1 Promoting a blended risk management approach: the place of programming and diversity within a security risk management strategy

Chris Williams, Penelope Kinch and Lyndall Herman

Introduction

When Van Brabant and colleagues (1998) introduced the initial 'security triangle' method, two decades ago, it transformed the approaches aid organisations used to address security risk management (SRM). The security triangle model postulated that an organisation would use either acceptance, protection or deterrence as an SRM approach, and that the choice was typically determined by the broader risk level in the location. During the last twenty years of practice and experience, this initially static and often siloed model has evolved to address the shifting contexts in which aid organisations work. The experience of CARE USA has demonstrated the need to move beyond viewing these foundational strategies as a set of distinct and often sequential options, and instead use a blended strategy to achieve the best results.

The acceptance approach is a traditional baseline for SRM in the sector, but it is increasingly insufficient in a high number of operating contexts when applied by itself, as conflict and criminal actors increasingly ignore conventional humanitarian protections. By blending acceptance, protection, and deterrence approaches, it is possible to incorporate acceptance practices in some of the sector's most insecure environments, whilst still mitigating risk via protection and deterrence approaches. It is also essential to remember that acceptance itself is not a singular model, as it encompasses degrees of acceptance ranging from tolerance or consent to being genuinely welcomed by a community. In some contexts where INGOs work it may never be possible to move beyond the level of tolerance.

Rather than relying on one SRM strategy or moving from approach to approach, CARE has found success when using a blended method. This is achieved through investment in meaningful and collaborative relationships with programming teams and placing an emphasis on recruiting and retaining staff of diverse profiles, both within the security team and more broadly within our country offices. Each of these approaches has resulted in specific and applicable lessons learned, on which CARE's security team is building. Furthermore, in some hostile and fragile contexts, SRM concepts must be integrated, and the blended approach may mean that acceptance – while still foundational – is a limited component of the SRM strategy. Several case studies will clarify these ideas by situating them in CARE's experience.

Collaboration with programming staff

In CARE's experience, acceptance is best used when it is one component of a balanced SRM strategy and co-owned by programming and security teams. Conflict and criminal actors do not always respect humanitarian protections, and in recent years increasing levels of violence targeted at aid workers have made clear that acceptance cannot be the only SRM strategy applied in many of the contexts in which CARE works. To enable sustainable programming and staff safety, it is essential to pursue a blended SRM approach that incorporates acceptance, protection, and at times deterrence. Further to this approach, the experience of the

Preview - don't share further

CARE security team has also revealed that effective operational acceptance cannot be owned by the security function alone; rather, programming teams must share ownership of any acceptance approach. Co-ownership ensures understanding of and buy-in to the protection and deterrence measures that are applied. The incorporation of programming teams as participants and proponents of an SRM framework based on acceptance is also key to moving beyond a community perspective that falls into a tolerance or consent category and into genuine goodwill, as programme quality and delivery is critical to maintaining this.

In practical terms, blending security strategies to resolve issues in the field is a tool for all staff – and particularly programme staff – rather than solely the remit of security teams. Indeed, the involvement of staff with a security function can occasionally detract from a locally led resolution by programme teams (see example below). As such, it is crucial that training for all staff mainstreams deliberate avenues for clearly articulating the mission of the organisation and resolving conflict in a manner that allows sustainable programming to proceed, rather than only focusing on tactical responses in the event of a security incident.

For example, CARE Yemen operates food distribution programming – a high exposure activity – across much of the country, amid protracted conflict and dire levels of humanitarian need. Yemen is a complex and high-risk context in which to work, and one that does not fit the traditional security triangle model for an acceptance-based approach. Security incidents occur at food distributions with greater frequency than anywhere else that CARE works. However, it is neither practical nor advisable for security staff to be present at distributions, as this can be perceived by recipients and local authorities as 'securitising' this service (Eroukhmanoff, 2017). CARE's work is life-saving and carried out in a transparent and principled manner that allows staff to clearly articulate the process for selection of recipient communities. Transparency around selection processes and deliberate communication of CARE's mission provide a strong baseline for acceptance, even in areas where CARE does not have a long history of providing services. Through internal training programmes run by the security team, which include conflict resolution and personal security, programming staff are taught how to explain these approaches to communities in an effort to support an acceptance-based SRM approach.

Nevertheless, acceptance is not always sufficient, and it is not uncommon for distribution teams to encounter armed individuals disrupting activities or threatening personnel. In order to enable a food distribution programme to proceed safely, for example, acceptance, protection and deterrence strategies are used in combination. In this instance, staff take action to protect themselves – either evasive or conciliatory – and cease programme activities (deterrence) until the threat can be appropriately managed. Resolving a threatening situation such as this requires nuanced understanding of local affiliations and skilled negotiation between CARE staff, community leaders and authorities to guarantee staff safety and allow distributions to resume. While staff have been trained by security teams in how to manage such situations, typically there are no security staff present throughout the process. This highly successful combination of strategies has helped enable the CARE Yemen team to sustain services in incredibly challenging circumstances.

It is more straightforward to assume acceptance where an organisation has a long history of quality programming within a community. Building trust is not an overnight activity, and CARE's experience of living and working within communities for decades is often key to a healthy acceptance-oriented SRM approach. However, this is often not possible in the case of new humanitarian crises in areas where the organisation has not previously worked – such as Syria. This does not rule out an acceptance-based approach, but typically these settings require a more deliberate blending of protection in the initial phases. It is also crucial that organisational leadership is aware of when acceptance levels are low, to ensure that any new programme activity or area falls within the organisation's risk appetite. An acceptance analysis is a key component of any proposal to expand operations in an insecure environment. This ensures that both operational teams and leadership are cognisant of the potential challenges.

Breaking down barriers that exist between the security and programming teams to better foster collaboration is also key. This involves connecting at more than a technical level and becoming partners in strategic endeavours, such as programme strategy design, support on grant applications, providing bespoke information and awareness sessions targeted to specific staff and programming profiles, as well as being accessible to those staff

with questions and concerns. In the same way that building acceptance within the community does not happen overnight, it also takes time to build relationships that foster and prioritise acceptance as an SRM approach. A key element of this is recruiting and retaining staff of diverse backgrounds.

Recruiting diverse staff

For CARE, the importance of recruiting a diverse and inclusive staff population is a moral imperative to localise the aid sector and is also an advantage in strengthening the acceptance components of an SRM plan. Staff diversity as a component of an organisation's SRM portfolio is an area in which CARE's security team is making significant contributions. What a diverse staff profile looks like is location and context-specific, and could involve gender, professional background, or ethnicity. To date, much of the security team's work in this area has focused on recruiting a diverse team across the headquarter and country office levels. Security team diversity, particularly when it brings in staff from different organisational and professional backgrounds, is instrumental in creating connections across functions within a country office. Additionally, by drawing on the experience of staff from diverse professional backgrounds and through collaboration with programme staff, CARE has seen an increase in the application of a blended SRM approach, rather than over-reliance on one approach or a traditional scaling of approaches (applying acceptance, protection, and deterrence sequentially). Staff diversity within programming and field-based teams is also crucial in building an organisation's acceptance by the local community.

Security staff from diverse profiles bring invaluable skills and experience to their positions, are more reflective of both the staff and community populations, and are often viewed as more approachable by colleagues, which in turn builds security culture. For CARE, this is best exemplified within the Safety & Security Focal Point (SSFP) programme, which sees staff appointed or volunteering to run the SSFP office in low and moderate risk locations. Through this programme, CARE has created opportunities for staff from non-security backgrounds to enter into and progress within the security sector. While much depends on the individual's goals and approaches, through internal training programmes and technical coaching, CARE has seen staff progress within the security field, moving from the voluntary SSFP programme into full-time international safety and security manager positions. This programme has encouraged staff with no or limited safety and security backgrounds to become safety and security champions, including staff from administration, IT, and programme backgrounds. While not possible in all contexts, developing avenues for current staff to learn about and build a career in safety and security within the organisation is an opportunity to both diversify the field and capitalise on pre-existing connections to internal programming and operational teams.

Recruiting and investing in local capacity – both security and programme staff – at the hyper-local level has been key in pursuing and maintaining an acceptance-based SRM approach for CARE in insecure environments. This approach creates a cadre of trained and talented local staff who best understand the local context and who can navigate the contextual nuances far better than a non-local, which in turn enhances CARE's acceptance strategies. This insight into local contextual nuance is at the core of a blended SRM approach: acceptance can and will only work to a point, particularly in insecure environments. Local and diverse staff are able to flag when a reconfiguration of approaches may be needed to respond to local changes or threats. Similarly, they best understand how and to whom in the community core messaging needs to be communicated.

CARE's work in Dadaab refugee camp in Kenya provides an excellent example of hiring from within the affected population to provide services to the community in education, community outreach, and WASH. In this instance, program participants became staff, who became advocates for the organisation and were able to explain CARE's mission, approaches, and objectives to fellow community members more successfully than outside staff. By virtue of their membership in the community and their local awareness, the safety of staff, the programme, and the recipient population is better served than if equally skilled people from a different location were brought in. There are, of course, situations where CARE observes significant tensions with local host communities who experience the economic and physical strain of hosting refugees and internally displaced people on what are often already marginal resources. In these instances, tensions can be eased by providing employment to local community members that is proportional to employment for members of the refugee or internally displaced community. One good example of this is in South Sudan, where CARE has hired a large proportion of local staff in various cities and regions. This has been a conscious strategy to build relations with local communities and has resulted in limiting disruption to operations due to ongoing youth protests related to employment opportunities.

However, this approach can also create issues, particularly when it is mandated or overseen by local or national authorities. When hiring locals to staff programmes is required but cannot be supported by appropriate capacity building (including lack of training access, limited education opportunities or professional experience, or due to perceptions of bias), this can have the opposite impact on acceptance. In such instances, improperly or inadequately trained staff can impact on programme quality and consistency. This leads to resentment and can imperil organisational acceptance and raise questions regarding the sustainability of programming. By investing in the local communities with whom we work, through employment and training opportunities, CARE shows a commitment to those communities. In turn, efforts to build and maintain local acceptance are understood as genuine and authentic by those communities. While it is not a fool-proof approach, it has yielded more success than not in recent years.

Lessons based on CARE's experience

Acceptance remains a key and foundational strategy for the SRM model in the aid sector. However, it needs to be balanced and contextualised as a blended rather than siloed approach. Experience has generated three transferable lessons for the sector.

The first lesson is that, as a security team, it is important to think beyond the tactical approaches to staff and organisational security and take the time and effort to build out soft skills such as negotiation, conflict resolution, and articulating CARE's mission in a clear manner. The professionalisation of the aid sector, as well as increasingly direct threats against humanitarian actors, has led to the development of professional security teams and resources in most aid organisations. This evolution has become more pronounced as security departments are required to address more than tactical approaches to operational security, and to build out a culture of security in an industry that has not traditionally needed to rely on such a structure. As such, the building of soft skills through both external and internal training – facilitated or hosted by programme teams – has been a key element of building these essential relationships and ensuring that security and programme teams complement each other.

The second lesson is that this process takes time. It cannot be rushed, and there is no formulaic approach to building relationships. This is true both internally, as lessons are learned from prior experience, and externally, in relationships with the multitude of actors who have an influence over an organisation's presence in a community. Funding influences much of this reality, as grants tend to run in two- or three-year cycles (or less for many humanitarian programmes) and recipient communities are very aware of this fact. Continued presence and engagement through consecutive grant cycles – or even outside of them – along with meaningful employment, capacity developing opportunities, and consistent quality programmes are all essential components of building genuine and long-term community acceptance. While CARE's largely restricted funding profile makes this approach difficult, there are opportunities here for organisations with a more flexible funding structure.

Finally – while much of the success of a blended acceptance approach is dependent on actors external to the security structure – effort and leadership must come from the security team. An adaptive and inclusive security team is an essential part of success. While security 'owns' SRM (and thus acceptance as an approach), in reality it is influenced by many other organisational actors. Security must drive this process through proactive and consistent engagement with programming teams, acknowledging the competing priorities of different functions, and enabling sustainable, quality programming. This also ensures that, when and if it becomes necessary, programming teams understand why security advises a modification of programming to incorporate elements of protection and deterrence as a situation moves beyond the scope of an acceptance-only approach.

Security teams can work to harness the benefits of an acceptance-based SRM approach. However,

Preview - don't share further

quality programmes that meet articulated community needs are what ultimately support an acceptance strategy. Adapting and blending approaches to account for varying degrees of acceptance is essential, and reliant on building comprehensive cross-functional relationships and ensuring that diverse and local staff are part of this process.

Bibliography

Van Brabant, K. 1998. Security and Humanitarian Space – perspective of an aid agency. Bochum, Humanitares Volkerrecht (1): 14-24.

Eroukhmanoff, C. 2017. Securitisation Theory. In International Relations Theory, ed. Stephen McGlinchey, Rosie Walters, and Christian Scheinplug (104-109).

Preview - don't share further

2 Debunkerising Acceptance: a view from the ICRC

Fiona Terry, Jean-Philippe Kiehl, Robert Whelan and Tamas Szenderak

Introduction: the relationship between acceptance and security

The first pillar of the ICRC's security model is 'acceptance' (Brugger 2009), a concept embedded in the ICRC's DNA that goes beyond concerns about security. Bestowed with an official mandate by states and enshrined in international humanitarian law (IHL), the ICRC's standard operating procedure is to gain approval for its presence and actions from both state and non-state parties to armed conflict. This formal agreement of the ICRC's role and presence is intended to accord security and safety to its staff and integrity to its premises, and to provide the legitimacy that is essential to the ICRC's efforts to persuade the parties to armed conflict to conduct hostilities in accordance with IHL.

The notion of 'acceptance' also underpins three of the fundamental principles of the Red Cross and Red Crescent Movement: neutrality, impartiality and independence. 'Neutrality' is often incorrectly misunderstood as a moral position. Instead it is an operational posture that aims to foster acceptance of the ICRC in even the most highly politicised contexts of armed conflict. As the principle explicitly states, the Red Cross does not take sides in hostilities or engage in controversies for a reason – 'to enjoy the confidence of all' (ICRC 2015:4). Acceptance is fostered by adhering to the principles of impartiality (not making any adverse distinction regarding who receives humanitarian assistance, giving priority to those most in need) and of independence (acting without interference from extraneous political, military, economic or other influences). To be effective, these principles must be explained and applied consistently.

The principles are further operationalised through several working modalities that also seek to enhance acceptance. By treating any observed breaches of IHL with strict confidentiality so they can be discussed in bilateral dialogue with the assumed perpetrators, the ICRC aims to gain acceptance of the need to respect humanitarian norms. Being transparent about what the ICRC does and why helps to allay suspicions of hidden agendas and considerable effort is placed on disseminating knowledge of the ICRC and broader Red Cross and Red Crescent Movement. Acting consistently across contexts so as to be predictable and coherent is important in promoting acceptance at all levels.

Whilst this framework never provided guarantees of either access nor security - to which the tragic deaths of ICRC delegates and blocked access attests - it has allowed the ICRC to save lives and alleviate suffering in conflict zones throughout the world for more than a century. Certain trends in armed conflict over the last decade, however, challenge some fundamental ideas underpinning this approach and warrant more attention. This article takes a closer look at the ICRC's security incident data before unpacking some of these new challenges, such as the proliferation of armed groups in contexts around the world. It then describes some of the ICRC's security concepts and practices intended to address these challenges before concluding with thoughts on moving forward.

Has humanitarian action become more dangerous?

The last few years has seen lively debates over whether the contexts in which humanitarians operate have become more dangerous.[1] Much of this debate is centered around the use and interpretation of data on security incidents against humanitarian actors. Data from monitoring organisations show a global trend suggesting that

1 For a summary of the issues see Stoddard, Harmer & Harver 2016.

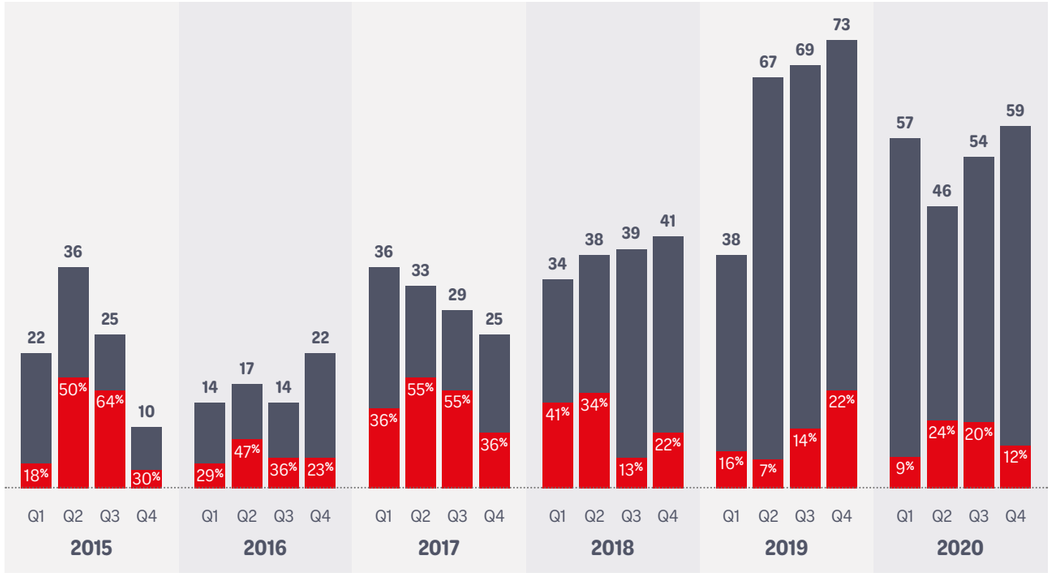
serious security incidents involving aid workers have gradually increased year-on-year. The number of recorded attacks on aid workers in 2019 exceeded the number in each of the years previously recorded by the Aid Worker Security Database (Stoddard et al. 2020).[2]

The ICRC's own data does not mirror this trend.[3] While there has been an increase in security incidents reported in recent years, this largely reflects the organisation-wide adoption of a custom-built internal reporting system, the *Security Management Information Platform* (SMIP), which was specifically designed to enable more comprehensive and integrated reporting of all security incidents. For each security incident report, ICRC staff record whether the evidence suggests that the ICRC was deliberately targeted or not, or whether this factor is unknown. Importantly, data from the last three years shows that the proportion of incidents targeting the ICRC has remained stable at around 20 percent, irrespective of the overall quantity of incidents. Furthermore, taking account of the growth in the ICRC's operational footprint over the last five years – from around 14,000 staff and 290 structures worldwide in 2015 to some 20,000 staff and 318 structures today – we see that proportionally the *rate of harm* for ICRC staff has steadily decreased and in 2020 stood at around one third of what it was in 2015.

Of course, there is much that the data does not say: it would be foolish to draw conclusions about the ICRC's level of acceptance on the basis of these numbers alone. The data does not show the number of places where it is too unsafe to work, such as much of south-central Somalia, or in which an armed group or authoritarian government has rejected the presence of humanitarians outright. Nevertheless, tracking security incidents – from seemingly innocuous stone throwing at cars by young children to direct threats against the lives of ICRC staff - enables us to monitor the local mood, review the context analysis and security strategy as required, and address misconceptions or errors on our part before they fester. Improvements to the ICRC's ability to monitor security are described further below.

In fact, one unexpected finding in the data is the rise in the number of incidents attributed to civilians. Those attributed to military forces, armed groups

Figure 1: Evolution of recorded security incidents since 2015 by quarter, showing the proportion of incidents (in red) deemed to have involved deliberate targeting.



2 At the time of writing, data on attacks against aid workers from 2020 is still being collated.

3 The ICRC has been collecting data on security incidents for decades although it cannot be relied upon to be complete, accurate and reliable in all instances. The definitions of key terms, the data capture and validation processes, the challenges around the subjectivity of reporting, the structure of the data models and other factors all represent limitations in the utility of the data. Hence while every effort is made to ensure a reliable dataset, there may be impediments to drawing solid conclusions from it.

Preview - don't share further

Figure 2: Graph depicting the types of security incident[5] caused by different perpetrators recorded in the year 2020. A large proportion of incidents (%) are caused by civilians and criminal actors. (Null values removed).

	Incidents without operational consequences	Important incidents	Serious incidents
Civilians	**45** (30%)	**26** (29%)	**1** (10%)
Criminals / Bandits / Organised crime	**33** (22%)	**17** (19%)	**3** (30%)
Non-state armed groups	**17** (11%)	**22** (24%)	**4** (40%)
Military	**18** (12%)	**13** (14%)	**1** (10%)
Unknown	**17** (11%)	**7** (8%)	**1** (10%)
Police	**11** (7%)	**3** (3%)	

and criminal actors have remained proportionally stable or declined over the last three years, while incidents caused by civilians – for example, disgruntled employees, communities not included in aid distributions, religious fundamentalists, ultra-nationalist or protest groups - have increased by 50 percent or more, predominantly in Asia and the Middle East.[4] Although carrying less severe operational consequences than incidents involving fighting forces or criminals, the increase in harm by civilians warrants deeper analysis, particularly to see whether this is more prevalent in protracted conflicts where aid has become an important stake in local economies, given that a large proportion of these threats have an economic motive. We shall return to this point below.

So, whilst the ICRC has not seen an overall increase in harm, some of this is due to a scaling back of exposure. The aspiration for acceptance everywhere has had to be tempered with the realisation that in many contexts our level of acceptance sits on a spectrum with acceptance at one end and rejection at the other. The mid-point is 'tolerance' of the ICRC. The spectrum is dynamic, shifting in accordance with internal and external events, and needs to be assessed for every relevant source of authority: the ICRC might have full acceptance from some and little from others. Identifying indicators of where to place the cursor on our level of acceptance along this spectrum is tricky.

Challenges to acceptance

Expanding our gaze beyond security statistics, the ICRC's observations on the ground highlight three developments of particular note that challenge the ICRC's capacity to foster acceptance.

First, the proliferation of armed groups - the vast majority of which have decentralised organisational structures (having either splintered from a larger group, as in Colombia, or emerged from communities as in Libya) - hinders the possibility of relying on a hierarchical chain of command to authorise access and give security assurances. The number of non-international armed conflicts has more than

4 Different types of perpetrators such as 'armed groups' or 'civilians' are not precisely defined but security specialists who review each incident apply their expertise to classify the main elements of each incident as consistently as possible. That said, there are many incidents where complex factors and unique combinations of elements defy simple classification, for instance when civilians and armed groups combine to perpetrate an incident.

5 The ICRC classifies security incidents under three categories: 1) A *serious* incident is an event that causes major harm to the physical or mental integrity of ICRC staff members and/or has a significant impact on operations. 2) An *important* incident is an event that constitutes a danger to the physical or mental integrity of ICRC staff members and may affect operations; 3) Incidents are designated as *without operational consequences* when the event constitutes a danger to the physical or mental integrity of staff members but did not affect operations.

doubled over the last two decades from around 30 at the end of the 1990s to around 100 today, and more than one-third of them involve three or more parties to the conflict (Nikolic, Ferraro & de Saint Maurice 2020). Furthermore, there is an increased regionalisation and globalisation of armed groups and their support networks. While contact with field level leadership is generally possible, communication with regional and global leadership is far more difficult. The fluidity of the environment and the speed at which alliances form and change hinders our ability to foster mutual understanding between aid organisations and armed groups. Moreover, we see an increase in the number of states intervening in armed conflicts beyond their territory, notably as part of coalitions, in partnerships or in direct support. Many of these states are 'middle powers' and may be assertive, and/or have had limited engagement with the international humanitarian sector in operational theatres, and thus have a different interpretation of humanitarian action. Throughout its history, humanitarian action has been manipulated and instrumentalised in the service of political interests (Terry 2002) but this tendency seems to be on the rise. The post-Cold War celebration of humanitarian ideals began to wane with the 'war on terror' of the early 2000s and has suffered an accelerated demise as dedicated aid departments are absorbed into bodies which reorient aid towards serving political and economic interests.

Second, the relationships between aid organisations, the communities they seek to help, and the authorities in charge have become increasingly transactional, part of what Alex de Waal (2018) terms the 'political marketplace' in which political services and loyalties are exchanged for material resources.[6] As mentioned above, in many protracted conflicts, humanitarian aid is part of the fabric of war economies. Where once humanitarians assumed they were safe by helping the people for which the armed group or government professed to fight, the 'capture' of aid resources by a group (local warlord, government authority, business community or other gatekeepers) for economic gain or as a tool of patronage is a growing phenomenon. Having a vested interest in keeping the aid enterprise spending money that can be tapped or directed to 'client' groups, those practicing 'aid capture' apply pressure to humanitarian organisations to act in a way that can undermine humanitarian principles, and can pose security threats to aid agencies that wish to address this issue. The rise in identity politics – political attitudes that promote the interests of a group based on racial, religious, ethnic, social, or cultural identity - further complicates attempts to explain the principle of impartiality, especially if needs are greater on one side.

The transactional nature of humanitarian assistance is not new: acceptance and access have long been premised on an unspoken understanding of the indirect benefit of providing vital social services to the population under the control of an armed group. It alleviates some of the responsibilities of governing. But this quid pro quo presupposes an affinity between the population and the armed group, which is not always the case: the Khmer Rouge-controlled IDP camps along the Thai-Cambodian border were off-limits to aid agencies in the 1980s. Over the last decade no access has been possible to regions of Afghanistan with high concentrations of foreign fighters because they have no local constituency to care for (Terry 2011). In some contexts, the regionalisation and globalisation of networks of armed groups exacerbates this trend, creating greater distance between populations and those who control them.

Another related challenge to establishing mutual trust with armed groups is the restrictive measures states impose on humanitarian actors interacting with certain groups, including under counter-terrorism legislation. Impediments to responding to humanitarian needs because of such legislation undermines the principles and purposes of humanitarian action, to the detriment of those in need of assistance and the reputations of humanitarian agencies.

The third potential challenge to acceptance comes from the spread of new technologies and social media. Whilst there are many positive aspects of making armed groups and communities more accessible through internet platforms and telecommunications, there are also risks to this 'digital proximity'.[7] Many armed groups are deeply suspicious of new technologies' potential for spying: this is certainly the case of Al Shabaab in Somalia which lost several senior members including its leader, Ahmed Godane, in targeted missile attacks (Martinez & Hughes 2014), which led to tight restrictions on who could access the territory they control, and limiting communication equipment. Another potential threat stems from the speed at which misinformation spreads and the risk that a malicious rumor about an aid agency could spread rapidly and rally an aggressive crowd. Misinformation might help to explain the rise in incidents perpetrated by civilians, highlighted above.

Adapting the ICRC's security management system to contemporary challenges

The ICRC's security management system has evolved over time to reflect these growing challenges. Its decentralised nature has not changed, based on the conviction that those closest to the field are best placed to understand the context (see Krähenbühl 2004). This approach emphasises understanding the ICRC's mandate, humanitarian principles and the application of the 'pillars of security'. But more recent emphasis has been placed on developing a systemic approach to security management across the whole organisation that aims to improve the quality and circulation of information and analysis to support the definition of acceptance strategies and overall decision-making. This has required maintaining a balance between a 'heuristic' approach to security based on experience, and a structured and inclusive process based on professional standards, procedures and institutional learning.

The ICRC has invested in its capacity to gather and analyse information on security incidents and potential threats and established a digital reporting system to help ICRC staff monitor trends. Looking at trends over time can help pinpoint incident triggers and better understand the 'weak signals' of impeding risk and supports our acceptance approach. There is still work to be done to harmonise definitions and identify objective indicators to help mitigate factors such as 'confirmation bias' (whereby people tend to interpret data as confirming pre-existing assumptions rather than challenging them), and in collecting, processing and analysing data on cross-border armed conflicts and humanitarian operations. The ICRC has invested more time and resources in producing political analyses of conflict-affected settings, with a dedicated research stream on the role of aid in the political economy of conflict and its consequences. This research stream might help to make sense of the increase in violence by civilians against the ICRC as we dig deeper into identifying the winners and losers of the economic windfalls injected by the aid sector and its impact on acceptance.

Managing and analysing information in a 20,000 strong workforce is a challenge in itself, particularly one organised along professional sectors (health, economic security, water and habitat, protection, communication, law.) The Security Unit at HQ has been working to embed principles of security management into each sector in the field and at HQ, including the obligation to apply 'minimum security requirements' across all ICRC sites. Its purpose is to systematise, through training and on-site support, a security risk management process that capitalises on the different knowledge, experiences and opinions of staff with very different profiles and functions, including different perceptions of acceptance. A thorough analysis of the ICRC's operational ambitions and footprint within the local political context is key because it helps us define the right balance between acceptance and other mitigation measures: on the one hand, privileging acceptance-only might expose staff to unforeseen dangers, but on the other, resorting to armored vehicles, armed escorts, or heavily guarded compounds can undermine efforts to gain acceptance. Such measures may also bring other risks, for instance paying for security services potentially fuels violence and associates aid organisations with those providing the services. A sound security risk management process, undertaken with an inclusive and participatory approach, takes all these factors into account and helps define the best approach.

A dedicated security forum operates both at HQ and in field structures to help ensure access to security information updates and procedures, as well as to flag and address emerging threats or challenges. On a quarterly basis, the Security Unit provides an overall view of the most exposed delegations' security risk exposure. This reporting is combined with initiatives led by other sectors of the ICRC, such as the annual mapping of the ICRC's relationships with non-state armed groups, to enable a broader

6 For excellent research around this theme see LSE 2021.

7 See ICRC blog series beginning with Marelli 2020.

understanding of where successes and impediments lie in efforts to be understood and accepted.[8] Stakeholder mapping and analysis includes security management issues, such as notifications made to local authorities of ICRC's plans in an area and green lights obtained from them to proceed. Other indicators of the ICRC's acceptance include the quality of the ICRC's dialogue with an armed group (what subjects we can broach); with whom are we permitted to speak; and the number and type of interactions allowed. Having a strong security risk management system in place helps us identify risks and opportunities holistically, assess the solidity of our network and avoid a siloed approach to acceptance.

Conclusions and implications

This article has sought to connect an ideal – acceptance - to one of its roles in preserving the security and safety of humanitarian staff. In doing so, the article has explained some of the practical ways that the ICRC has sought to better understand and mitigate risk. But there are some higher-level considerations linked to the challenges identified that need deeper consideration.

One major area of further work is to consider whether the current structure of the ICRC – reflecting its historical past – is capable of addressing the new challenges highlighted above. The ICRC remains quite state-centric and is structured and staffed to respond to the bureaucracy of states. The proliferation of non-state armed groups and their regionalisation and globalisation suggest that the ICRC might need to adapt its set-up to be better equipped to deal with such transnational entities. Recent research has helped us understand sources of influence on the behaviour of members of state armed forces and armed groups, based on their organisational structure, and demonstrated the need to engage with a greater array of potential influences if we are to make inroads into promoting restraint on the battlefield (ICRC 2018). We now need to improve our ability to work in the borderlands and across borders. To do this we need to reinforce regional hubs so they can play a more central role in networking with and reaching out to groups that increasingly join transnational networks and support systems, with a view to increasing engagement opportunities and thereby acceptance of the ICRC.

The rise in security incidents committed against ICRC staff by civilians also warrants greater attention, particularly with regard to how it affects our acceptance. We need to dig more deeply to understand the circumstances of these events, whether they are connected to something the ICRC did, or failed to do, and how to reverse this rising trend. We also need to link this observation to ongoing research into misinformation, disinformation and hate speech in armed conflicts and its influence on the attitudes and behaviour of civilians (see Tiller, Devidal & van Solinge 2021).

The proliferation of armed groups, the growth of identity politics, and the increasingly transactional nature of relationships between humanitarians and state and non-state entities is likely to make it harder to gain acceptance as a neutral, impartial and independent humanitarian organisation. But it is difficult to envisage another means of gaining acceptance to reach those in need, regardless of who they are or what they may have done, other than to put these principles into practice and demonstrate the purely humanitarian intention of our aid. The expanded access to the internet and hence to information across all corners of the world make acting in a consistent and coherent manner across different contexts all the more important. The principles of neutrality, impartiality and independence provide a vital thread through which to consider how different groups might perceive ICRC actions and communications. Acceptance from communities and political authorities of the ICRC's presence and operations is best promoted through proximity to the people most in need, and here the specificity of humanitarian security management is precisely to support acceptance-related efforts holistically, from context analysis to programme designing, and not to force a security-driven bunkerisation of humanitarian action.

8 In 2020, the ICRC was in contact with 465 armed groups worldwide. Although this number fluctuates each year, it represents thousands of direct and indirect interactions with armed groups across hundreds of sites and at all levels of an armed group's hierarchy.

Preview - don't share further

Bibliography

Brugger, P. (2009) "ICRC operational security: staff safety in armed conflict and internal violence", *International Review of the Red Cross*. 91 (874).

de Waal, A. (2018) *Mass Starvation: The History and Future of Famine*. Cambridge, Polity Press.

ICRC (2015) *The Fundamental Principles of the International Red Cross and Red Crescent Movement*. Geneva, ICRC. Available from: https://www.icrc.org/sites/default/files/topic/file_plus_list/4046-the_fundamental_principles_of_the_international_red_cross_and_red_crescent_movement.pdf

ICRC (2018) *The Roots of Restraint in War*. Geneva, ICRC

Krähenbühl, P. (2004) 'The ICRC's approach to contemporary security challenges: A future for independent and neutral humanitarian action', *International Review of the Red Cross*. 86 (885).

LSE (London School of Economics) (2021) *Conflict Research Programme*. Available from: https://www.lse.ac.uk/ideas/projects/conflict-research-programme

Marelli, M. (2020) 'Hacking humanitarians: moving towards a humanitarian cybersecurity strategy', (January 2020, blog). Available from: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/

Martinez, L. & Hughes, D. (2014) 'Top Al-Shabab Leader Killed in Airstrike, Pentagon Confirms', ABC News, 5 September 2014. Available from: https://abcnews.go.com/International/top-al-shabab-leader-killed-airstrike-pentagon-confirms/story?id=25265232

Nikolic, J., Ferraro, T., & de Saint Maurice, T. (2020) "Aggregated intensity: classifying coalitions of non-State armed groups." *ICRC Humanitarian Law & Policy Blog*. Geneva, ICRC

Stoddard, A., Harmer, A., & Harver, K. (2016) 'Data are not dangerous: A response to recent MSF CRASH critiques'. Humanitarian Practice Network. Available from: https://odihpn.org/blog/data-are-not-dangerous-a-response-to-recent-msf-crash-critiques/

Stoddard, A., Harvey, P., Czwarno, M. & Breckenridge, M.J. (2020) 'Aid Worker Security Report 2020: Contending with threats to humanitarian health workers in the age of epidemics' *Humanitarian Oucomes*, August 2020.

Terry, F. (2002) *Condemned to Repeat? The Paradox of Humanitarian Action*. Ithaca, Cornell University Press.

Terry, F. (2011) 'The International Committee of the Red Cross in Afghanistan: Reasserting the Neutrality of Humanitarian Action', *International Review of the Red Cross*. 93 (881), 173 – 188.

Tiller, S., Devidal, P. & van Solinge, D. (2021) 'The "fog of war" … and information'. Humanitarian Law & Policy (blog), 30 March 2021, available from: https://blogs.icrc.org/law-and-policy/2021/03/30/fog-of-war-and-information/

Preview - don't share further

Choice architecture and organisational SRM buy-in

Araba Cole and Panagiotis Olympiou

Introduction

Choice architecture is the deliberate design of the context in which choices are offered to a targeted group of people, and it is the responsibility of the choice architect – in this case, the SRM practitioner – to facilitate or hinder desired behaviours through the way in which choices are presented (Thaler & Sunstein, 2008). Choice architecture is used in multiple areas, such as government and advertising[1], to facilitate the desired behaviour of targeted groups. This article explores how choice architecture can be adapted to increase SRM buy-in within humanitarian organisations, which we consider essential to strengthen the acceptance component of the organisation's SRM strategy.

SRM buy-in from within an organisation and its staff at all levels is essential both to preserving the wellbeing of personnel and to support their ability to deliver effective, do no harm programming. In turn, achieving these objectives helps to safeguard an organisation's acceptance by external actors. If buy-in is not achieved, individual actions as well as organisational shortcomings in the implementation of an otherwise sound SRM approach can affect both an organisation's results and perceptions of their operation and delivery. Therefore, maximizing buy-in from within can play a significant role in both the robustness of SRM per se as well as acceptance more broadly. Choice architecture – along with other aspects of cognitive and behavioural research – can help explain why buy-in sometimes fails, and provide insights and practices to help increase it.

Fundamental to both SRM buy-in and acceptance by external actors is perception: perceptions guide behaviour, and behaviour shapes individual choices (Kahneman 2013). The technical aspects of SRM – which come in the form of standard operating procedures (SOPs), guidelines, etc. – often do not account for *actual* human behaviour or fluctuations in personal diligence. While SRM may correctly identify security risks and propose logically coherent solutions, these solutions are not always followed by individuals, which often turns out to be the weakest link of the SRM chain. There are two ways in which SRM can engage with the human element to improve organisational buy-in: addressing perceptions, and utilising choice architecture. SRM professionals can address staff perceptions of SRM by considering the following questions. Do staff also see risk where the security professionals do? Do staff consider the measures implemented to be commensurate to programmatic objectives? Do external stakeholders perceive the organisations' activities as aligned with the do no harm principle? Perceptions are often a target of security professionals, who try to influence these by means of communication, training, and as a last resort, human resources measures (verbal or written warnings, termination of contracts or other disciplinary actions as a result of not adhering to the security protocols of an organisation's actions). While work on perceptions is important, it is also fleeting in a domain that is very dynamic, results-driven, and characterized by high staff turnover within missions. These approaches are thus not failsafe, and they may leave behaviours unaltered with little other recourse available to ensure buy-in throughout the organisation, hence the importance of choice architecture as another means of improving buy-in.

Instead of targeting staff perceptions, knowledge or skills, choice architecture aims at intervening in the environment in which staff operate, and so directly affects their behaviour. Instead of solely seeking to change behaviours by instruction, it *induces* the desired behaviours by offering a particular choice or set of choices, in a particular way. We propose that this approach is both essential and complementary to other SRM techniques, as it facilitates better organisational buy-in which in turn enables the safe and effective program delivery essential for sustained acceptance by external actors throughout the program lifecycle.

Our analysis begins by examining the limitations and obstacles to SRM buy-in within organisations, taking into account issues of perception, communication, and resourcing surrounding security risk management. We then look at relevant research and its value to NGO SRM. Finally, we demonstrate how the learning from these research reports can be applied to SRM practices in NGOs in order to gain stronger organisational buy-in.

Obstacles to organisational buy-in

In and of itself, SRM can be a burden to the operations of NGOs. Many staff see the implementation of SRM as detracting resources from their primary objective: program implementation. Notably, SRM often requires staff members to adjust their behaviour in a way that may be additional and external to their self-perceived core professional identity (be it a logistician, a protection expert, a humanitarian, a programme manager, or other). Moreover, SRM might call for a set of everyday (and often mundane) actions, which are implemented differently in the professional setting than in the private life of the same individual (e.g. locally hired staff driving organisational vehicles wearing seat belts, but not while driving their personal vehicles). Moreover, under time and other constraints, even diligent employees can find themselves downgrading security tasks when demands more central to their job function become urgent.

Not only can SRM be expensive and obtuse, but it can also be hard to persuade people of the value of good SRM. NGOs often lack the key metrics used to evaluate SRM performance as seen in other sectors, such as returns on investment (RoI) and return on prevention (RoP).[2] There is effectively a problem of negative proof: how to prove something (e.g., a major security incident) did *not* happen as a result of SRM efforts. Fundamentally, as a result of slim incentives, the significant effort and resources required, and a conscious or unconscious lack of prioritisation, staff and managers do not always make choices conducive to successful SRM and acceptance. Choice architecture, with its foundational principles of behavioural insights and cognitive biases, can be used to remedy this.

Leveraging biases

At the heart of choice architecture is the fundamental concept that humans are not always rational decision-makers: we do not necessarily automatically choose of our own volition what is safest for us or what serves our larger and long-term objectives. We are, in fact, human, and our choices and behaviour deviate from logical expectations, and these deviations provide the space for choice architecture. In our case, where compliance and buy-in of SRM may seem logical in insecure operating environments, this is not always the norm. Significant work has been done in identifying how human behaviour deviates from a rational norm, particularly in the face of risk, in the form of cognitive biases (Taleb 2018). We will outline here some of these biases and what they can look like, and in the next section indicate how choice architecture can be used to help overcome them and improve SRM buy-in.

One of these biases, *loss aversion*, has been highlighted as a key motivator in decision making. In the face of certain loss, most people prefer a gamble, while in the face of certain gain, a gamble is very unattractive. For example, the security arm of an organisation wishes to install a new warehouse locking system to prevent possible theft, but the budget holder is willing to gamble that such theft will not occur and declines to authorise the expense (which is seen as a certain loss). Loss aversion can be a significant obstacle to SRM buy-in, with security measures being seen as a loss of time, money, energy, and sometimes all three. However, once we understand what loss aversion is and how it influences behaviour, we can use choice architecture to present the choice differently (even if the choice is a simple Yes or No – in the example above, funding or not funding the locking system). Framing a choice of behaviour on the basis of "gains or losses relevant to the status quo" (Kahneman and Tversky, 1984:343) can impact on the choice made. In the

1 Choice architecture has already been deployed very successfully in other sectors. Thaler & Sunstein (2008) developed the concept of the 'nudge' which has gone on to see practical application in the UK government by David Halpern who led the 'Nudge Unit' or, more formally, the Behavioural Insights Team. By capitalizing on behavioural insights and cognitive biases they had significant successes in affecting citizens' decision-making to help improve results in areas such as tax collection and unemployment. Another arena where such understanding has paid enormous dividends is in marketing and advertising (Shotton 2018), and data on consumer choices is becoming one of the biggest commodities on the market (Matsakis 2019, Melendez & Pasternack 2019).

2 As a performance indicator, return on investment (RoI) evaluates the economic benefit of an investment, as compared to the investment's cost. Return of prevention (RoP) measures an organisation's economic benefit deriving from ensuring occupational safety and health. Examples of such investment pertaining to SRM could be hostile environment awareness training (HEAT) or hands-on personal safety courses, physical security installations like automatic locks, or medical evacuation and kidnap and ransom insurance.

example above, framing the installation of the new warehouse locking system as an investment which will save an organisation thousands of dollars in misappropriated stock rather than solely presenting the initial cost of the new system will be much more attractive to the budget holder and decision makers involved.

Similarly, the *fundamental attribution error* describes people's tendency to explain an individual's behaviour by attributing her actions to her personality, while simultaneously underestimating the significance of contextual and situational factors at play (Shotton 2018). Although instinct leads us to almost always believe that a behaviour is the result of one's character, social psychology experiments (Jones & Harris 1967) have shown this to be a fallacy, and that context or specific situation affects behaviour to a greater extent than we intuitively perceive. For instance, an NGO driver in rural Lebanon who fails to carry out desired SOPs at a checkpoint despite his training and instruction by management may at first instance appear to be negligent. However, upon closer inspection he may well be responding to a feature of the environment: his social ties with checkpoint personnel may oblige him to adhere to social expectations rather than organisational SOPs. Incorporating this insight into one's analysis and systems design allows for a more nuanced understanding of behavioural causes, thus opening up a wide range of opportunities for achieving the desired results by moving the focus from the individual to the environment in which she operates. While there is not one answer on whether adhering to all local social norms necessarily safeguards an organisation's acceptance, misalignments between SRM protocols and employees' behaviour flag points of friction to the SRM practitioner designing procedures.

Our perception of risks can also be similarly fickle. When thinking about risks such as causes of fatalities or assessing how dangerous something is, we often conjure images and information that we might have recently been exposed to, for instance in omnipresent social media or news. This is an example of the *availability heuristic*[3] (Kahneman & Tversky 1974) which prompts us to reach for the most readily available and vibrant information to answer a question or solve a problem. For example, let's consider a delegation of donors who had planned to visit a provincial capital in Eastern Afghanistan by road. During the fortnight before their travel, improvised explosive device attacks on this road increased from one to three, a development which led the delegation to seriously consider cancelling their visit, despite the fact that similar or even higher numbers of such attacks had been seen in multiple instances during the previous year. The fact that this relative spike was recent, however, had a disproportionate impact on the delegation's perception of insecurity, despite all other factors pointing to a normal level of risk. Once again, knowledge of this cognitive bias can provide an opportunity to SRM practitioners to ensure that relevant SRM information is salient in the minds of those choosing a course of action, and help balance the effect of recent and vibrant information in decision making.

The *representativeness heuristic* (Kahneman & Tversky 1974) is another bias that can cause blindness to risk. If something is representative of or looks like something that is safe or normal, then we are unlikely to respond; if it doesn't look like our archetypes of a threat or a danger, then we are unlikely to challenge or mitigate against it. From an SRM perspective, this can cause a critical myopia when dealing with risk, which can manifest itself as resistance to SRM by personnel within an organisation; potential threats and hazards may not always be easily recognisable and so a plan to mitigate them may be challenging to justify or enforce. This has been a significant challenge in Afghanistan, where female suicide bombers were highly effective due to women not being seen as threatening, as well as cultural barriers against searching women (either by men, or the hiring of female guard personnel). Women were not *representative* of the threat, nor were they representative of the solution.

Though it may be rational to support organisational SRM in order to facilitate safe and responsible programming and acceptance by stakeholders, this is not always the reality due to some of the deeply ingrained cognitive hardwiring described above. Choice architecture enables SRM practitioners to overcome some of these biases to help increase effectiveness and buy-in of their SRM measures. We will examine some key uses in the next section.

3 A heuristic is a means of problem solving that utilises an approximation or 'rule of thumb' rather than an optimal solution.

Preview - don't share further

Uses for the SRM practitioner

In a world where trying to generate SRM buy-in can often feel like trying to sell an unpopular product to a hostile market, these insights are of significant value to the SRM practitioner who wishes to increase buy-in, make programmes safer, and gain the trust and acceptance of stakeholders. Here are a few examples:

- Choice architecture methods can be used to increase the likelihood that SRM measures - e.g. SOPs, physical security measures - are adopted by making them easy, attractive, salient, and timely (the *'EAST'* principle, Halpern 2015). If the desired behaviour - for instance, incident reporting by staff in the field - is unattractive, challenging, or inconvenient then it is unlikely to be carried out. As security practitioners we must think about making the desired choice the one that meets the least resistance. Rather than security incident reporting being laborious, bureaucratic, or incurring punishment if staff fail to complete it, incident reporting could be made available via the most convenient means for the staff member (e.g. WhatsApp voice note), and in a format that is simple and convenient. Doing so would be a point of *reward* by management, and with the EAST principle in mind, reporting on incidents would be far more likely to be carried out. This can be reinforced with positive messaging to staff that praises swift incident reporting, and explains how they have contributed to organisational safety.

  Organisations can use this principle not only internally, but also to maximise the external feedback which is essential for a successful acceptance SRM approach. All too often, feedback mechanisms such as affected communities' feedback and grievance redress mechanisms are under-used due to a lack of behavioural insight; choice architecture (like EAST) can vastly improve such mechanisms, providing organisations with the grassroots understanding vital to maintaining an effective acceptance approach.

- Rather than resistance to proposed SRM approaches being an amorphous feature of security within NGOs, we now have the insights to better understand the points of friction that can result from cognitive biases and their corresponding perceptions and behaviours. Through better understanding of resistance points or the shortcomings of measures, it is easier to overcome them and thus increase buy-in. For instance, when there is a singular high-profile incident within a context (an outlier event, such as a kidnapping of a foreign national in Kabul), it is common to see disproportionate organisational reactions that are at odds with SRM advice (such as the widespread implementation of curfews despite no evidence of incidents being more likely at night). This is an example of the *availability heuristic* at work, where a vibrant and recent dramatic event becomes the driver of decision-making rather than a holistic consideration of the wider context. Individual reactions can then be reinforced and perpetuated by *social-proofing* as such measures gain traction across the wider NGO community. Being aware that such biases and errors are at play, an SRM practitioner now knows that she must address these heuristics in her communication with management, providing broad and balanced information, to help counter the visceral impact of a high-profile recent event on choices made. This can be achieved through regular security and context briefings, either dedicated or bolted on to existing management meetings, as well as other forms of regular security communications such as weekly reporting and circulation of relevant articles and analysis.

- Context, not only personal attributes such as role or disposition, can be utilised as a part of a choice architecture approach in SRM. By considering the context in which safety and security decisions and behaviours take place, practitioners can better understand staff members' choices. While the exact adaptations of SRM policy will differ from one case to another, the cognitive process remains constant. For example, group-thinking in a large stakeholder engagement meeting may undermine the nuances of an NGO's proposal, where multiple members of the local community have competing interests. By choosing a more amenable context, such as bilateral discussions with individual stakeholders in more relaxed settings, the interlocutor is better placed to create a more conducive context and gain greater acceptance, thus contributing to the safety of the NGO's operations.

- Choice architecture can be used to combat cognitive biases that cause myopia towards risk when dealing with outlier, high impact, extremely low probability events, known as *black swans* (Taleb 2007). When framing our choices and decisions we are prone to fixate narrowly on a single course of events without

Preview - don't share further

a wider perception of other outcomes, and are thus vulnerable to a host of biases. *Confirmation bias*[4] as well as the *What You See Is All There Is*[5] *bias*, can be debilitating to contingency planning and crisis management, as they fail to allow for maximum perception of and adaptation to future developments. Using exercises such as Heuer's *Analysis of Competing Hypotheses* can actively account for such biases and can widen the perspective of management when making choices under uncertainty (Heuer 1999). This can lead to more robust decision-making that incorporates a greater spectrum of outcomes, for instance when crisis management teams consider critical incidents or significant contextual developments like elections or even aggressive transitions of power. Failure in the face of critical, rare incidents is a common, albeit unrepresentative, critique to acceptance of SRM approaches, and success in this arena can greatly enhance not only organisational buy-in in the future, but also stakeholders' and communities' trust in organisational resilience, further increasing acceptance.

- Finally, a key lesson from the methodologies used in the application of choice architecture is to consider, measure, and observe peoples' *actual* behaviour, rather than what one thinks is obvious, or imagines what people *should* be doing. Therefore, SRM practitioners could greatly benefit from gaining additional understanding of the reasons driving undesired behaviour: *why* are safety procedures not being followed by staff? *Why* do management fail to integrate safety and security concerns in proposal and project design? To gain insight into these questions, SRM practitioners can use structured observation, small scale experiments, and testing of their hypotheses in different configurations of individual and group settings. Experimentation and testing not only clarifies the reasons behind the shortcomings of SRM measures, but it also engages staff and management, thus generating ownership. Introspection and the involvement of staff increases buy-in through the very process of gaining understanding.

Conclusion

Thinking and research on cognitive biases such as loss aversion, the availability and representativeness heuristics, and fundamental attribution errors can shed light on obstacles to SRM buy-in within an organisation. Armed with this knowledge, we can adjust security practices to target these obstacles, using aspects of choice architecture to facilitate desired behaviours, choices, and decisions from staff and other actors, which also helps increase acceptance. After all, acceptance as an SRM strategy often faces challenges stemming from failures to implement technical aspects of SRM. Choice architecture can equip SRM practitioners with actionable means to increase technical successes, thus maximising the organisational buy-in of security programming, including acceptance strategies.

This article presents only a fraction of the concepts and research conducted on behavioural insights, and its application in choice architecture. It does nonetheless demonstrate the role of SRM practitioners as choice architects who can utilise behavioural insights to enrich their practice and invigorate organisational buy-in of SRM strategies. This in turn leads to the safer and more effective delivery of aid and greater acceptance by stakeholders.

4 The confirmation bias refers to the habit of using new information to confirm rather than challenge or disprove existing beliefs, opinions or hypotheses (Oswald, M. & Grosjean, S 2004).

5 *What You See Is All There Is* refers to the propensity to make decisions without considering the existence of known unknowns or unknown unknowns (Kahneman 2011).

Bibliography

Cialdini, R. (1984). *Influence: Science and Practice*. New York, HarperCollins College Publishers.

Halpern, D. (2015). *Inside the Nudge Unit: How Small Changes Can Make a Big Difference*. London, Random House.

Heuer, R. (2001) [1999]. *Psychology of Intelligence Analysis* (2nd ed.). Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

Jones, E. E., & Harris, V. A. (1967). The attribution of attitudes. *Journal of experimental social psychology*, 3(1), 1-24.

Kahneman, D. & Tversky, A. (1974) Judgements of and by Representativeness in Kahneman, D., Slovic, P., & Tversky, A. *Judgment under uncertainty: heuristics and biases*. Cambridge, Cambridge University Press.

Kahneman, D. & Tversky, A. (1974) Availability: A heuristic for judging frequency and probability in Kahneman, D., Slovic, P., & Tversky, A. *Judgment under uncertainty: heuristics and biases*. Cambridge, Cambridge University Press.

Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American Psychologist*, 39(4), 341–350.

Kahneman, D. (2013). *Thinking, Fast and Slow*. London, Penguin Books.

Matsakis, L. (2019) **https://www.wired.com/story/wired-guide-personal-data-collection/** (accessed 30052021)

Melendez, S. and Pasternack, A. (2019) **https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information** (accessed 30052021)

Oswald, M. & Grosjean, S.(2004), "Confirmation bias", in Pohl, Rüdiger F. (ed.), *Cognitive illusions: A handbook on fallacies and biases in thinking, judgement and memory*, Hove, Psychology Press.

Shotton, R. (2018). *The Choice Factory: 25 behavioural biases that influence what we buy*. Hampshire, Harriman House.

Taleb, N. (2007) *The Black Swan*. New York, Random House.

Taleb N. (2018) *Skin in the Game: Hidden Asymmetries in Daily Life*. New York, Random House.

Thaler, R. & Sunstein, C. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press.