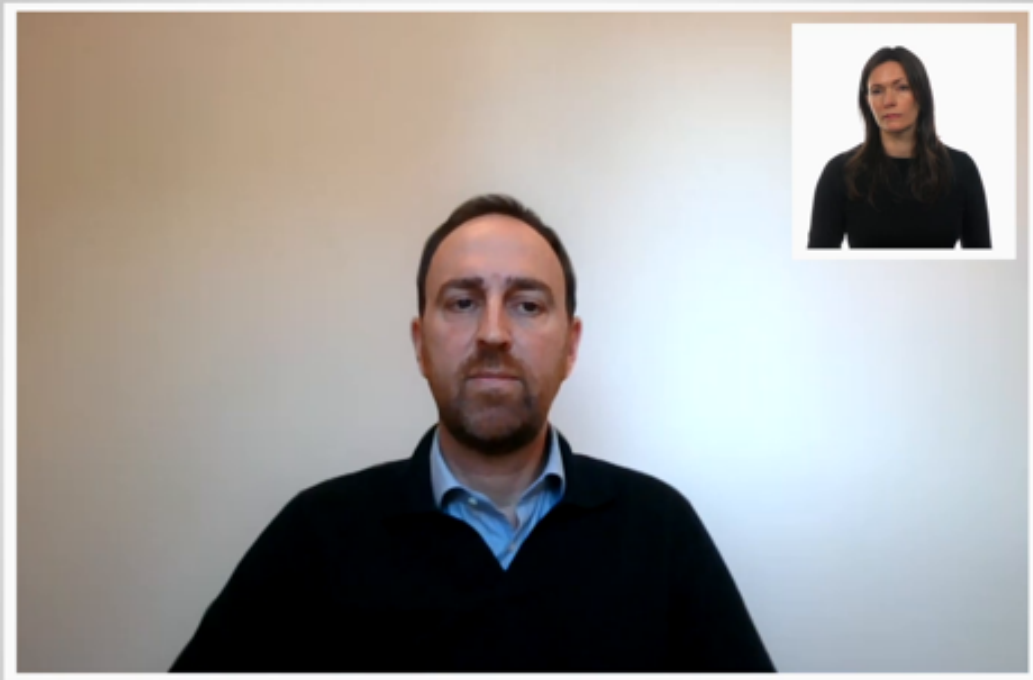
.....

.....

.....

.....

.....



and seeks to diversify the source of power supply used, for example, the combination of grid, solar, and backup generators. This can increase the likelihood that service providers can find ways to ensure the operational continuity and service delivery when a destabilising event occurs.

notes

summary

8m 49s





Key strategies for Essential Service Resilience

1. Remote operation capabilities should be built on safety-by-design principle.

2. Building in redundancies in systems delivering essential services.

3. Humanitarian practitioners should analyze how the conduct of hostilities impacts the delivery of essential services and assess the actions and behaviors of parties to armed conflict.

Third, humanitarian practitioners, technicians, and engineers have a vital role that extends beyond emergency preparedness, resilience building, and assistance.

notes

summary

9m 4s





Key strategies for Essential Service Resilience

1. Remote operation capabilities should be built on safety-by-design principle.

2. Building in redundancies in systems delivering essential services.

3. Humanitarian practitioners should analyze how the conduct of hostilities impacts the delivery of essential services and assess the actions and behaviors of parties to armed conflict.

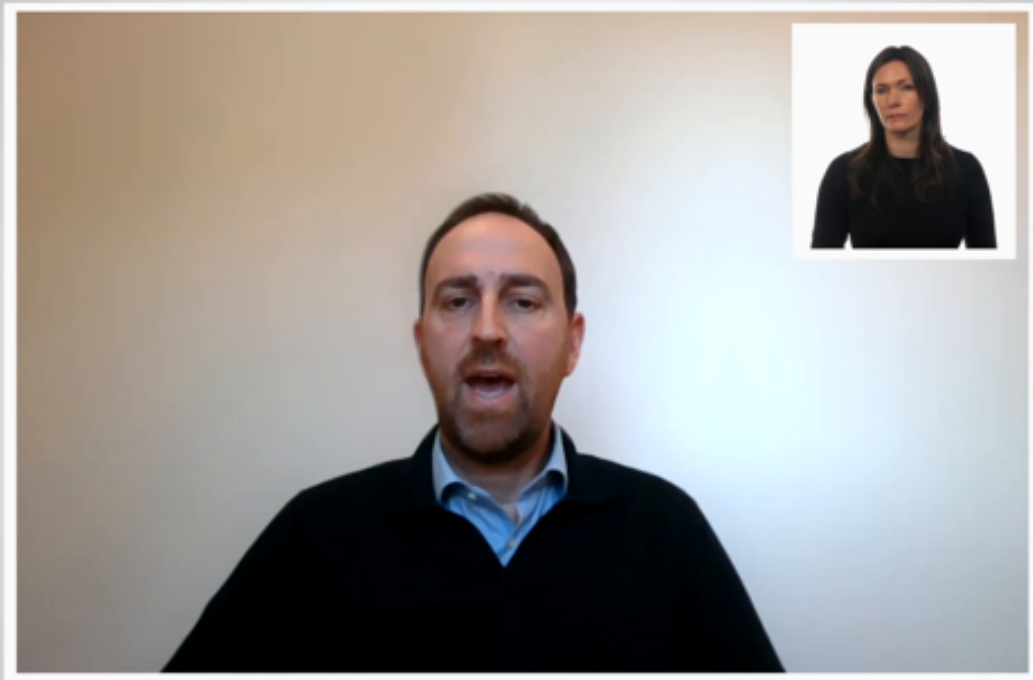
Their expertise are crucial in analysing how the conduct of hostilities impacts the delivery of essential services and assessing the actions and behaviours of parties to armed conflict.

notes

summary

9m 14s





Documenting these impacts and their humanitarian consequences is indispensable, as it directly informs the legal and protection dialogue that organisations

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

9m 25s



.....

.....

.....

.....

.....

Image reference



In order of appearance

PICTURE1 : Picture named Response to Cyber Incidents by VIK from Adobe Stock

PICTURE2 : Picture provided by Cléa Thouin

PICTURE3 : From Metamorworks from Adobe Stock

PICTURE4 : Utility worker by Aimired from Noum Project

PICTURE5 : Picture provided by Cléa Thouin

PICTURE6 : Picture provided by Cléa Thouin

like the ICRC have with parties to armed conflict to prevent or mitigate civilian harm. Michael, you've given us a very helpful overview of the main concerns around cyber operations affecting essential services, and also steps that organisations can take to prevent or mitigate some of the impact. Thanks so much for sharing your insights, Michael. We really appreciate it. Thanks, Cléa.

notes

summary

9m 37s

