HUMANITARIAN INNOVATION GUIDE
SECURITY PRIMER

Security can be defined as the *absence* of threats to the safety, wellbeing and rights of an individual, organisation or community and their assets. The focus should be on both crisis-affected populations and the staff and volunteers of organisations seeking to provide assistance.

An asset is something of value that can be degraded, damaged, lost, destroyed or otherwise harmed. It is becoming ever more critical for organisations to understand that such assets are not only physical, but also digital.

Information gathered regarding any individual has the potential to be misused and ought to be protected from theft, loss, exploitation, distortion and disruption.

Trust within the local community is also a key asset that can enable individuals and organisations to work in an insecure environment.

Insecure humanitarian environments are prone to both conventional threats as well as emerging digital threats, presenting a range of challenges for conducting user research, design activities and pilot tests.

CONVENTIONAL THREATS

Humanitarian contexts – situations of armed conflict, rapid onset natural disasters, epidemics – are often insecure, both for crisis-affected populations and for those who serve them.

Conventional threats include violence, extreme deprivation and human rights abuses, with both vulnerable communities and humanitarian practitioners at risk of:

- Aerial bombardment and the systematic targeting of civilian infrastructure;
- Organised violence, social unrest and criminal activity such as theft and burglary;
- War-time rape and gender-based violence as an instrument of war;
- Chronic malnutrition and/or heightened exposure to infectious and communicable diseases;
- Forced displacement and/or the denial of movement/ safe passage;
- Arbitrary arrest, detention and torture; and
- Human trafficking and other forms of exploitation

EMERGING DIGITAL THREATS

While you will need to pay attention to conventional threats, the humanitarian sector is also learning about the range of new digital threats and vulnerabilities that crisis-affected populations and humanitarian practitioners are facing in fragile contexts.

These tactics are part of a growing arsenal of tools and capabilities that repressive governments, armed actor groups, criminal networks and terrorist organisations have at their disposal to target, surveil, degrade and disrupt civil society organisations they perceive to be hostile to them.

Broadly speaking, there are two types of emerging digital threats:

- **Surveillance, monitoring and intrusion**
  Humanitarian actors and civil society groups operating in crisis environments have become valuable targets for hostile actors who are making use of novel surveillance and intrusion tools to intercept and extract sensitive data on crisis-affected populations.
- **Weaponisation of information**
  Humanitarian actors and civil society groups are at risk from tactics such as targeted disinformation and defamation campaigns, online harassment campaigns, and "DDoS" attacks to take down websites, all of which serve to erode, degrade and destroy operational capabilities.

HIF Humanitarian innovation fund | elrha

hif@elrha.org | higuide.elrha.org | elrha.org/hif | @The_HIF

METHODS AND APPROACHES TO MITIGATE THREATS

In order to operate safely and responsibly in humanitarian environments, you must avoid exposing vulnerable groups, colleagues, partners or other actors to inadvertent security threats through the innovation process, and protect the assets that matter to your project.

To do this, you must (a) understand a potentially very unfamiliar – and rapidly shifting – threat landscape, and (b) devise strategies and approaches to anticipate, mitigate, respond to, and recover from conventional and emerging threats.

In the following section, we provide brief guidance on a number of methods and approaches you might employ, as well as links to recommended further reading.

ASSESSMENTS

Context analysis

Context analysis involves gathering actionable information about the place in which innovation activities are carried out, including:

- Information about the environment, such as security conditions, politics, economics, demographics, social norms and culture
- Information about particular stakeholder or actor groups, such as government, armed groups, UN agencies, NGOs, municipal service providers, or politically, ethnically, or religiously affiliated communities

Threat modelling

Threat modeling is a process of:

1. Defining assets, such as people, data or reputation
2. Identifying how ways of working and information systems affect these assets
3. Identifying potential threats and assessing vulnerabilities (in practice or in systems) that allow the threats to unfold
4. Understanding the impact that adverse events would have on your operations
5. Scenario planning for situations in which threats and vulnerabilities lead to compromised systems, damaged assets and other unintended consequences

This process helps to define countermeasures to prevent and/or mitigate the effect of these scenarios and build out a set of recommendations for responding to the most urgent and consequential risks.

Risk assessment

Risk is a function of probability (the likelihood that an adverse event might occur) and impact (or consequences) of the event in question.

The probability of an adverse event is determined by its prevalence (or frequency) and the vulnerabilities (or weaknesses) in systems or processes that allow it to impact an operation.

The impact of an adverse event is a factor of its scope and scale. Impact on people can be substantial either in terms of the number of people affected, or the degree to which they are affected. Impact on systems can be substantial either in terms of the degree to which a system is affected, or the seriousness of the threat.

STRATEGIES

When it comes to physical security, there are three different types of strategy in insecure environments:

Acceptance – building a safe operating environment through consent, approval and cooperation from individuals, communities and local authorities

Protection – reducing the risk, but not the threat by reducing the vulnerability of the organization (e.g. fences, guards, walls)

Deterrence – reducing the risk by containing the threat with a counter threat (e.g. armed protection, diplomatic/political leverage, temporary suspension)

The security context will dictate the strategy you take, but wherever possible an acceptance strategy should be the first option. If elements of protection are required, then this is the next step. Only in extreme circumstances should deterrence strategies be used.

DIGITAL HYGIENE

RESOURCES FOR YOU AND YOUR TEAM

While ensuring digital security will depend on the context, threat modelling, available resources and the complexity of operational systems, there are seven key areas that constitute an appropriate baseline for digital hygiene:

- Ensure all software is up-to-date with the latest patches and features
- Ensure responsible credentials and account management (eg, using a password manager and two-factor authentication)
- Encrypt and backup hard drives and mobile phones for data storage
- Make use of encrypted communications (eg, emails, instant messengers) and secure file sharing
- Ensure privacy and anonymity when surfing the web (eg, using VPN, Tor, browser plugins and secure search engines)
- Understand best practices for connecting to the internet
- Consider the security of mobile devices, and precautions to take while travelling

There are numerous online resources and guidance materials improving awareness of these issues and advising on appropriate tools. We have collected some of the best ones. We highly recommend consulting these guidance materials and online repositories.

- privacytools.io (n.d.). Available: https://www.privacytools.io/
- Electronic Frontier Foundation (n.d.). Surveillance Self-Defence Toolkit. Available: https://ssd.eff.org/en
- Tactical Tech Collaborative (n.d.). Security in a Box. Available: https://tacticaltech.org/projects/security-in-a-box-key-project/
- Scott-Railton, J. (2017). Digital Security Low Hanging Fruit. Available: https://www.johnscottrailton.com/jsrs-digital-security-low-hanging-fruit/
- Rory Peck Trust (n.d.). Digital Security. Available: https://rorypecktrust.org/resources/digital-security/
- Access Now (2011). A Practical Guide to Protecting Your Identity and Security Online and When Using Mobile Phones. Available: https://www.accessnow.org/cms/assets/uploads/archive/docs/Protecting%20Your%20Security%20Online%20-%20A%20Practical%20Guide%20(design).pdf
- Me and My Shadow (n.d.). Training Curriculum. Available: https://myshadow.org/train
- Me and My Shadow (n.d.). How to Control Your Data. Available: https://myshadow.org/increase-your-privacy
- Reporters without Borders (n.d.) Online Survival Kit. Available: https://rsf.org/en/online-survival-kit

THREAT MODELLING

RESOURCES FOR YOUR PROJECTS AND PROGRAMMES

Please refer to the following guides and tools for carrying out risk assessments and threat modelling:

- Tactical Tech Collaborative (n.d.). The Holistic Security Manual. Available: https://holistic-security.tacticaltech.org/index.html
- European Interagency Security Forum (2017). Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies. Available: https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/
- Internews (2014). SaferJourno: Digital Security Resources for Media Trainers. Available: https://www.internews.org/resource/saferjourno-digital-security-resources-media-trainers