WATER AND CYBER SECURITY PROTECTION OF CRITICAL WATER-RELATED INFRASTRUCTURE

Hichem Khadhraoui Director Operations Geneva Call
Online event 17/11/2020

Water as a weapon or method of warfare

A target in armed conflict

- Destruction of water infrastructure
- Poisoning of water
- Incidental harm and lack of maintenance

Water as a weapon

- Flooding
- Cutting off supply

Forms or attacks

- Kinetic or cyberattacks
- State or armed non-state actors

Long term humanitarian consequences

Armed Groups and Cyberwarfare

Advantage is that they are cheaper and easier to carry out than a physical attack with potential immense consequences

ANSAs do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations.

ANSAs conducting cyber warfare would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect.

Armed Groups and Cyberwarfare

Threat posed by Armed Groups against water-related infrastructures

Role of Armed Groups controlling populations and water-related infrastructures

State support and «Transfer of technologies» to Armed Groups

Attribution of an attack to a State or an Armed group could also be a problem when determining the applicability of IHL

Recommandations

Engaging relevant Armed Groups on the humanitarian consequences of cyberwarfare against water-related structures

Pursue dialogue in panels and relevant workshops to include the Armed Groups perspective on the subject of cybersecurity and protection of water related infrastructure