GPPi

GLOBAL PUBLIC POLICY
INSTITUTE

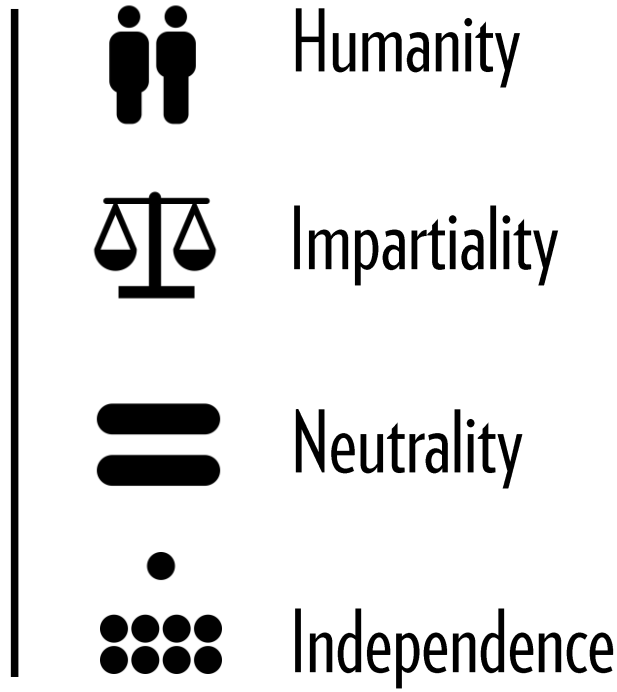
Infrastructure & Humanitarian Issues

Rahel Dette, October 2015
Cyberwar & Cyberpeace, VdW

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

Humanitarian...

... aid and action designed to save lives, alleviate suffering and maintain and protect human dignity during and in the aftermath of man-made crises and natural disasters, as well as to prevent and strengthen preparedness for such situations.

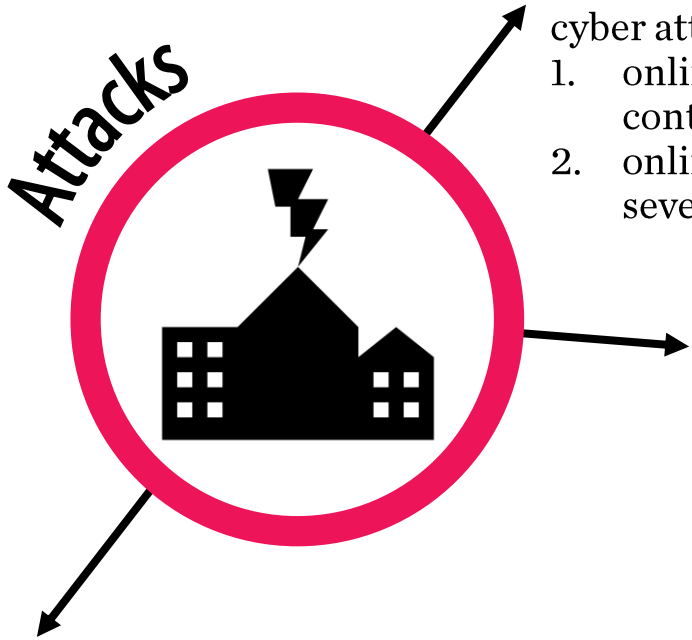


GPPi
GLOBAL PUBLIC POLICY INSTITUTE

This presentation offers five impulses as areas, issues and questions that apply to both:

- the humanitarian impact of cyber attacks or warfare, and
- the cyber strategy of humanitarian organizations.

GPPi
GLOBAL PUBLIC POLICY INSTITUTE



The **Talinn Manual** identifies two types of cyber attacks:

1. online activities used within the context of on-going warfare, and
2. online activities that cause damage so severe that they amount to warfare.

In both cases, **"attacks"** are those activities that cause "injury of death of a person or damage or destruction of objects." Attacks on data count if these hamper the functionality of services and as a result cause said damage.

The consequences of cyber attacks, in other words, clearly would require and fall under the scope of **humanitarian action**. Unlike with the outbreak of civil war, for example, there is little experience with assessing this kind of damage. This relates to both critical infrastructure attacks and other digital strategies.

How do we recognize, and prepare for, cyber-related humanitarian damage?

gppi.net

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

While international experts are considering the legal implications and guidelines for the potential outbreak of cyberwar, the **mandate for humanitarian response** in such an event is not clearly assigned.

Existing humanitarian organizations could be well-equipped to **manage and respond to disasters** where critical infrastructures have been wiped out and basic needs can no longer be covered. They are likely not prepared to respond at large scale to new types and increasing numbers of cyber-related attacks. As technical experts see increasing risks for such attacks, they should engage traditional humanitarian actors to plan preparedness.

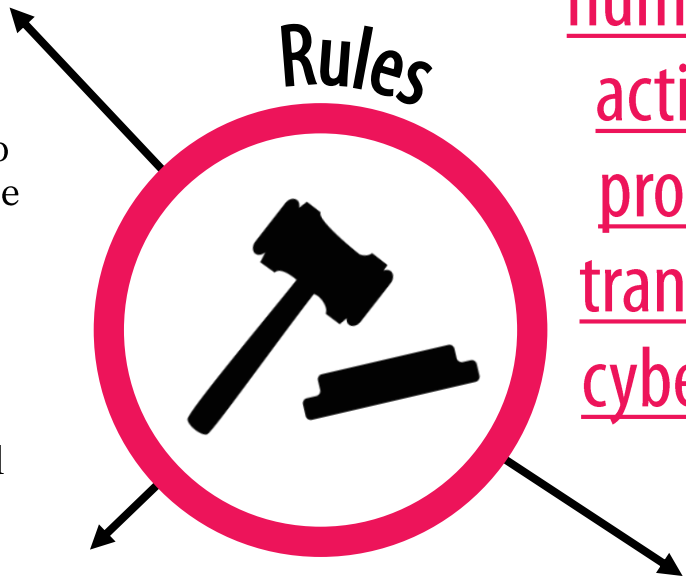
There is also a **technical gap**. Do cyber-related attacks require new types of assistance and protections?

Who is responsible for responding to cyber-related damage?

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

How are humanitarian actions and protections translated to cyber space?

International humanitarian law (IHL) offers guidelines on **legal and governance questions** with regards to cyber warfare. At the same time, IHL and humanitarian response would likely have to change and beadapted to fit the context of attacks and warfare being carried out digitally.



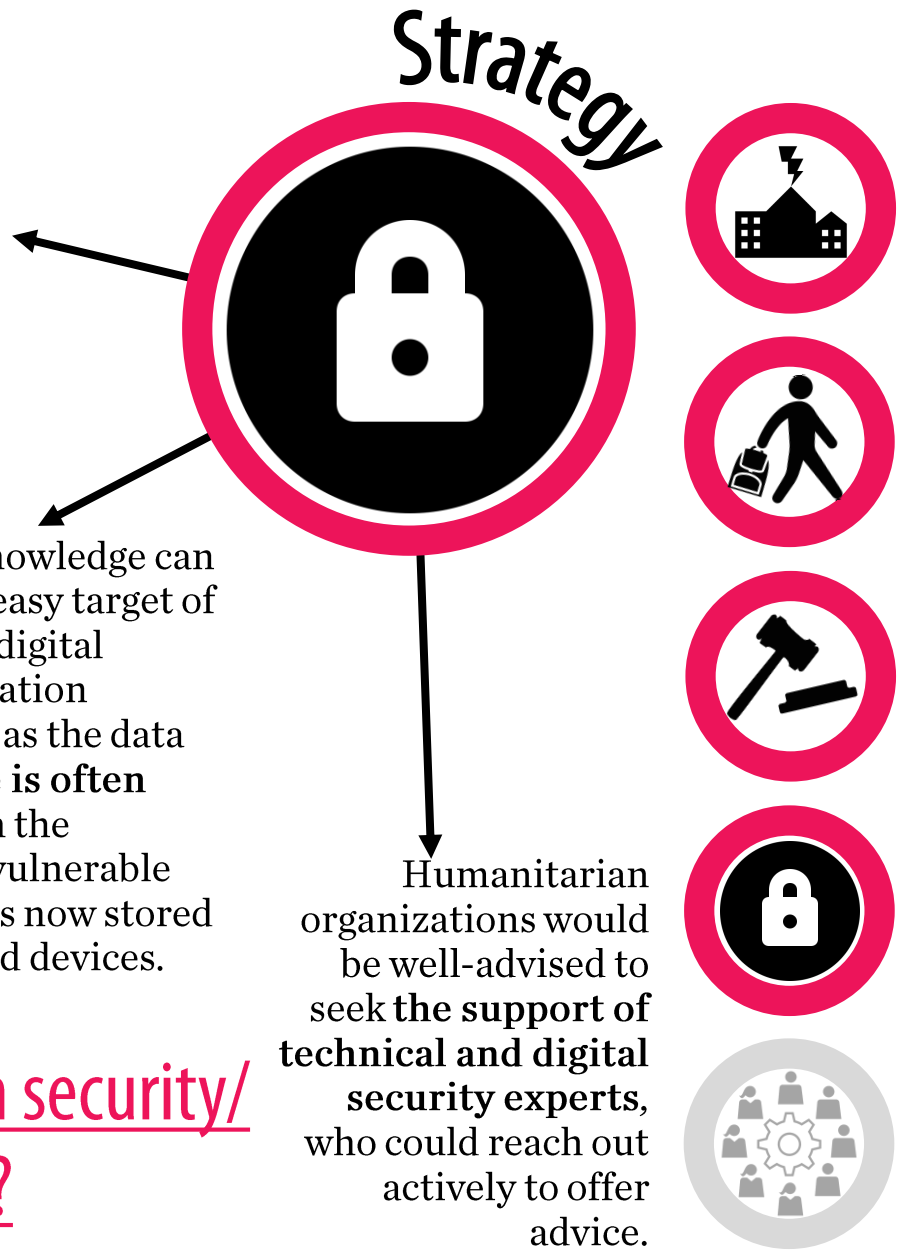
In traditional warfare, it is not permissible to attack hospitals and schools, for example. The Tallinn Manual suggests that same should apply for **humanitarian communications**. Practically, however, how could protected and private communication channels between aid organizations and affected communities be guaranteed?

There are big capacity and knowledge gaps. What would humanitarian response in a digitized context look like? Who bears responsibilities, who sets rules and guards them? More **direct exchange between technological and humanitarian experts** will be key.

gppi.net

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

Most humanitarian organizations right now are not only unlikely to be prepared for the event of large-scale cyber attacks, they also often lack the capacities, strategies and capabilities to recognize and mitigate **existing digital threats**.



The gap in technological and technical knowledge can make non-profits in the public sector an easy target of cyber criminals or those who can exploit digital vulnerabilities of information communication technologies. This can be very dangerous as the data and **information humanitarians handle is often extremely sensitive**, including details on the whereabouts and well-being of the most vulnerable populations. More and more of this data is now stored in the cloud or on unsecured, unencrypted devices.

Humanitarian organizations would be well-advised to seek **the support of technical and digital security experts**, who could reach out actively to offer advice.

What should humanitarian security/ privacy measures look like?

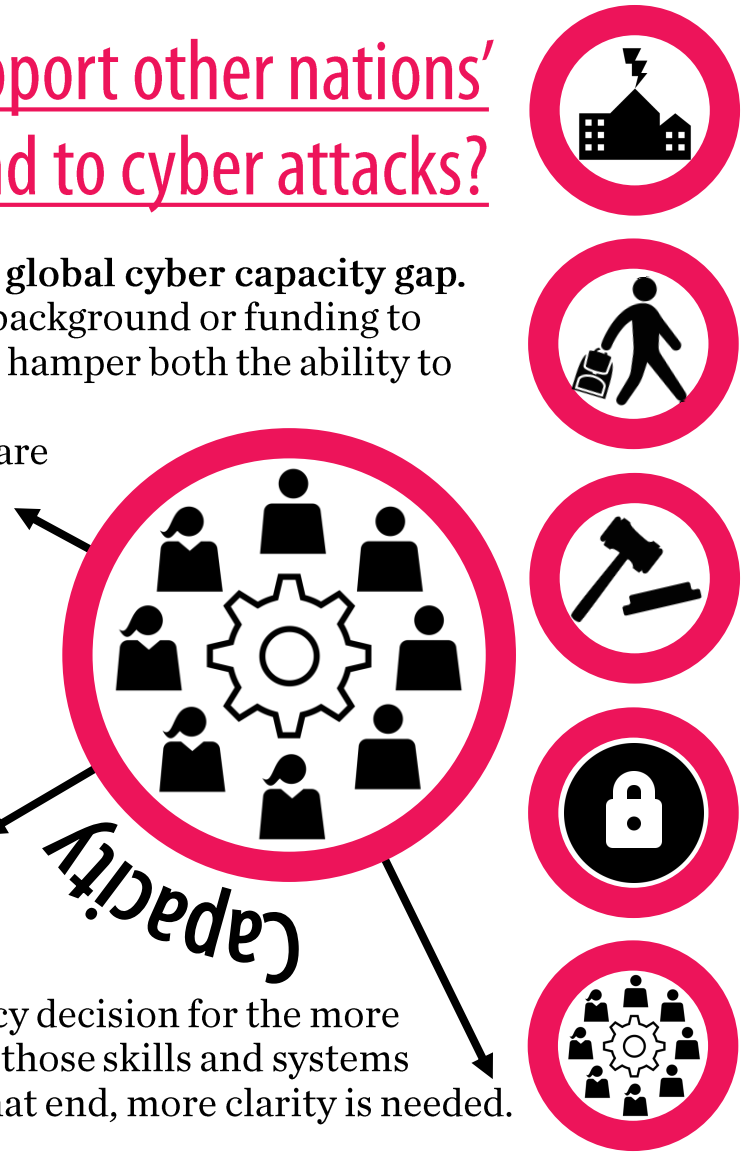
gppi.net

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

How do we support other nations' capacity to respond to cyber attacks?

Another key consideration must be the expanding **global cyber capacity gap.** A number of nations do not (yet) have the ability, background or funding to invest in preparedness for digital attacks. This can hamper both the ability to effectively target cyber crime globally and it can also put to risk precisely those communities, who are already living in insecure or unstable conditions, including humanitarian disasters.

Indeed, in many instances those **militant or organized groups** who might exploit digital vulnerabilities in software or social media may be more likely to target the countries within which they operate before attacking others.



Cyber capacity building represents a difficult policy decision for the more developed nations, however, given the **dual use** of those skills and systems required to provide self-defense capabilities. To that end, more clarity is needed.

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

Cyberwar / Humanitarianism

gppi.net

GPPi

GLOBAL PUBLIC POLICY
INSTITUTE

@raheldette
rdette@gppi.net