PROFESSIONAL STANDARDS FOR PROTECTION WORK

BY HUMANITARIAN AND HUMAN RIGHTS ACTORS DURING ARMED CONFLICT AND OTHER VIOLENCE

Chapter 8
A PROTECTION APPROACH TO DIGITALRISK AND DIGITAL TECHNOLOGIES

AMNESTY INTERNATIONAL

NRC

HUMAN RIGHTS WATCH

DRC DANISH REFUGEE COUNCIL

Global Protection Cluster

HPG Humanitarian Policy Group

handicap international

humanity &inclusion

OXFAM

IFRC

MEDECINS SANS FRONTIERES

OCHA

InterAction

ICVA
A GLOBAL NGO NETWORK
FOR PRINCIPLED AND EFFECTIVE
HUMANITARIAN ACTION

JRS
JESUIT REFUGEE SERVICE

UNHCR
The UN Refugee Agency

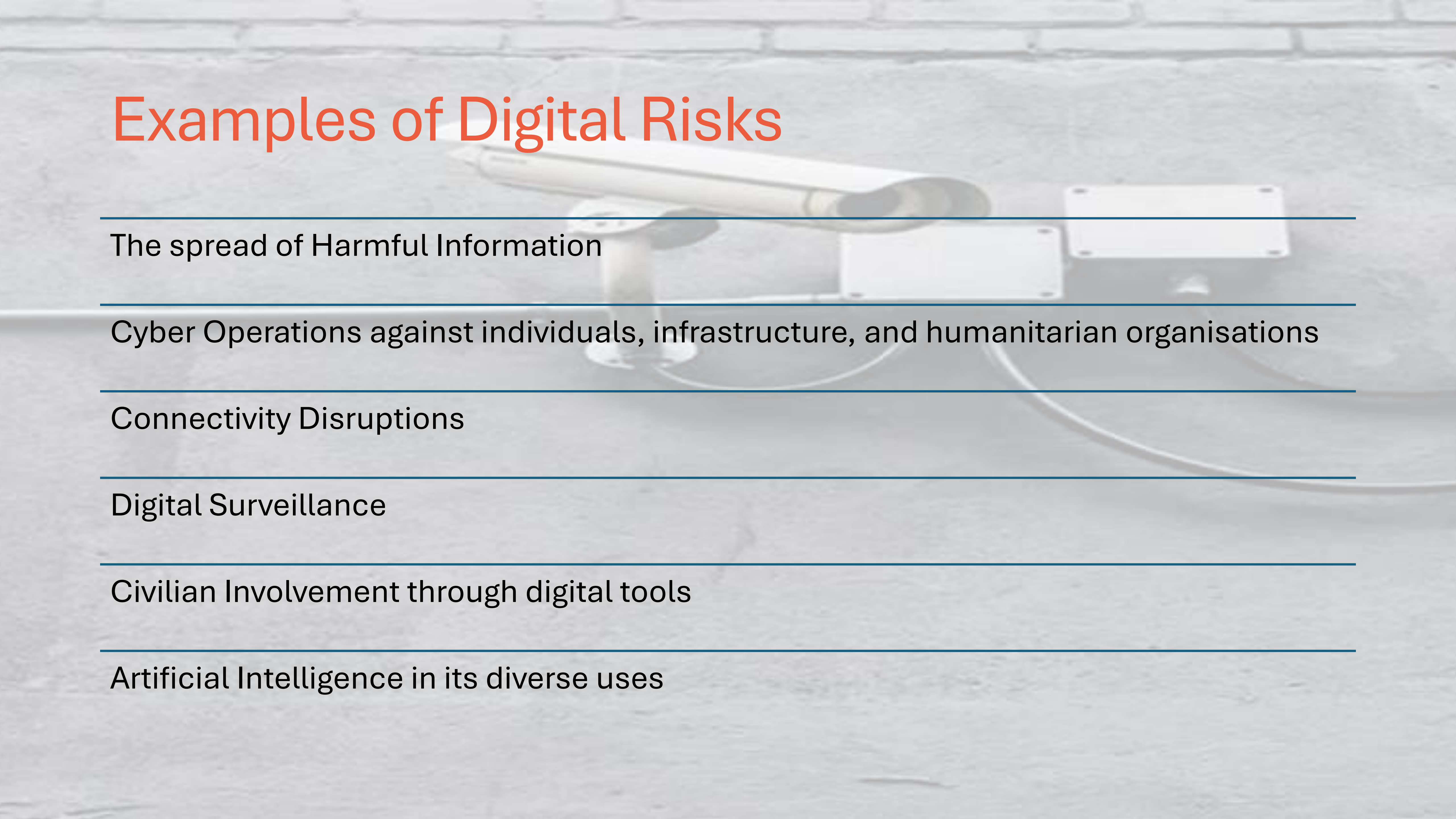
UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

COMITE INTERNATIONAL GENEVE

ICRC

Why Ch.8 on Digital Risks?

Digital Realities



Examples of Digital Risks

The spread of Harmful Information

Cyber Operations against individuals, infrastructure, and humanitarian organisations

Connectivity Disruptions

Digital Surveillance

Civilian Involvement through digital tools

Artificial Intelligence in its diverse uses

Key Concerns – Harmful Information

- Harms to people affected by conflict and violence
- Impact on conflict dynamics, fueling hatred and violence
- Violations of international law (enabling recruitment of children, etc.)
- Undermining protection action; safety and acceptance

Key Concerns – Cyber Operations

- Disrupting, disabling, degrading critical and essential infrastructure and services
- Manipulating, damaging or deleting humanitarian, health or other civilian data
- Targeting people in situations of vulnerability
- Undermining protection response and information

Key Concerns – Connectivity Disruptions

- Access to information and effective warnings
- Loss of family contact
- Disrupting protection work and reporting on violations
- Impacting livelihoods
- Loss of access to some digitally enabled services
- Undermining information integrity

Key Concerns – Civilian Involvement

- Exposing civilians to attacks
- Loss of protection under international law
- Exposing digital infrastructure to attacks
- Increased targeting of civilian entities (more vulnerable to cyber attacks)
- Challenging interpretation of distinction between combatants and civilians

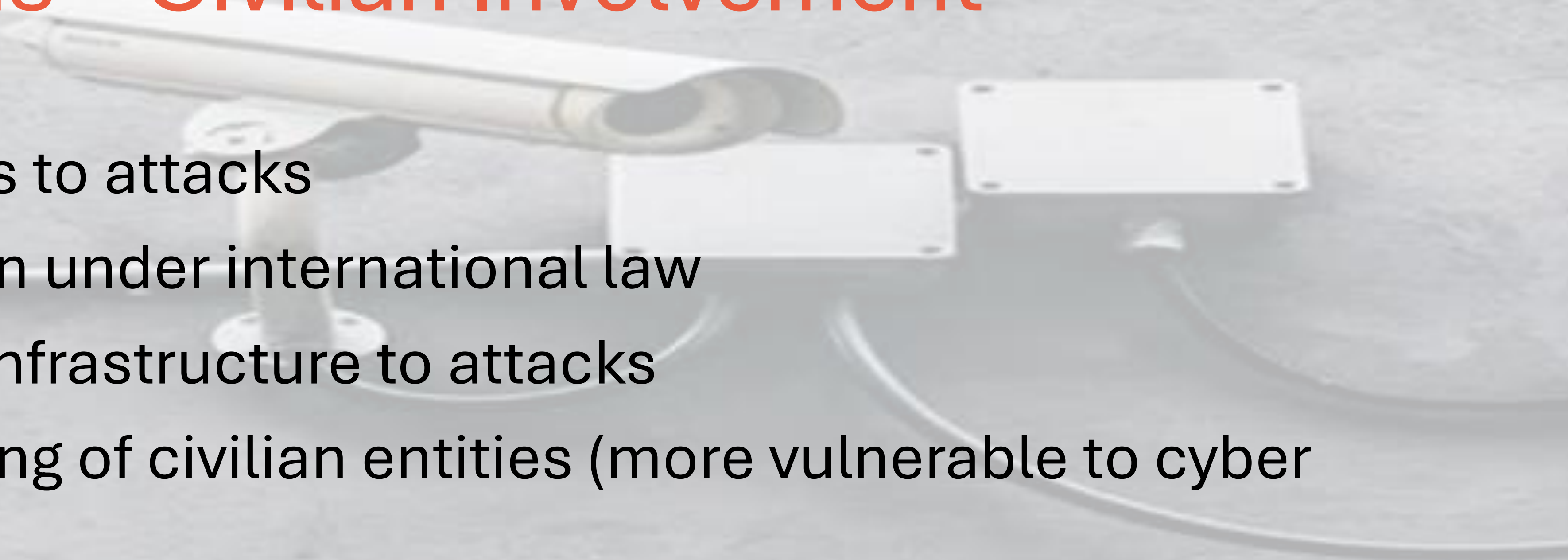
Key Concerns – Digital Surveillance

- Undermining fundamental rights
- Enabling harmful behavior by states, non-state groups and private actors
- Misusing protection data
- Undermining data protection
- Undermining protection work

Key Concerns – Artificial Intelligence

- Premature integration in protection work and community engagement
- Integration in military decision making and targeting and weapons
- Eroding human judgement and control
- Unregulated use in high-vulnerability contexts
- Lack of adequate vulnerability based safeguards in commercial tools
- High risk of abuse of various actors (criminal, armed groups, states, private actors)
- High risk of propagating bias, error, discrimination etc.
- High data protection risks

Key Concerns – Civilian Involvement



- Exposing civilians to attacks
- Loss of protection under international law
- Exposing digital infrastructure to attacks
- Increased targeting of civilian entities (more vulnerable to cyber attacks)
- Challenging interpretation of distinction between combatants and civilians

I. DIGITAL RISKS AS PROTECTION RISKS

Standard 8.1: Protection actors must take all feasible measures to minimize risks that are enabled by digital technologies and might have consequences for the rights, safety and dignity of affected populations

II. A PRINCIPLED PROTECTION APPROACH TO DIGITAL TECHNOLOGIES

RESPECTING THE PRINCIPLES OF HUMANITY, IMPARTIALITY AND NON-DISCRIMINATION

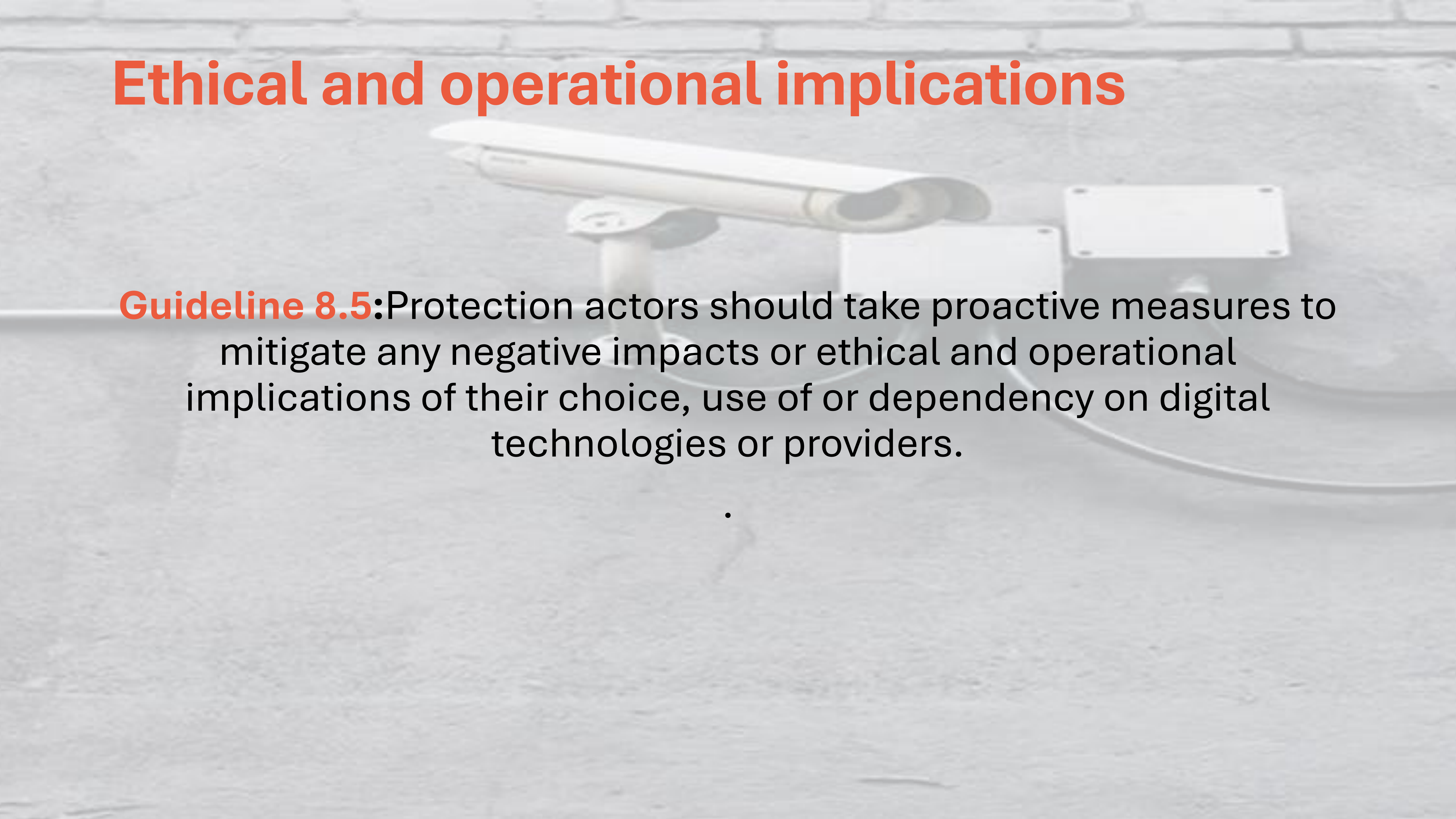
Standard 8.2: Protection actors must ensure the principled delivery of protection action through digital tools and solutions

Do No Harm

Standard 8.3: Protection actors must avoid and mitigate the harmful effects that could arise from the use of digital tools and solutions in their activities.

People-centric and inclusive digital technologies

Standard 8.4:The development and deployment of digital tools and solutions designed for protection action must be people-centric and inclusive.



Ethical and operational implications

Guideline 8.5:Protection actors should take proactive measures to mitigate any negative impacts or ethical and operational implications of their choice, use of or dependency on digital technologies or providers.

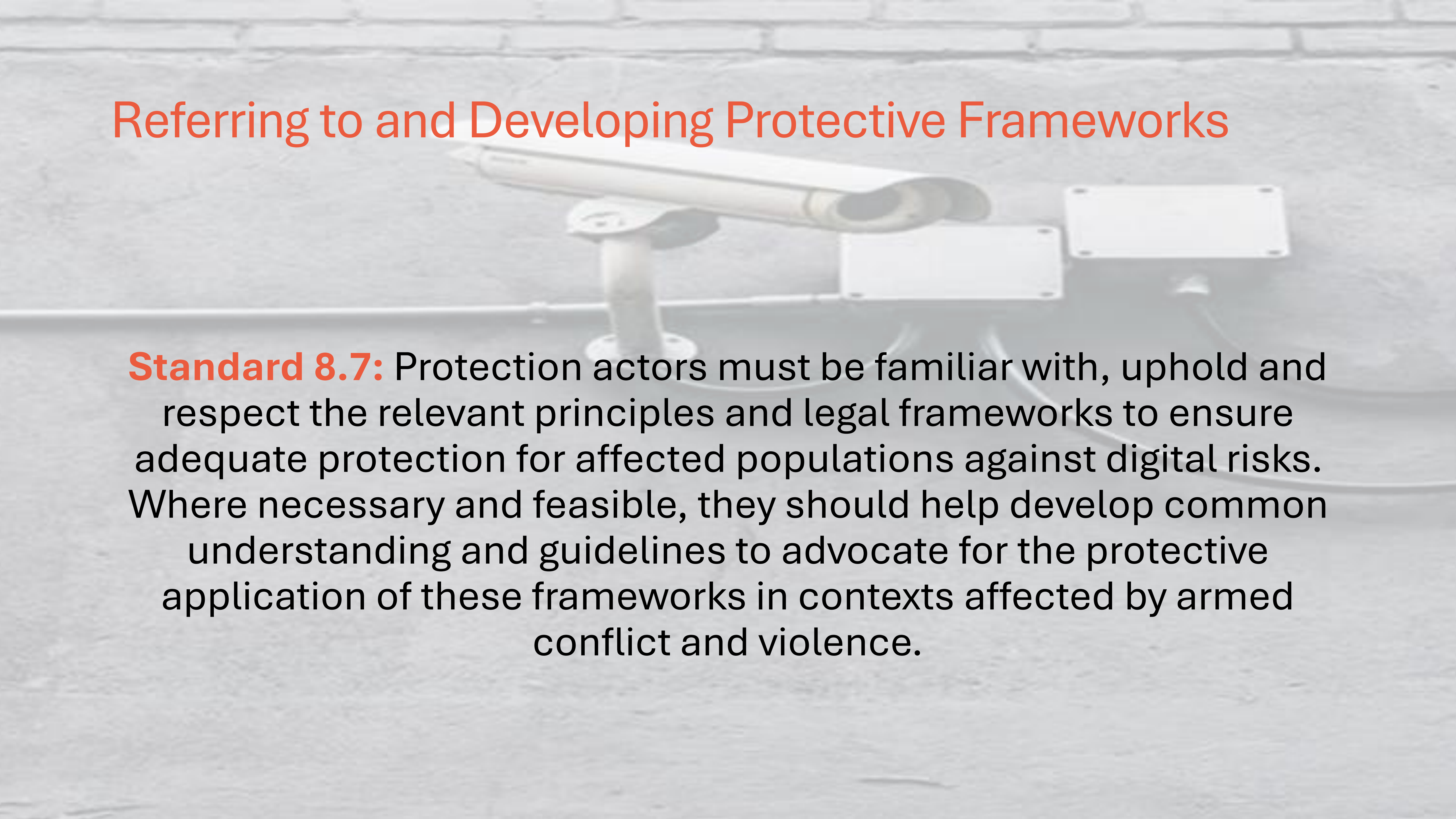
.

III. ENHANCING PROTECTION OUTCOMES IN THE DIGITAL AGE

Integrating digital risks in protection strategies

Guideline 8.6: Protection actors should integrate digital risks and their harmful effects in their protection documentation and assessments. Accordingly, they should include and implement adequate responses and mitigating measures in protection

Referring to and Developing Protective Frameworks



Standard 8.7: Protection actors must be familiar with, uphold and respect the relevant principles and legal frameworks to ensure adequate protection for affected populations against digital risks. Where necessary and feasible, they should help develop common understanding and guidelines to advocate for the protective application of these frameworks in contexts affected by armed conflict and violence.

Engaging in dialogue on Digital Risks

Standard 8.8: Protection actors must engage with relevant actors and establish protection dialogue on digital risks, related protection concerns and rights violations.

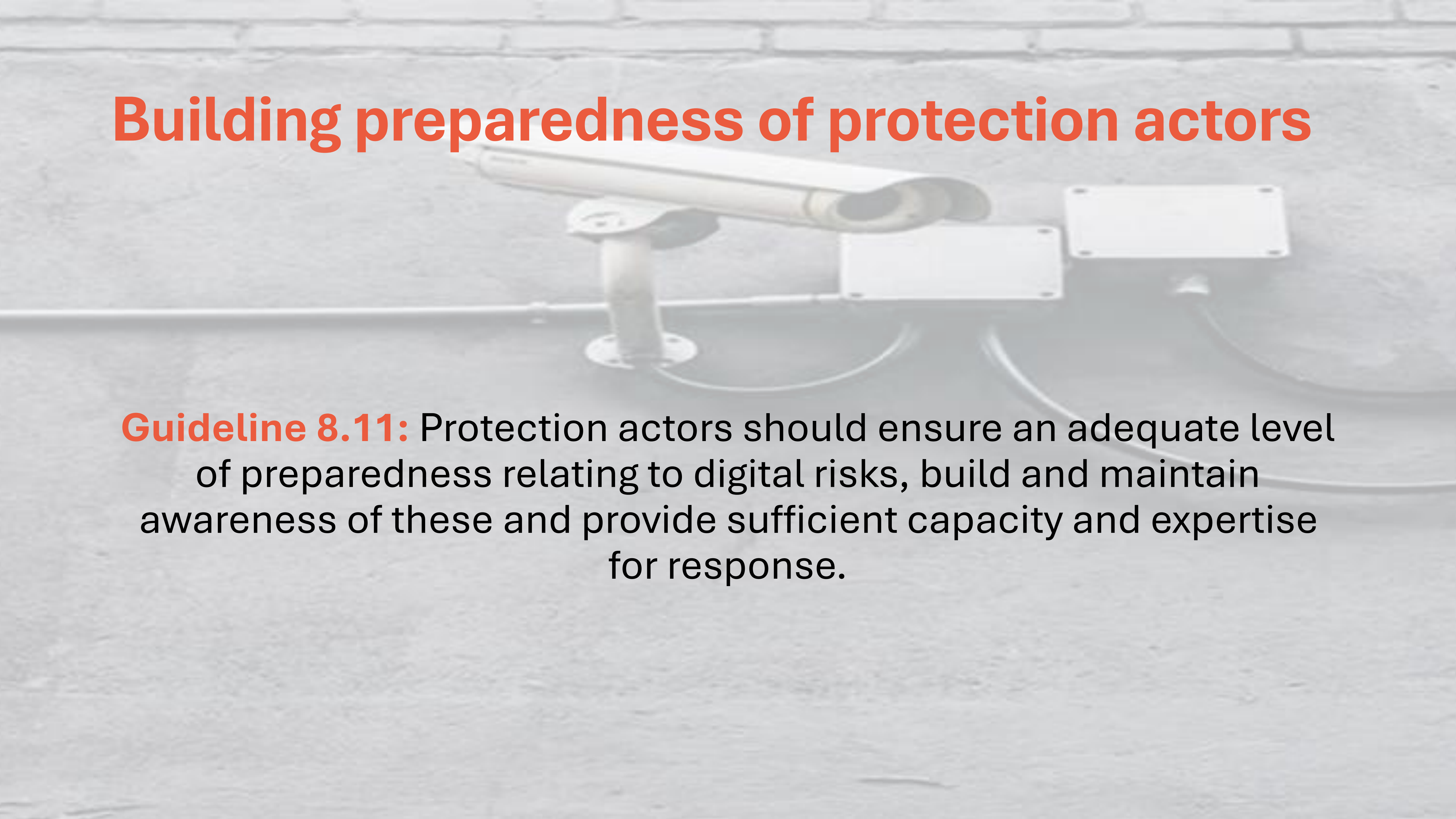
Strengthening affected people’s self-protection capacity and their resilience to digital risks

Guideline 8.9: Protection actors should consistently build upon, support, promote and strengthen, where and when feasible and appropriate, affected people’s capacity for self-protection and their resilience to digital risks.

Ensuring complementarity of protection action in the digital age

Guideline 8.10: Where relevant, protection actors should cooperate with diverse expert stakeholders to complement their own actions to address digital risks

Building preparedness of protection actors



Guideline 8.11: Protection actors should ensure an adequate level of preparedness relating to digital risks, build and maintain awareness of these and provide sufficient capacity and expertise for response.