Organisational Security Community:

Challenges and opportunities for community strengthening

THE ENGINE ROOM

Introduction

The Engine Room conducted community research with the organisational security (orgsec) community between April and September 2019. Working in partnership with Internews, we set out to build our understanding of this community, the challenges they face, and the opportunity for new and updated resources to support them. Specifically, this research fed into the development of a Monitoring and Evaluation (M&E) framework for use by orgsec practitioners and feeds into the re-development of the orgsec.community tools – a listserv and wiki for the orgsec community.

This research sought address the following questions:

1. What is orgsec, and how can we think about impact in this practice?
2. What is the value of community spaces for orgsec practitioners?
3. What opportunities exist to increase the usefulness of the orgsec.community tools?

This community research consisted of desk research and a literature review, attendance at key community events – including the Internet Freedom Festival (IFF) in Valencia and RightsCon in Tunis – and 16 interviews with a diverse group of organisational security practitioners.

This report is a summary of our learning and includes a number of opportunities for community organizing of organisational security practitioners.

What is organisational security?

Definitions

A consensus about what constitutes security and how this is best achieved is emerging in pockets of this community. Hankey and Clunaigh emphasised how the definition of security "should be personal to each Human Rights Defender (HRD)", but broadly speaking, it is about the "enabling the work of HRDs"... "in the face of hostile forces and acts". [1] There is a growing trend towards advocating for long-term engagements with organisations and defenders, considering security in an 'integrated' [2] and 'holistic' [3] way – where digital, physical, legal and psychosocial security are all considered – and a shift away from one-off trainings. That being said, in their 2015 paper in the International Journal for Human Rights, Bennett et al [4] caution against "systematisation and standardisation in protection activities", highlighting the risk that this could lead to a "rigidity and exclusivity" that doesn't match the rapid shifts in the kinds of threats that defenders face or the changes in the way civil society protects and promotes human rights.

Through our community research, we uncovered disparate descriptions and definitions of organisational security, with practitioners using and relating to different languages depending on their geography, background and the communities they support. Common features of orgsec that came through in most of our conversations included the long-term nature of the practice, the focus of building capacity amongst staff and taking a holistic approach.
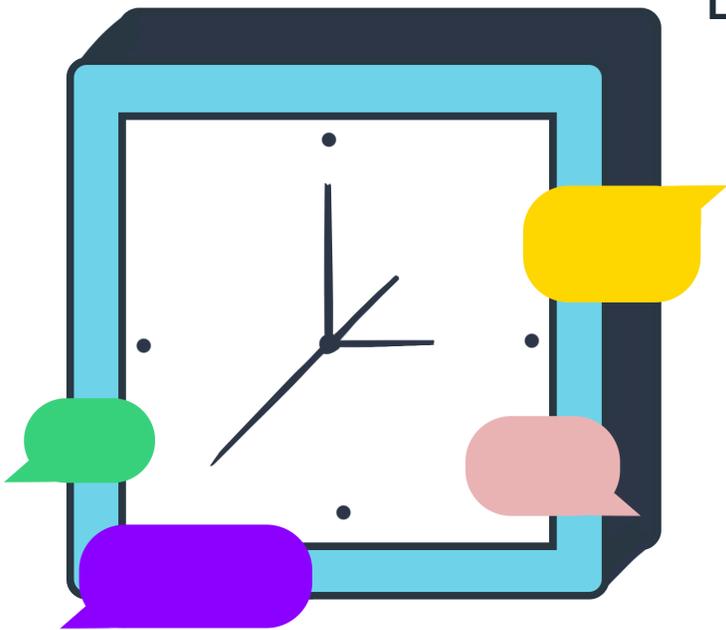
Long-term support

Practitioners described orgsec as working with organisations over months to years, not hours, days or weeks. Across all of our interviews, practitioners shared the view that "long-term support is the only way to make [an organisation] more resilient", with one practitioner emphasising that the first year of your relationship might just be about the organisation "getting ready to do this work." The importance of follow up was also emphasised in our interviews: "Being able to follow up with organisations [is important]; usually, support for organisations ends with the audit or recommendations but for culture change it takes time and follow up." The shift towards longer-term engagements within the organisational security community was also evident at IFF in 2019. Practitioners spoke of the benefits of having more time to get to know an organisation and their context; having a chance to check in with the organisation after making recommendations to help them with implementation, to make adjustments where context has changed. [5]

Capacity building amongst staff

Practitioners consistently talked about the importance of capacity building amongst multiple members of staff in an organisation, where possible. This was felt to be the key to sustainable impact and change within an organisation. In this context, capacity building is not only about looking for changes in the technical infrastructure of an organisation, but also looking for change at the human level. One practitioner summed it up as "both working directly, and working with the staff who will hold the work."

Holistic security

Related to this focus on people is the idea of "accompanying" organisations as an orgsec practitioner, rather than supporting or training them. This subtle shift in language communicates the ideal role of an orgsec practitioner as a facilitator, helping staff in organisations to develop a "deeper understanding or intuition in how to collectively manage and strategise around core organisational processes". Organisational security was seen as a holistic security approach by the majority of our interviewees. One practitioner defined holistic security as "integrating awareness and practices around security – whether that's wellbeing, physical, digital security – within all aspects of the organisation." Such an approach involves considering the people, training, strategy, process, workflows, digital security, budget, policy, staff, travel: "All the things organisations grapple with". This idea is echoed in a collaborative, reflective blog post [6] written by two orgsec practitioners, Slammer and Maya Richman: "So many orgs that I work with do not have written organizational policies. This includes employee code of conduct, conflict resolution processes, communication and storage guidelines. Security and safety is bound to all of that. It's more than just deciding what data to encrypt or an organization's password management. It's about taking care of every part of our work."

"It's about taking care of every part of our work"

The language

However, there was a feeling from some practitioners that the vocabulary and models of support around orgsec are US-dominated. There was a call for more locally specific language and framings: "Both in terms of vocabulary and models it's very US-dominated. I have discussions with Latin American orgsec people. They say 'first we need Latin American models', they feel these US models don't apply." For example, a number of our interviewees pushed back on the language of "security", as it carried negative connotations in a country with a military dictatorship in recent memory. These practitioners use language of safety and wellbeing instead.

Practitioner backgrounds

This community of practice is extremely diverse, both in terms of practitioners' backgrounds and expertise, the kinds of support and capacity building they offer to Human Rights organisations, and the format this support takes. Amongst our interviewees for this community research, we spoke with practitioners with wildly different journeys into this work. People's backgrounds ranged from roots in activism, feminist social movements and social sciences to previous roles in private sector security and computer science – and everything in between.

This introduction from Aspiration Tech summarises this diversity most effectively:

> " *Information security trainers and technology capacity builders who support human rights organizations constitute a broad and multifaceted stakeholder group within the human rights technology ecosystem. Their profession requires uniquely interdisciplinary abilities, from technical literacy, to educational training, pedagogical knowledge, facilitation practice, well developed interpersonal skills, and a deep understanding of social, political and economic contexts. They help human rights workers to build security culture in their*

organizations, and acquire the knowledge and confidence to take control of the technology they decide to use. They aim to provide them with tools to operate sustainably, and with practices that will fortify their stakeholders' rights and safety. "[7]

These sentiments were echoed at IFF in 2019, where practitioners emphasised in multiple sessions how organisational security work is often characterised as a "technical" practice, but that in reality, communication and engagement skills are often more important.[8]

Impactful orgsec

Impact is context-dependent

Although organisational security is a diverse and varied practice, as highlighted previously, Tactical Tech have noted that "the digital security training community is increasingly collaborating, professionalising and exploring new approaches in a more systematic manner than before."[9] This study highlighted the enthusiasm amongst the digital security training and capacity building community for co-developing "a shared body of knowledge and professional standards", which could include a theory of change for the practice as a whole. The need for a collaborative approach in developing metrics of success has been emphasised elsewhere, in order to ensure that they "meet the practical needs and substantive concerns of a diverse community"[10].

The challenges around developing a single theory of change for such a of risk analysis and security practices for HRDs" is entirely dependent on context. Whilst there are tools that are commonly used, including "activity mapping, actor mapping, analysis of security incidents and use of the 'risk formula'

in order to produce an analysis of their environment upon which to base security and emergency plans" [11], practitioners will use these tools in different ways, at different moments and with varying levels of rigour depending on the context. As the authors highlight:

> **"The logic of such an approach is quite clear: there is no 'one-size-fits-all' approach to security, and no trainer should prescribe arbitrarily 'secure' measures, since the development of appropriate security measures requires a profound understanding of the set of forces contributing to the risk level of the particular HRD or organization concerned." [12]**

This sentiment was echoed in our community research interviews, where practitioners talked of the need for a nuanced and flexible approach. One practitioner described the difference between best practice in an organisation with "established, well developed organisational processes with a clear management structure" and another organisation where there is "no capacity to deal with a risk assessment", in which case, providing "obvious assistance (such as switching to licenced software)" might be more appropriate. Another practitioner talked about the importance of understanding the historical context. For example, in Eastern Europe where there is a "history of surveillance, and an acceptance that this will continue, getting people to be more critical is already a plus." Another interviewee summed it up neatly: "There are lots of different routes to impact. What works with one organisation doesn't work with others."

The context-dependent nature of organisational security practice was also highlighted in sessions at IFF in 2019 [13]. Even the outputs of a security audit can vary, including the length of a report. For some organisations, a two page summary might be the best approach, where you know the staff have limited capacity to engage with detailed recommendations. For other organisations, a 30-page report would be more appropriate.

## The importance of civil society organisation (CSO) buy-in

Whilst acknowledging the context-dependent nature of orgsec, from our conversations with a diverse group of practitioners, CSO buy-in and ownership emerged as a key enabler for impact that was relevant and worth striving towards in most, if not all, situations.

The importance of CSO buy-in and ownership is related to the focus on capacity building mentioned previously. Ensuring that the organisation prioritises security increases the likelihood of sustained impact with an organisation. This could look like:

→ **One or two staff members seeing security as part of their role** - "Who is the person who's responsible [for security] in the organisation? There has to be someone. Someone who feels 'this is my job'."

→ **Work to make sure organisations understand the reasons for prioritising security** - "[T]he 'Why' is important.... I'm unlikely to follow a cumbersome policy if it's not justified... Digital security... it is quite cumbersome. The more our partners understand why we're asking for this... what it can do for them - the more likely they are to follow it."

→ **Seeking buy-in from senior leadership** - "Getting the director on board... has long term impact - it becomes a priority."

Barriers to effective support

Our conversations also highlighted some consistent barriers to practitioners providing effective support. These barriers include high staff turnover within CSOs and a lack of capacity or resources within CSOs to prioritise security. These barriers were seen to be more structural and outside of practitioners' control, and could be priority areas for funders and other intermediary organisations to address.
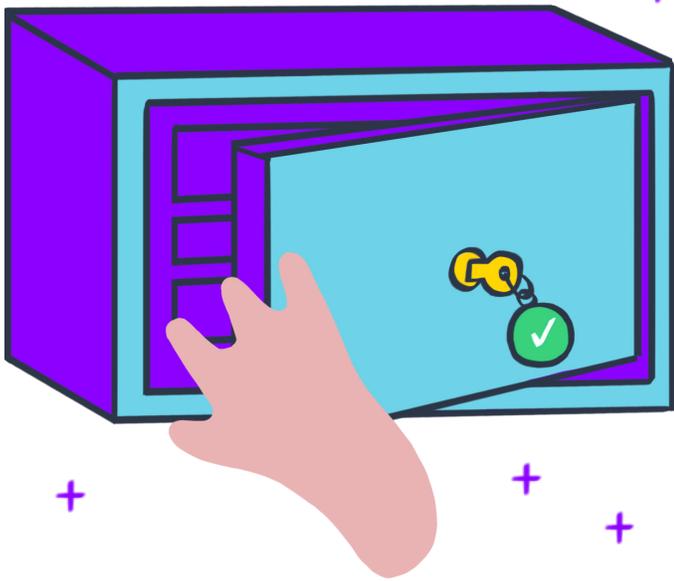
High staff turnover within CSOs poses a major challenge for practitioners. You invest time, energy and resources in building the capacity of staff in an organisation, but when those staff move on, they take this new understanding and skill with them: "This is the conversation we've been having with the partners: I say 'I know this organisation already trained you and your staff, why is there no policy in place?' … And they say, 'All the staff they trained have quit'".

Although the idea of finding individuals within organisations to "champion" security speaks to the importance of CSO ownership, described previously, this approach does leave an organisation vulnerable to knowledge loss: "Orgsec is very dependent on... a champion who spearheads it in the organisation... when you leave, and the champion leaves, this is problematic."

CSOs not having the capacity (time, mental, energy, financial) to engage with the process is another barrier to effective orgsec practice. Particularly for small or under-resourced organisations (which is increasingly the case within civil society), there are often more urgent priorities: "You're fighting an uphill battle – people are completely stretched. They don't have large budgets. They can't hire an infosec officer if they have three paid staff. If there are 30 paid staff, they're doing the work of 60 people. They have little time and other more pressing priorities. For example, dealing with a funding proposal always comes first."

Assessing the impact of orgsec support

Given these findings, there are a number of important considerations to bear in mind when designing an approach to monitoring and evaluation, or impact assessment, within orgsec. The approach needs to cover a wide range of indicators to account for the varied and holistic nature of orgsec support; the interface needs to be simple so that busy practitioners can engage in a way that doesn't take them away from the work itself; and the approach needs to account for the varied contexts in which this work happens.

Although some best practices have been developed in the org sec community, there has been no comprehensive evaluation of org sec methods to determine their effectiveness. It's clear that human rights organisations need support and that org sec must be effective on some level, but there are questions around level of impact and how to increase impact, especially when resources are limited. The Engine Room worked with Internews and several practitioners from various backgrounds to design a monitoring and evaluation framework that org sec practitioners can use to measure the impact of their work.

"there has been no comprehensive evaluation of orgsec methods to determine their effectiveness"

By building a deeper understanding of the impact of their work, practitioners can focus on what works in different contexts, refine approaches to increase impact and convince funders to invest in org sec. Presenting evaluation as an essential part of the support process can help organisations see the value of understanding the ways they are improving and where any gaps remain. This framework is designed to measure changes in organisational knowledge, attitude, behavior and condition, giving a clear and comprehensive picture of the achievements and solutions practitioners enable. It is a blueprint for how change can happen.
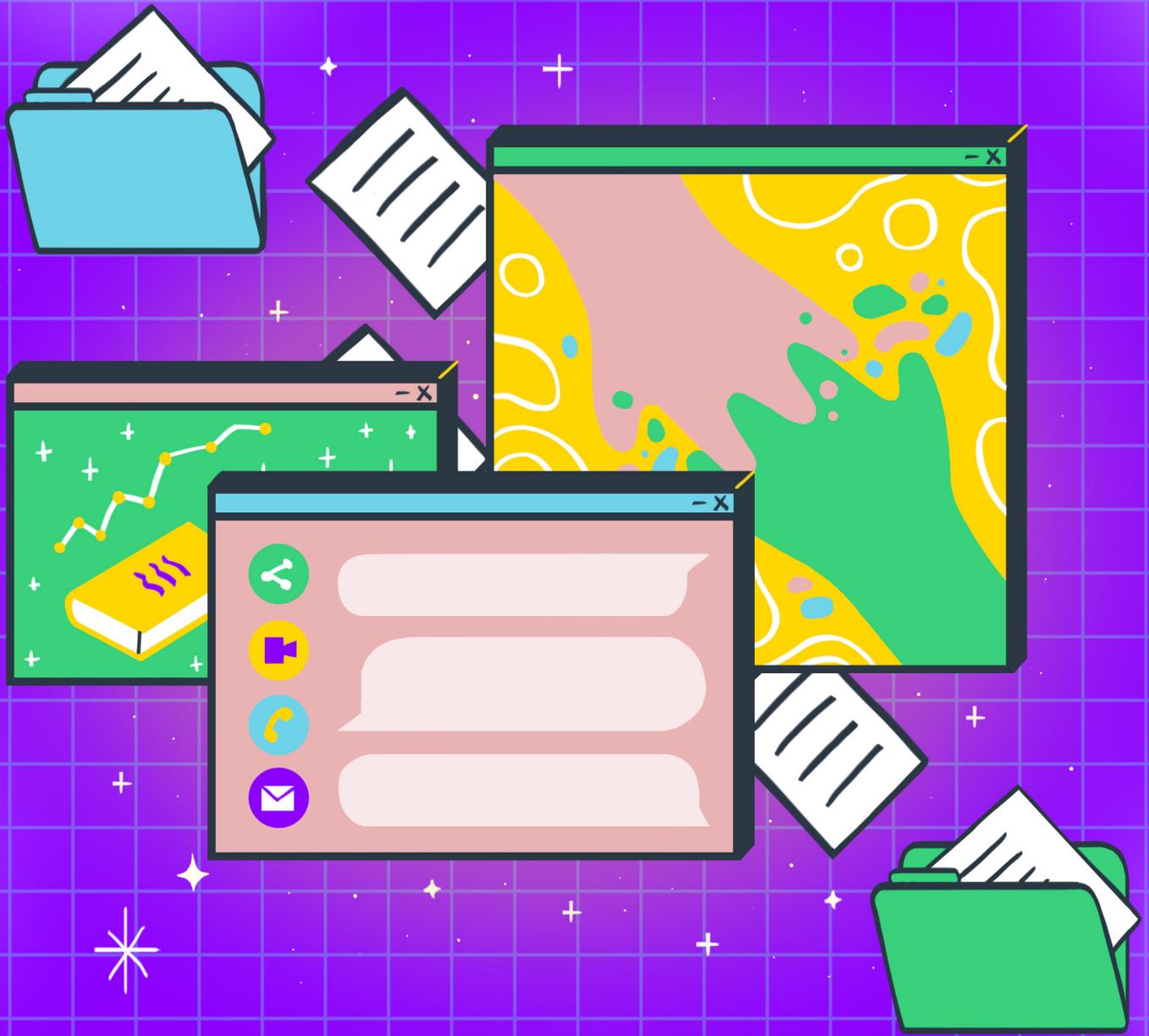
The value of community spaces in orgsec

Across the literature, and in community events, the collaborative nature of this community, and the thirst for more opportunities to connect with and support one another was evident. Tactical Tech speak of "enthusiastic support for the emerging environment of collaboration and coordination amongst the wider digital security training community". In their research[14], they found that practitioners felt the impact of being part of a community was manifold – it results in perceived increases in the quality of the work they do through being exposed to new principles, methodologies and approaches. Practitioners can learn more quickly, itself a form of harm reduction as the alternative is learning "through trial and error", which surely comes at a great cost to HROs and requires a large investment of time. Connecting and collaborating also helps practitioners to feel less isolated.

There are multiple networks of security practitioners that coordinate collective efforts to create and improve methodologies and resources. Aspiration Tech's research highlighted the fact that "the creation and cultivation of in-person and online spaces for security practitioners to meet and interact has helped them to build and strengthen trusting relationships, and has provided channels through which to share knowledge and skills, and most importantly support one another"[15].

Practitioners have highlighted a need for spaces dedicated explicitly to knowledge and skill sharing[16], including more opportunities for connecting and collaborating across disciplines – between psychosocial, legal, physical and digital security practitioners.[17]. More consistent documentation and reporting of incidents, threats and learning has also been highlighted as one way of facilitating knowledge sharing amongst the community [18].
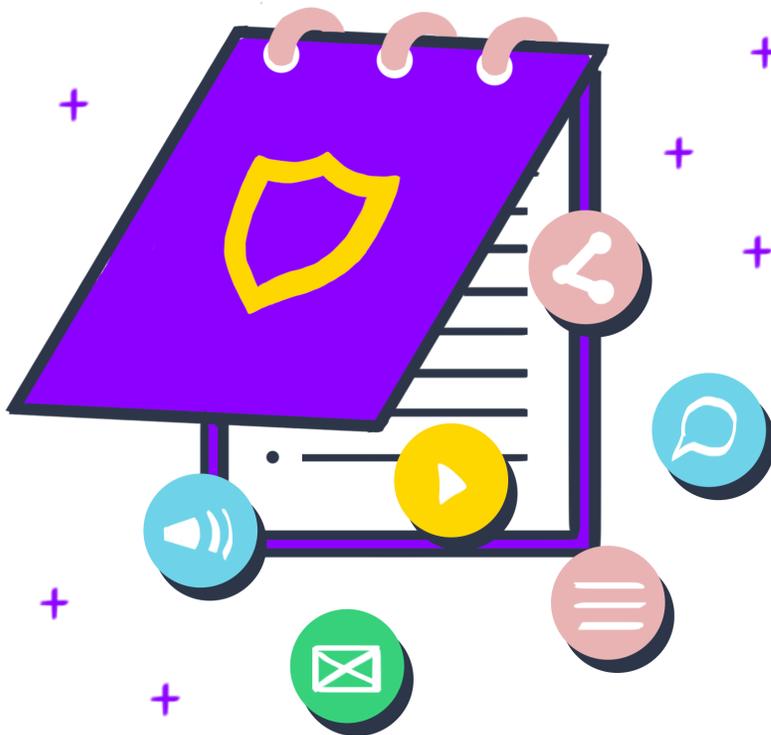
In Aspiration Tech's research, peer-to-peer mailing lists were seen by practitioners to "hold space for remote and asynchronous discussions between folks living in very different geographies. Interviewees indicate these lists as their preferred and most trusted sources of information and peer learning online."[19]. They also found that "Community-designed, community-led, and community-owned" efforts around community building, collaboration and learning were seen to be more effective than those imposed from the outside, or by funders.[20]

Our interviews with practitioners supported these ideas and helped to frame the value of community into two broad buckets: one around increasing and strengthening relationships, and the other around sharing knowledge and skills.

Forming and strengthening connections

Where community spaces exist, digital and physical, practitioners can:

→ **Connect with each other**
→ **Build and strengthen trusting relationships**
→ **Support one another and feel less isolated**
→ **Become more resilient as a community**

These community spaces are critical for forming connections, which deeply impact the quality and safety of orgsec work. For example, as a newcomer to this space, it can be difficult to learn about the nuances around language and framing in civil society. Having access to a community can facilitate and accelerate that learning process. Community spaces also offer an easy way

for practitioners to identify their peers. As one practitioner put it, "Who are our peers? The world of digital rights is so diverse it is hard to know who my peers are".

Practicing orgsec openly can also be dangerous in certain regions, which adds another layer of complexity in connecting and participating in community spaces: "We hide from the evil, but also from each other, so it's hard to find each other". Increasingly, orgsec practitioners work independently as contractors or consultants, often being the only practitioner offering support to any given civil society organisation. Another practitioner said, "It's causing a lot of emotional exhaustion for practitioners. Feeling individually responsible for many different groups, you can't tap out. It's so much pressure to feel like you need to know everything for a group. If you get it wrong, you could really harm them." A diverse and strong network can also increase the resilience and sustainability of this community. As one practitioner put it: "We have certain adversaries – government, the private sector – these people will always be there. They will be more powerful, [they have] more resources. How can we guarantee our continuity? How can we withstand these changes?"

"We hide from the evil, but also from each other, so it's hard to find each other"

Learning and growth

Within community spaces, practitioners can also:

→ Share knowledge, threat information and skills
→ Collaborate across disciplines
→ Learn faster and improve the quality of their work

The value of an international orgsec community is in connecting people working internationally, or in different contexts, to surface and debate different techniques. "To learn about different perspectives and experiences – these are gems for me!" In sharing learning across regions, "best practices", concerns and information can travel faster, reducing wasted effort across the sector in learning the same lessons again and again. "If there could be an online forum, where we can also share skills, interface with other orgsec practitioners to share skills and challenges. I don't know if there is any". As practitioners work independently, and don't have access to personal or professional development opportunities that being part of an organisation can provide, peers can provide that support, and allow one another to feel more confident in their approaches. As one practitioner said: "It brings me back to Earth, to be more certain, to move away from the doubt".

As another practitioner mentioned, "I've always been alone working with an organisation. A platform or list could be a way to help us find each other to collaborate on process... it could allow us to learn from each other. We all have gaps. If I could work with others, [where skill sets complement one another], we could get better together."

Barriers to community participation

Through our community research, two major barriers to participating in community spaces emerged. The first was around the unequal distribution of resources across regions – with a non-representative prioritisation of Western perspectives, framings and experiences. The second is an absence of trust.

Regional power disparities

The unequal distribution of power and resources for orgsec practitioners in different regions manifests in a number of ways. At IFF this year, the regional disparity in terms of how well developed the organisational security community was apparent[21]. Whilst networks such as the Rapid Response Network were reasonably well developed and resourced in Eastern Europe and (northern) Latin America, this network was just emerging in MENA. This network serves multiple purposes: forming connections and collaborations with other practitioners, sharing advice and information about incidents, discussing new methodologies and techniques, identifying weaknesses in response to emerging threats, and mapping activity in the region. Regions without local community events or gatherings, and without organisations that act as regional hubs in the region (such as Digital Security Lab in Ukraine) are also at a disadvantage, without easy access to the knowledge, learning and support that these spaces provide.

In our interviews with practitioners from Latin America and MENA, the prioritisation of certain perspectives and experiences over others emerged as another barrier to participation. This manifests primarily through language, and prioritisation of English. Resources are often only available in English; community spaces require participation or engagement in English (the majority of sessions at IFF this year were in English only), and training and listservs run by Western organisations are often only delivered in English. This means that organisations and individuals need to be able to speak English to form connections, develop and grow. As well as through language, this power imbalance also manifests through the structures and models that are taught or shared in community spaces. In addition, there is a disparity in the kinds of organisations that lead and facilitate community initiatives and spaces: "So much digisec stuff internationally is dominated by American and European actors".

Absence of trust

Trust is an essential component of any functioning, successful community. With online spaces, building trust is even more difficult than doing so in person. Many of the practitioners we spoke to have close friends in their network that they share questions and challenges with. These trusting relationships are important to them. "When they have questions or want to compare notes they have a handful of people they go to, they email within that circle". Quite rightly, however, this trust doesn't often extend beyond groups of practitioners who know one another personally. Through our research, community membership and community leadership emerged as key factors that affect how much trust exists in a particular community space.

Who is part of a community space affects how comfortable people feel sharing and engaging

During a session at RightsCon, practitioners talked about the orgsec.community listserv, and how the number of people on the list had increased rapidly, but people didn't know who had joined. This made people feel reticent to share, highlighting the importance of transparent membership and/or transparent joining processes. Some practitioners we spoke to only felt comfortable and safe in community spaces that were exclusively for women and non-binary people, or for people who shared their values.

Community leadership

Whether or not practitioners feel comfortable engaging in a particular community space also depends on the organisation or group that runs the space. "People have to trust the group doing it. That isn't something you can invent". This is related to the power disparity barrier described previously. Spaces and structures that replicate existing power imbalances, with American or European actors wielding the most influence and control, are not trustworthy for many practitioners. As one practitioner put it, "I'm not thrilled with the idea of Western groups managing this globally". Another interviewee summed this up powerfully: "As any initiative – it needs a leader, or a leading group... is OTF leading, or The Engine Room? Why are the white people leading? ...Why is it a guy? It cannot be an individual effort, it's not fair. It repeats the same patterns... I have zero interest in being part of something that replicates [the same power structures] and the tokenism of engaging marginalised populations."

Opportunities

Principles for inclusive, resilient community spaces

When considering the value of community spaces for practitioners, as well as the barriers that exist to participating in these spaces, four key principles emerge which, when adhered to, could help to create and sustain inclusive and useful community spaces.

1. For the community spaces to function, thrive, and create real value for the community, **trust** between members is essential.
2. To avoid perpetuating power imbalances, and address the barriers to participation that exist, the spaces need to be **inclusive**, and prioritise the needs of those practitioners who have been underserved by existing systems of support.
3. The spaces need to be **fair and respectful** of members' capacity to contribute.
4. To foster trust, and ensure community needs are being met, members need to be aligned on the **values** being embodied by these spaces.

What these principles look like in practice will vary depending on the makeup and goals of different community spaces, but we hope they can act as useful prompts, whether you're starting a new community space, revisiting and refreshing policies and practices, or reflecting on groups you've been a part of in the past.

Footnotes

[1] Rethinking Risk and Security of Human Rights Defenders in the Digital Age
https://academic.oup.com/jhrp/article-abstract/5/3/535/2188773?redirectedFrom=PDF

[2] **http://www.integratedsecuritymanual.org/**

[3] **https://holistic-security.tacticaltech.org/**

[4] Critical perspectives on the security and protection of human rights defenders.
http://eprints.whiterose.ac.uk/95532/1/Bennett_et_al_2015_IJHR.pdf

[5] Chilled digital security, IFF 2019
https://docs.google.com/document/d/1W_O3SWdlY5OemlEvhAnkZxMJsrDpt2A3SlSUuHD0wMs/edit#

[6] **https://medium.com/read-write-participate/a-slow-and-faraway-conversation-between-slammer-musuta-and-maya-richman-d47311ec65fd**

[7] Forging Careers in Human Rights Information Security Today
https://aspirationtech.org/files/AspirationHRTechPractitionerSustainabilityReport.pdf

[8] **https://docs.google.com/document/d/1W_O3SWdlY5OemlEvhAnkZxMJsrDpt2A3SlSUuHD0wMs/edit#**

[9] Digital Security Trainers' Practices and Observations
https://secresearch.tacticaltech.org/media/pages/pdfs/original/TrainersPractices_Observations.pdf

[10] Training Digital Security Trainers: A Preliminary Review of Methods, Needs and Challenges
https://internews.org/sites/default/files/resources/InternewsWPDigital
Security_2013-11-29.pdf

[11] Rethinking Risk and Security of Human Rights Defenders in the Digital Age
https://academic.oup.com/jhrp/article-abstract/5/3/535/2188773?redi
rectedFrom=PDF

[12] Rethinking Risk and Security of Human Rights Defenders in the Digital Age
https://academic.oup.com/jhrp/article-abstract/5/3/535/2188773?redi
rectedFrom=PDF

[13] 5 day non-technical SAFETAG training, IFF 2019
https://docs.google.com/document/d/1W_O3SWdlY5OemlEvhAnkZxM
JsrDpt2A3SlSUuHD0wMs/edit#heading=h.l998sx2tnjw0

[14] Digital Security Trainers' Practices and Observations
https://secresearch.tacticaltech.org/media/pages/pdfs/original/Trainer
sPractices_Observations.pdf

[15] Forging Careers in Human Rights Information Security Today
https://aspirationtech.org/files/AspirationHRTechPractitionerSustaina
bilityReport.pdf

[16] Forging Careers in Human Rights Information Security Today
https://aspirationtech.org/files/AspirationHRTechPractitionerSustaina
bilityReport.pdf

[17] What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World
https://freedomhouse.org/sites/default/files/What%27s%20Next%20 -%20The%20Quest%20to%20Protect%20Journalists%20and%20 Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf

[18] Training Digital Security Trainers: A Preliminary Review of Methods, Needs and Challenges
https://internews.org/sites/default/files/resources/InternewsWPDigital Security_2013-11-29.pdf

[19] Forging Careers in Human Rights Information Security Today
https://aspirationtech.org/files/AspirationHRTechPractitionerSustaina bilityReport.pdf

[20] Forging Careers in Human Rights Information Security Today
https://aspirationtech.org/files/AspirationHRTechPractitionerSustaina bilityReport.pdf

[21] Regional networks, IFF 2019
https://docs.google.com/document/d/1W_O3SWdlY5OemlEvhAnkZxM JsrDpt2A3SlSUuHD0wMs/edit#