Digital Security as Strategy for Resilience

BRIEF DECEMBER 2020

Digital security as a strategy works to strengthen resilience among Human Rights defenders, activists, civil society organisations and journalists working to advance Human Rights and democracy all over the world.

The online space is an integral part of development cooperation and central in regards to poverty reduction from a Human Rights perspective. Since 2010, internet users all over the world have experienced a deterioration of their rights.[1] Alongside the spread of COVID-19, social, political, and digital landscapes have rapidly shifted and the pace of the introduction of digital tools and practices into our lives has notably accelerated. While many tools and practices represent new ways of connecting, collaborating, or preventing the spread of the pandemic, they also introduce risks of overreaching data collection, expanding surveillance powers, or accelerated digital attacks on people, communities, and organisations. The trends of a shrinking democratic space in the forms of a rise in authoritarianism, autocratization, and attacks on freedom of expression and media freedom affect the safety and security of the environment in which civil society organisations, Human Rights defenders (HRDs) and activists all over the world live, work, and act.[2] Digital security, and awareness thereof, is therefore becoming essential in the work of protecting and promoting Human Rights and democracy. It affects all dimensions of poverty – resources, opportunities of choice, power and voice, and human security[3] – and is relevant to all levels of development cooperation.

This brief focuses on digital security as a strategy and practice that intersects with many aspects of development cooperation. It takes on Human Rights based and holistic approaches to security in general and to digital security in particular. The brief puts forward that digital security as a strategy can have a transformative effect and significantly strengthen organisational and community resilience.

A HUMAN RIGHTS BASED APPROACH TO DIGITAL SECURITY

This brief takes a Human Rights based approach to digital security and defines it in relation to right holders such as Human Rights defenders (HRDs), civil society organisations, journalists, and other communities who rely on information and communication technologies (ICT) such as the internet, in their work and everyday lives. Digital security is an all-encompassing term that includes tools and good practices to protect and secure people, data, information, and assets in the online and offline world, and is an integral part of security in general.[4] In the context of civil society groups, digital security is a measure of an individual or organisation's ability to mitigate risks that exploit vulnerabilities (technical or not).[5] A Human Rights-based approach puts people at the centre of digital security and addresses the technological, social, and legal aspects of security together. The approach promotes trust and security in technologies and practices that reinforce human security.

"People, in particular Human Rights defenders (HRDs), groups that are subject to intersecting discrimination and marginalisation, and journalists, rely on the internet and its availability, integrity and confidentiality to exercise their Human Rights. If the internet is not secure, then their ability to exercise their rights can be threatened, and in extreme cases, their personal security."[6]

(Association for Progressive Communications)

Digital security, or the lack thereof, is intertwined with the protection of Human Rights such as privacy, freedom of expression and of assembly, and the right to information. Different types of online activities concern these different rights in various ways. Unlawful tracking of movements and habits for example, can represent an infringement on privacy. Privacy is essential for the protection of human dignity and the development of self and identity. It is also necessary for the protection of other rights such as the right to freedom of expression, the right to peaceful assembly, and the right to seek and receive information. Using an app to meet up with others to participate in protests, strikes, sit-ins, or demonstrations is an example of how the use of technology relates to freedom of assembly, which ensures the right to gather publicly or privately and collectively express, promote, pursue and defend common interests.

Repercussions for discussing sensitive issues on social media or expressing opinions online, constitute barriers to freedom of expression. Searching or sharing information about a sensitive topic or about a political representative concerns the right to seek, receive, and impart information. Freedom of information, together with freedom of expression are cornerstones to democracy as they enable meaningful participation in public life and social and economic growth.[7]

1 Freedom House (2020) The Pandemic's Digital Shadow.
2 Sida (2019) Democracy in the Digital Age: Challenges and Opportunities for Development Cooperation
3 See Sida Poverty Tool Box for additional material regarding dimensions of poverty
4 Definition from forthcoming complimentary thematic brief Sida (2020) Digital Security / ICT Dialogue Support 2020.
5 Email exchange with Daniel Bedoya Arroyo, Digital Security Helpline Director, Access Now.
6 Association for Progressive Communications (2020) APC policy explainer: A human rights-based approach to cybersecurity.
7 UNESCO Freedom of expression: A fundamental human right underpinning all civil liberties.

A HOLISTIC APPROACH TO SECURITY

A holistic approach to security makes it possible to take into account all interrelated facets of security (technical, legal, physical, psychosocial), and to address them as such. Digital security is connected to all these aspects of security and should be assessed with a holistic mindset that considers risks beyond the online world.

The holistic approach to security emphasizes the need for Human Rights defenders and civil society to engage in self-care in order to protect their physical and mental well-being while conducting their work. Human rights defenders and civil society face both direct or indirect threats to their well-being, including stress and trauma. In this light, the act of engaging in self-care becomes a political act of self-preservation. Well-being and the experience of security is subjective, personal, and varies greatly depending on a number of factors such as previous experiences, beliefs, gender identities.

The Holistic Security Framework

The holistic approach defines security for Human Rights defenders (HRDs) as **"well-being in action"** to position security as an enabler for HRDs to conduct their work. Here, well-being is subjective, gendered and personal, and is the measure of resilience in light of physical violence, but also structural, economic, gender-based and institutional violence, harassment and marginalisation.

With HRDs' increasing reliance on information and communication technologies, digital security and information integrity are vital components of overall security. Protection and awareness measures are integrated with other aspects of security, fostering awareness and use of tools, tactics and strategies to ensure HRDs' physical, psychological, digital, and organisational agency and resilience.

Practicing holistic security also represents a strategy of resilience. Staying safe and practicing self-care while being at risk in constantly shifting landscapes requires attention, risk assessment, adaptability, and agility to mitigate and reduce the threats.

"We should remember that the threats and challenges we face as Human Rights defenders are always changing. In our work, 'unexpected' events are the norm and no single security plan will work in every situation. We need to expect the unexpected and stay 'present', engaged and centred to hone our ability to cope."

(On resilience and agility, from the Holistic Security Manual, Tactical Tech)[8]

FACTORS AFFECTING EXPERIENCE OF SECURITY

Threats can affect people differently, and there are several factors that affect the experience of security in general and digital security in particular. Background and identity affects online behaviour, choice of services, trust in platforms or news sources, and general online activity. Gender, sexual identity, and sexual orientation are key factors in this.[9, 10] Gender intersects with other factors such as ethnicity, indigeneity, age, disability, health, migration, marital or family status, beliefs, culture, social origins, economic self-sufficiency and legal and political frameworks that all serve to mould experiences of security or the lack thereof. Emotional well-being, stress, and trauma also affect how you take to digital security measures.

"The extensive list of digital safety threats women can face [...] often spark fear and mistrust among women and results in them leaving the digital sphere altogether. In addition, this hostile environment also poses significant threats to the freedom of speech and expression of female users."

(New America)[11]

In addition, digital and data literacy affect the experience of security and the ability to develop and employ digital security measures. This includes understanding of how the internet works, awareness of data protection rights, privacy, and awareness of common data collection practices, but also knowledge of what tools to use and how to use them. There is also an increasing need to include media literacy skills into our understanding of data literacy in order to tackle and protect against information distortions such as mis- and disinformation.[12]

"The types of digital and data literacy that citizens need today are complex. They involve not only being able to read and verify news and content, but also, understand the technical and media economics of digital platforms, how they are funded, what their different features and affordances mean and how they function, how to change their privacy and content settings and importantly their individual and collective rights. Digital and data literacy therefore have a strong political, civic and ideological aspect."

(Carmi, E. et al, 2020)

8 See the The Holistic Security Manual by Tactical Tech for more information about framework, strategies, and other resources.

9 See for example Access Now Digital Security Helpline: In 2020, LGBTQ groups are facing more online harassment than ever showing that digital attacks targeting LGBTQ communities are becoming more sophisticated and intrinsically connected to each other.

10 For a more in-depth understanding of how online safety is affected by gender see Sida Thematic Brief (2019) Gender Based Violence Online.

11 See New America (2018) Perspectives and Policies on the Digital Safety of Vulnerable Communities: The Digital Safety Landscape for an overview of digital safety landscapes of youth, women, and racial and ethnic minorities.

12 For a discussion on the definition of data literacy and its definitions see Carmi, E. & Yates, S. J. (2020). What do digital inclusion and data literacy mean today?. Internet Policy Review, 9(2).

The needs of each individual vary greatly based on background and context, but a lack of data literacy in regards to these needs increases the risks and potential harms, whether they be personal, social, physical, or other, and reduces the ability to participate in society.[13]

COMMON DIGITAL SECURITY THREATS

Security threats and attacks come in many different shapes and forms and are facilitated and amplified by digital technologies. Current academic and public knowledge regarding digital security threat relies heavily on reports from private security firms in which civil society threats are underrepresented. A study published in the Journal of Information Technology and Politics suggests security firms produce a systemic bias in reporting on digital security threats, focusing on select types of security threats, such as high end threats to high-profile victims, while neglecting civil society threats.[14] This reporting affects discussions on security threats in academic debate and public policy and also highlights the need to better understand digital security threats, and who is behind those threats, from a civil society perspective. Sida's partner Access Now, has through their Digital Security Helpline observed a number of common threats that present illustrative examples of incidents affecting many of the communities that they support in their work:

- **Phishing and account compromise:** Individuals and organisations from civil society sometimes need to manage sensitive information and data. Adversaries know this and commonly try to compromise online accounts, especially through phishing attacks where they try to trick the victim into sharing valuable information or accepting malicious code by pretending to be a trusted sender.[15]
- **Targeted surveillance and malware:** There is a rise in the use of so called spyware, software able to monitor and listen in on communication and activities, to target civil society and Human Rights defenders.[16]
- **Denial of Service attacks:** Denial of Service (DoS) attacks prevents users from accessing a website or service and are especially common against media organisations.[17]
- **Harassment:** Human Rights Defenders and civil society activists are often victims of harassment in efforts to silence their voices. Online harassment is among the biggest digital threats to LGBTIQ communities, followed by account compromise and censorship and indicate that hate speech on social media is becoming more severe.[18]
- **Censorship on social media:** Adversaries abuse reporting features of social media platforms to take down legitimate content of Human Rights defenders. Removed content might be especially relevant for a small window of time (for example, documenting Human Rights violations during protests) so even if appeal processes to keep the content up succeed, the information will not be available during the time it would be the most relevant.
- **Physical attacks to compromise digital assets:** Adversaries can compromise assets and sensitive information through the confiscation – often without a due process – of devices and assets. In certain environments, this means arresting or kidnapping the victim, seizing their devices and forcing them to hand over their passwords.[19]

For more information on these types of digital attacks and how to protect against them, see Digital Security / ICT Dialogue Support 2020 (forthcoming Sida Brief).

RESPONSE TO DIGITAL THREATS – RECOMMENDATIONS

The report of the Special Rapporteur on the right to privacy lays out a number of recommendations for states and other actors in regards to protecting rights holders from privacy infringements and strengthening their digital resilience. Examples of recommendations to state and non-state actors include, but are not limited to:

- Support research into the right to privacy and gender to better understand the benefits, prevention and mitigation of harms arising from infringements of privacy;
- Introduce effective policies and programmes, with specific attention given to women and gender-nonconforming defenders, that address the risks and systemic and structural discrimination and violence that they experience;
- Ensure the privacy of communications of Human Rights defenders who engage with multilateral institutions and international and regional Human Rights bodies and promptly investigate any allegations of actions to the contrary;
- Ensure that online media are not used to violate the rights to privacy of Human Rights defenders through, for

13 Carmi, E. & Yates, S. J. & Lockley, E. & Pawluczuk, A. (2020). Data citizenship: rethinking data literacy in the age of disinformation, misinformation, and malinformation. Internet Policy Review, 9(2).

14 Lennart Maschmeyer , Ronald J. Deibert & Jon R. Lindsay (2020): A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society, Journal of Information Technology & Politics

15 For examples see the "Doubleswitch" social media attack on advocates in Venezuela and other countries, Access Now and phishing attacks using third-party applications against Egyptian civil society organizations, Amnesty International and independent media and human rights activists from Uzbekistan, eQualitie

16 See for example the Moroccan human rights defenders targeted by malicious NSO Israeli spyware, Amnesty International

17 The Salvadorian Magazine Revista Factum suffered for example a week-long digital attack for denouncing corruption by the president of El Salvador, Qurium Media Foundation and the online newspaper Premium Times Nigeria experienced digital attacks as pressure for an investigate story, Qurium Media Foundation

18 Access Now (2020) Digital Security Helpline: In 2020, LGBTQ groups are facing more online harassment than ever

19 List of common threats and related reports provided by AccessNow, December 11, 2020.

example, the publication of private contact information by a third party, identity theft or threats of sexual violence;
- Ensure that there is comprehensive protection for secure digital communications, including by promoting strong encryption and anonymity-enhancing tools, products and services and resisting requests for back doors to digital communications;
- Support research into digital technologies and the experiences of security of women and the lesbian, gay, bisexual, transgender and intersex community on the extent, causes and effects of infringements of privacy and the harms arising, and on the effectiveness of measures to prevent, eradicate, prosecute and provide reparation for such harm.[20]

STRATEGIES TO STRENGTHEN DIGITAL RESILIENCE

Strategically developing and implementing good digital security practices as an integral part of an overall strategy contributes to strengthening organisation and community resilience and crisis readiness. These practices prove increasingly essential alongside a shrinking democratic space. Having a digital security strategy strengthens and empowers individuals and organisations in their work and well-being. It also promotes solidarity and support among individuals, organisations, communities, and networks. Embracing a pro-active approach to security and strengthening digital resilience can prevent serious security incidents and mitigate their potential effects if they were to take place. Digital security as a strategy can consequently serve as a resource, protecting information and communication as assets and improving long-term sustainability.

While there are initiatives invested in supporting organisations and communities to assess and respond to threats they face[21], digital security strategies are most effective when organisations and communities are themselves invested at every level. This results in stronger organisations, not just when it comes to digital security, but generally, in regards to how they work, how they use technology, and how they communicate, for example. Security strategies should be adapted to the specific political, economic, social, technological, legal and environmental context in which the organisation or community operates, which is best done by the organisation or community itself, operating in that context.

"Bringing groups together to discuss and share perspectives on the risks and threats they observe is the only successful way to ensure security processes are well-informed and tailored to the needs of specific communities."

(Interview with Access Now)

Three categories of security strategies for Human Rights defenders and civil society:

- **Acceptance strategies** involve engaging with other actors (allies, neutral parties and opponents) to foster tolerance, acceptance and ultimately support of Human Rights activities in society. This is often carried out through advocacy, campaigning, diplomacy and education activities.
- **Protection strategies** emphasise learning or implementing new methods and practices which focus on defending the space for work. This can also mean turning to allies for protection and bridging gaps in our existing security practices.
- **Deterrence strategies** focus on raising the cost of carrying out attacks against the organisation or community, be that monetary cost, reputational cost or otherwise. These strategies also depend heavily on advocacy, campaigning, diplomacy and education activities, and require well-developed actor maps in order to know which allies can help raise the cost of attacks.*

(Building New Approaches to Security, from the Holistic Security Manual, Tactical Tech)

* https://holistic-security.tacticaltech.org/chapters/strategise/3-2-building-new-approaches-to-security.html

The human-centred, holistic framework of digital security aims to transform the dynamic from digital being a limiting and threatening factor, to an empowering and sustaining strategy. Digital security may, if implemented without a human rights based approach, have the effect of reducing agency and limiting human rights defenders' ability to act. By incorporating digital security into sustainability strategies, digital means and resources can instead empower Human Rights defenders and civil society organisations. By gaining knowledge, capacity and resources, they are in charge of leveraging these to improve efficiency, reduce risks, and protect their abilities to achieve their goals. This, however, requires work, time, and resources.

"It's hard. It takes resources – mostly time. And we often don't have that time. With time, the board, executive and the staff, and funders too, can take the opportunity to understand how things work within the organisation, the environment within which they work, the range of risks, the ones they are willing to accept, and how they plan to deploy and instil the procedures and policies, and revisit them."

(Interview with Privacy International)

20 List of recommendations drawn from Report of the Special Rapporteur on the Right to Privacy. A/HRC/43/52

21 See for example AccessNow's Digital Security Helpline and CivicSpace.Tech

In order to implement this, donor organisations can strengthen collective ways of protection that further reinforce HRDs' and CSOs' agency and resilience and provide support and capacity through long-term engagements.

COLLECTIVE PROTECTION

"For us, it's all part of the ecosystem. We have to stop separating NGO security as some 'other' and rather see it is part of the larger problem that we must all solve. And this is because we approach digital security like healthcare, it's a common good. It cannot be siloed, as you're only as "secure" as your weakest link."

(Interview with Privacy International)

The responsibility of ensuring the security, safety, and digital security of HRDs and civil society often falls on rightsholders themselves (individuals, groups, or organisations that may be subject to threats, harassment, attacks etc.). Although there is much these actors can do to strengthen their digital resilience and overall security, duty bearers, the state and private actors, are equally responsible of creating a safe, conducive, and enabling environment for everyone involved in the protection of Human Rights.

"Remedial actions to address gender-based breaches of privacy are needed at the international, regional and national levels. Preventive strategies that address the behaviours of individuals alone have been ineffective." [22]

(Special Rapporteur on the right to privacy, 2020, p. 4)

According to the report of the United Nations Special Rapporteur on the right to privacy, current state and non-state actions and responses to infringements of privacy, in particularly based on gender, have been weak and remedial action is needed on all levels. Donor organisations are very well positioned to support policies, organisations, and initiatives that contribute to creating a safe and enabling environment, while also recognizing that digital security can be resource intensive – and costly. In addition, the Human Rights Council emphasizes the role that media organisations can play in providing adequate safety, risk awareness, digital security, self-protection training, equipment, and insurances to journalists and media practitioners, especially when on dangerous assignments or in oppressive environments.[23] Instead of only addressing individuals or individual organisations, there is a stronger call for broader action that includes all actors in regards to the protection of Human Rights defenders and civil society.

Collective protection, such as advocated by Protection International, introduces a shift in focus on the protection of Human Rights defenders from otherwise victimized individuals to instead include all actors involved in enabling a safe a secure environment for civil society and Human Rights defenders.[24]

This includes actors that are enabling, involved in, or responsible for different types of attacks that ultimately may force people offline, as well as legal or regulatory bodies that can do more to protect rights holders and hold attackers accountable. Focusing only on individual protection could undermine attempts to strengthen and protect Human Rights defenders at large, since they are involved in collective processes, networks, and communities working together. The collective protection approach promotes instead an expansion of protection mechanisms.

"The collective protection of human right defenders (HRDs) goes hand in hand with the strengthening of social movements and social fabric."

(Protection International, Collective Protection of Human Rights Defenders)

Strategically building capacity through a holistic approach to digital threats creates resilient and sustainable networks of support to Human Rights defenders. By strengthening rapid responders, local protection networks, and security trainers' capacities or by providing sustainable funding, this contributes to sustainable and long-term protection.[25, 26]

ENTRY POINTS FOR SIDA

Donor organisations are very well positioned to support organisations and rights holders, as well as policies and initiatives that contribute to creating a safe and enabling environment for the protection of Human Rights and democracy. Suggested actions to strengthen digital resilience include:

- Work to empower partner organisations. Ensure that they retain and maintain their own agency (ability to decide and act for their own benefits) by supporting them in building the knowledge, capacity, and resources that they need. Recognize that they are in charge of leveraging these to improve efficiency, reduce risks, and protect their abilities to achieve their goals.
- Provide support and capacity through long-term engagements, foster grassroots, and strengthen collective ways of protection that further reinforce partner organisations' agency and resilience.
- Recognize that the development of digital security strategies and practices require resources, funding, staff, and training, and that it is both time and labour costly processes. Make sure to address this in dialogue with partners, and take it into account in risk and budget analysis.
- Support organisations and initiatives that seek to

22 United Nations Special Rapporteur on the Right to Privacy (2020) Report on the Right to Privacy. A/HRC/43/52

23 The Human Rights Council (2018) Report of the Human Rights Council, Thirty-ninth session A/73/53/ADD.1

24 Protection International, Collective Protection of Human Rights Defenders: A Collective Approach to the Right to Defend Human Rights

25 For an extensive list of mechanisms and organizations see Sida Overview (2020) *Supporting physical, organisational and digital security: Mechanisms and organisations supporting human rights defenders, civil society and media.* Document nr: 044666/20

26 See for example Hivos Digital Defenders Partnership Program (DDP)

empower others in the eco-system to build and cultivate their own digital resilience.
- Support policies and holistic practices that elevate civil society and Human Rights organisations and put them at the center of their work.
- Encourage and facilitate collaboration and knowledge-sharing between networks and communities to promote a collective approach to protection of Human Rights defenders.
- Encourage and facilitate collaboration and knowledge-sharing between states, companies, religious bodies, civil society, Human Rights institutions, professional organisations and individuals to secure the benefits of digital security for all.
- Encourage diversity in perspective in the design, development, and regulation of digital technologies to prevent discrimination, privacy infringement, and other activities that hinder the protection and advancement of Human Rights and democracy.
- Continue supporting secure communication for Human Rights defenders, providing training against online threats, building capacity in advocacy for democracy and Human Rights, and building best practices for improving access to information and the internet for those living in poverty.

FURTHER READINGS AND RESOURCES

Sida: Supporting physical, organisational and digital security: Mechanisms and organisations supporting human rights defenders, civil society and media. Document nr: 044666/20

Sida: Digital Security / ICT Dialogue Support 2020 (forthcoming).

Special Rapporteur on the Right to Privacy: Report on Right to Privacy. A/HRC/43/52 https://documents.un.org/

The Citizen Lab: Targeted Threats
https://citizenlab.ca/category/research/targeted-threats/

The Citizen Lab. (2020). Gender & Digital Security: Results from a Scoping Study https://citizenlab.ca/wp-content/uploads/2020/11/gender-report-v3.pdf

APC: Policy Explainer: A human rights-based approach to cybersecurity https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cyber-security

APC: Why Gender Matter in International Digital Security
https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security

AccessNow: A First Look at Digital Security
https://www.accessnow.org/cms/assets/uploads/2020/10/A-first-look-at-digital-security-OCT2020.pdf

AccessNow: Digital Security Helpline Public Documentation
https://communitydocs.accessnow.org/

CivicSpace.tech
https://www.civicspace.tech/about/

Hivos Digital Defenders Partnership: Digitial First Aid Kit
https://www.digitaldefenders.org/digital-first-aid-kit/

Frontline Defenders: Digital Protection
https://www.frontlinedefenders.org/en/programme/digital-protection

SAFETAG
https://safetag.org/

Tactical Tech: Holistic Security Manual
https://holistic-security.tacticaltech.org/

Art. no.: sida62356en, urn:nbn:se:Sida-62356en Åtta.45 2020

SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY
Address: SE-105 25 Stockholm, Sweden. Office: Valhallavägen 199, Stockholm
Telephone: +46 (0)8-698 50 00. Telefax: +46 (0)8-20 88 64
E-mail: info@sida.se. Homepage: http://www.sida.se

Sida