Realistic Evaluation and the 5Is: A systematic approach for evaluating security interventions.

Introduction

This chapter advocates for the security profession to adopt a more robust approach to evaluating security interventions, and furthermore, that attempts to do so should consider the utility of two under used approaches. The first of these is a wider utilisation of realistic evaluations, and the second is greater use of the 5Is framework for crime prevention. Moreover, this chapter proposes the adoption of an integrated approach that combines realistic evaluation and the 5Is framework for crime prevention. Several advantages of doing this are identified including:

- a methodical and consistent approach to designing and evaluating security interventions;
- a framework that supports security professionals to think systematically through (i) the challenges and issues they need to tackle, and (ii) the ways in which their proposed solution might go some way to addressing this;
- a greater consideration of the ways in which an intervention has/has not achieved its intended objectives, to support replication and adaption in the future to different contexts and settings;
- an understanding of how an intervention has been carried out, the steps and stages taken, and the people and organisations involved in delivering this; and,
- the adoption of user-friendly approaches grounded in their practical applicability.

The use of Realistic Evaluations and 5Is in the Security Field

Realistic evaluations were first proposed by Pawson and Tilley (1994) over 25 years ago. Compared to other fields such as public health, there is a surprising lack of uptake of these in the security profession. To date no systematic reviews have been published on the use of realistic evaluations in crime prevention or security. An initial quick search identified the use of these for evaluating a range of security interventions including: CCTV in car parks (Gill, 1999; Burns-Howell and Pascoe, 2006); drug deterrence (Leone, 2008); domestic violence (Taylor-Dunn, 2016); credit risks and fraud (Ranisavljević and Hadžić, 2016); reporting of sexual violence (Solymosi et al, 2018); and, autonomous driving (Zelle et al, 2020). Outside of the security realm, realistic evaluations have been used more extensively, perhaps none more so than public health (Marchal et al, 2012; Salter and Koathari, 2014; Gilmore, 2019; Quintans et al, 2020; and Mirzoev, 2021). A detailed consideration of possible reasons for this is beyond the scope of the chapter. However, public health evaluations receive considerably higher levels of research investment than security (Wiebe, 2021). Salter and Koathari (2014) highlight a set of challenges to conducting realistic evaluations which may in part explain the limited uptake including that: they are time and resource intensive; they lack detailed learning and guidance as to how best design the Context-Mechanism-Outcome (CMO) configurations (a discussion of these to those unfamiliar is offered later in this chapter); it is challenging to identify appropriate outcomes; and, inherent difficulties exist in systematically defining relevant contextual factors and or mechanisms.

The 5Is framework for crime prevention and community safety (Ekblom 2011) is a process model based on a set of tasks necessary to deliver effective security interventions, namely: intelligence; intervention; implementation; involvement and impact. However, like realistic evaluations, it has been sparingly used in the security field. Indeed, within policing and crime prevention, a more commonly used approach is the SARA model (Scanning, Analysis, Response and Assessment). The question that arises therefore is why the limited uptake of both realistic evaluations and the 5Is framework amongst security professionals? One possible explanation might be that there is a lack of both evaluation research and crime prevention process models in the security field, and whilst that is perhaps partially true, the direction of travel seems to be towards alternative evaluation designs and security frameworks.

In crime prevention and policing there has been a more recent drive towards adopting the so-called gold standard randomised control trials (RCTs) for evaluation (Dezember et al, 2020). This can also be directly observed in the security profession, and it could be argued that this might render realistic evaluations as old hat and out of kilt. That said, RCTs were developed as an evaluation methodology prior to realistic evaluations so they are not a particularly new approach either. RCTs are useful for providing robust evidence as to whether an intervention achieved its outcomes, or if it was cost effective. They do not offer further guidance as to how it was delivered, what made it successful, and are inadequate when evaluating interventions in multiple settings (Bullock and Tilley, 2009). RCTs offer limited clues as to the potential to replicate an intervention in a different place and context, particularly if few RCT evaluations have been undertaken, and these have been applied in limited settings. Security is a rapidly moving field, and those tasked with responding to security vulnerabilities cannot wait around for an RCT evidence base to build up. Therefore, a substantial upscaling of RCT evaluations is necessary before security practitioners can have confidence in the likely success of an intervention. Moreover, this would be based on the interventions demonstrated as being generally effective, resulting in a leap of faith that they will work in their local setting.

Within the Policing Profession, especially in the UK, there has been a recent resurgence of Problem Orientated Policing Approaches (POP) linked to problem solving. Internationally, there has been recognition of POP as illustrated by the award of the Stockholm Prize to its founder, Herman Goldstein (Goldstein, 2018). A recent systematic review of POP suggested it is a highly effective strategy for reducing crime and disorder with relevance for security professions. Indeed, in their analysis, Hinkle et al, (2020) identified 39 studies from 2006 to 2018 that met the eligibility requirements of their systematic review, of those 24 were appropriate for meta-analysis, and they found crime reduction interventions using POP were associated overall with a 30% reduction in crime.

The resurgence of POP is highlighted here as a reminder of institutional and organisational memory loss, and, furthermore, that we should not discount realistic evaluations or the 5Is, despite their lack of uptake by security professionals. The 5Is framework has been criticised as being complex and more time consuming than SARA, and realistic evaluations have also faced similar criticism compared to other evaluation designs (Salter and Koathari, 2014). Alternatively, SARA can be challenged for lacking sophistication (Ekblom, 2006), and as discussed above, alternative evaluation designs have several limitations, not least in identifying likely transferability and replication to other settings. The recent HM Treasury Magenta Handbook (HM Treasury, 2020a) provides some excellent overviews and guidance on a range of evaluation designs available, and it is worthy at this point of highlighting the supplementary appendix (HM Treasury, 2020b) which is a detailed contemporary guide on using realistic evaluations. Given its lack of uptake for security evaluations, perhaps this may serve as a timely reminder to those in the security profession of their relevance.

To support an evidence-based approach, a range of UK government 'what works' centres have arisen. Indeed, there are now nine 'what works centres' and three affiliated networks including health and social care, education, crime reduction, early intervention, local economic growth, ageing, wellbeing, homelessness, social care, youth offending, youth employment, and higher education. Whilst these serve as a useful reference point for identifying best practice, they have several limitations. Indeed, one of the key challenges when designing a new security intervention is attempting to draw from the 'what works' evidence base, given previous interventions will generally have been delivered in a different setting and context. Some efforts to address this include the adoption of realistic evaluations in the What Works for Children's Social Care, and the EMMIE framework adopted by the College of Police What Works for Crime Reduction (Johnson et al, 2015).

Given the limited what works evidence-base in the security field (Brown et al, 2018 Tompson et al, 2020), this chapter begins to explore why the additional effort of adopting a realistic evaluation and 5Is approach might be worthwhile. Moreover, it is suggested that combining these two approaches offers a systematic and highly flexible approach to evaluation. Afterall, the 5Is is more than a set of steps to support intervention delivery and evaluation. It is a knowledge framework designed specifically to help practitioners share knowledge, best practice, and learning (Ekblom, 2011). It was also developed to inherently address the mechanisms and context elements of realistic evaluations, as it incorporates the Conjunction of Criminal Opportunity (CCO) framework (Ekblom, 2018). Therefore, this chapter calls for a reconsideration of the value of both these approaches and offers a detailed discussion of how they can be complementary and, when combined, can add considerable value.

Security professionals and the challenges of evaluation

Evaluation can take many forms, and definitions vary considerably across different disciplines and areas of practice. Perhaps a useful starting point is to consider evaluation as a *systematic process to determine the value, merit, effectiveness, or worth or a particular action*. For this chapter, these actions are considered as those intended to improve the security of a particular setting or place and associated users. Security is considered in a broad sense consistent with the ethos of this handbook as discussed in the Introductory Chapter. In terms of actions designed to improve security, for consistency this chapter will term these as *security interventions*. These may also be considered security programmes, schemes, measures, or other activities and actions designed as a response to an identified security threat or weakness. Examples may include the use or adoption of a new technological solution, manipulation of modification of the design of an environment, training of staff, a revised set of standard operating procedures, increased protection of IT systems, social engineering, education, awareness raising, or alarms and security patrols. For consistency, in this chapter these are grouped under the umbrella of *security interventions*, and the purpose of most evaluations is to ascertain whether an intervention has achieved its objectives.

Evaluation is not straightforward, and a myriad of methodologies exist as to how to go about conducting an evaluation. A basic starting point here is to ask did it work and, in essence this is the thrust of what any evaluator is trying to identify. However, as will become apparent in this chapter, evaluations require a much more nuanced approach. For example, even if an evaluator identifies an intervention as successful, this may not help when attempting to replicate this intervention in another area. More pertinent questions include: who was involved; what did the intervention deliver; what elements of the intervention worked well; what was the context in which it was delivered; and to what extent was it successful?

The appropriateness of any evaluation strategy will depend not only on the type of intervention, but what exactly the evaluator is trying to find out about it. Conventionally, evaluation is divided into outcome (also termed summative impact) and process evaluation. Process evaluation is designed to explain how a security intervention has been delivered and should cover the entire sequence of activities leading up to the planning, initiation and maintenance of specific interventions and supporting tasks such as training and mobilising other stakeholders. It is used to answer the question *what can be learned from how the intervention was delivered* (HM Treasury, 2020a). Outcome evaluation determines the extent to which the impact of an intervention in the real world can be directly attributed to that intervention. It determines *what difference an intervention has made* (HM Treasury, 2020a). A range of potential alternative evaluation functions exist including pilot, efficacy, effectiveness, developmental, and contribution evaluations. For a useful overview of evaluation designs the reader is referred to the Magenta Book (HM Treasury, 2020a). These are beyond the scope of this chapter and not considered here. As a broad rule of thumb, the appropriateness of evaluation design will be governed by the purpose of an intervention, and the associated questions that the evaluation is attempting to identify. To consider some of the specific challenges of evaluating security interventions, we return to consider process and outcome evaluation in more detail.

Challenges for outcome evaluations of security interventions include examining the impact of multiple interventions (e.g., layered security), lack of statistical power when small scale interventions are introduced, and restrictions due to the sensitive nature of some interventions, for example in counterterrorism. Process evaluations have their own limitations (Ekblom 2011; Ekblom & Pease 1995). Assessments of the diverse implementation tasks that make up individual security interventions are patchy and haphazard, and findings hard to retrieve and integrate. Indeed, the chance to learn from failures is often missed. Evaluations of security interventions rarely contain sufficient consideration of context, required to make an informed judgement about their transferability. For evaluation to inform practice it must be of sufficiently robust methodological quality, context sensitive for transfer to alternative settings, and organised into a rich, retrievable body of knowledge (Bullock & Ekblom 2010). Moreover, a security culture of urgent response rather than evaluation, inadequate training and guidance on evaluation principles, techniques, and agendas, and the challenges of evaluating complex multi-layered interventions have all contributed to a lack of robust evaluations of security interventions. Security professionals cannot wait for a body of rigorous evaluations to be built up before they can act. Evaluation is complex and errors of inference easily made. Forcing practitioners to sit through protracted courses is not feasible. When a limited evidence base exists, we should encourage security professionals to be innovative, but at the same time this should be theory driven and robustly evaluated.

To fill this significant knowledge gap, approaches to ‘what works’ will trade-off coverage against quality. Alternative approaches to help bridge this gap include identification of causal mechanisms, for example realistic evaluation (Pawson & Tilley 1997) and Theory of Change (Serrat 2017). This chapter proposes the use of realistic evaluation combined with the 5Is Framework for Crime Prevention as an overarching set of principles that can be used to empower practitioners to grow evaluation knowledge. It is proposed that security professionals can use these techniques and principles to support them in designing, commissioning, and conducting evaluations of security interventions.

Realistic Evaluation

Realistic evaluation (Pawson and Tilley, 1994, 1997) was constructed with the intention of understanding the effectiveness of an intervention, using an approach that ensures the findings of any evaluation are directly transferable to practice. It therefore to some extent bridges the gap between process and outcome evaluations, as it attempts to measure both (i) whether the intervention's intended outcomes have been achieved, and (ii) at the same time understand to what extent the intervention is attributable to any measured change and the processes by which that change was brought about. Realistic evaluations are designed to ask what works, how, why, and in what situation. Thus, they are particularly informative for evaluating security interventions, considering the field's weak evidence-base compared to other disciplines. As Pawson and Tilley (1994) state it allows you to ''remember A', 'beware of B', 'take care of C', 'D can result in both E and F', 'Gs and Hs are likely to interpret I quite differently', 'if you try J make sure that K has also been considered." As specified by HM Treasury (2020b) they are particularly suited to evaluating new interventions and trials, for understanding how to apply the learning of evaluation to adapt to new intervention contexts, and to offer a better understanding of interventions that have previously been evaluated with mixed results. They are less relevant in evaluating interventions where there is a good degree of knowledge about how, why, and where they work, and when there is limited requirement to understand how an intervention has worked. Given the lack of robust evaluations of security interventions, it is suggested that in the security realm currently, these latter two will rarely apply.

Realistic evaluation focusses on three primary components. These are the **C**ontext within which an intervention is implemented; the **M**echanisms by which the intervention might achieve change, the how; and, the intended **O**utcome of the measure introduced, or what success might look like. These are often referred to as the **CMO** configurations of realistic evaluation. To put this in layman's terms the evaluator is testing did an intervention work, how did it work, what situation was it delivered in, and what were the processes that it used to deliver this identified change.

Realistic evaluation is starkly and proudly theory driven, and theories of change fundamentally underpin its design. Whilst this may not initially appeal to the security professional in a rapidly evolving field, a pause for reflection might give time to consider the benefits of this. If we consider theory as a set of beliefs or assumptions that underpin action (Weiss, 1997), then this offers a frame of reference through which a security practitioner can understand what security issue needs addressing and why they think their solution will go at least some way towards resolving this. Afterall, if an evaluator is to unpick how an intervention has been implemented, a first stage is to clearly ask why it was implemented in the first place.

There are some parallels with the use of logic models now widely advocated in the evaluation literature (Smith, Li, and Raffery, 2020). Logic models are diagrammatic representations of the resources, activities, outputs, outcomes, and impact of an intended intervention. They are like theory of change models, but logic models and similarly systems change models are perhaps better suited to evaluating large programme interventions and strategic perspectives (Blamey and Mackenzie, 2007). Realistic evaluations are appropriate to evaluating security interventions as they require the designers of an intervention to formalise the development of theory testing. They go beyond logic models by asking those responsible for the security intervention to unpack which mechanisms are triggered in different contexts, and how they might lead to differential outcomes. They are required to methodically think through the conditions needed for an intervention to trigger the intended outcome. This is pertinent when trying to establish the outcomes of a set of likely multi-layered interventions present in most security interventions. It requires the design of interventions to include precise terms and definitions, and a lack of standard terminology has been problematic in the security field (Ekblom and Sidebottom, 2008).

Pawson and Tilley (1994, 1997) consider mechanisms to be a combination of the resource offered by an intervention, and the participants reasoning as a response to this. Therefore, this is considered a generative mechanism linked to both a human agency and the mechanics of an intervention. This chapter will return to discuss this when examining the 5Is crime prevention framework in more detail. The reasoning of CMO is that the mechanisms (of change) will only activate under certain conditions. To achieve this requires an understanding of both context and its fluidity of change, to understand what works, for whom, in what circumstance, and why. The benefit of this causative design is that if offers greater promise in understanding the potential transferability of a security intervention than other approaches, and therefore is grounded in its practical applicability and the likelihood of successful replicability.

Realistic evaluations may usefully consider the inputs, outputs, and outcomes of an intervention. Inputs can be considered as ‘what is used to do the work’, the resources that have been applied to carry out the identified intervention tasks including finance, materials, and time, for example additional security patrols, better physical security. The outputs refer to *what is produced or delivered* and relate specifically to the products and services that have arisen out of the intervention actions, a direct result as it were of the inputs. The outcomes relate to *what the intervention intends to change in the real world* and are a more longer-term goal than the outputs. Examples might include reduction in levels of violence, improved mental wellbeing, or a reduction in cyber-attacks.

An outcome evaluation seeks to identify the extent to which a security intervention achieved its intended long-term goals. A process evaluation unpicks the relationship between intervention inputs and outputs to identify how outcomes occurred and therefore both are necessary for a realistic evaluation. These inputs, outputs and outcomes can be considered against the identified theory of change, the context within which an intervention is implemented, and the casual mechanisms of change by which an intervention achieved its outcome(s). This process is depicted in Figure 1.

A further advantage of realistic evaluation designs is that they allow a recognition that interventions are likely to be developed from previously trialled ideas, be it in a different context, on a smaller scale, or from a different discipline. It encourages the designers of the intervention to think through this when specifying context-mechanisms-outcomes. Therefore, it is highly flexible and adaptable for security professionals who can (i) use mechanism of change principles to transfer ideas to new contexts, and (ii) to adapt replication as an innovative approach.

Insert Figure 1 about here

The 5Is framework for crime prevention

The 5Is framework (Ekblom, 2011) was developed as a practice orientated tool to transfer and share crime prevention and community safety knowledge. Indeed, its primary function is to be a knowledge framework to capture, assess, consolidate, and replicate good practice. However implicit in the identification of good practice is a need for robust evaluations of security interventions. The 5Is can be considered to have a broad range of functionality including: a checklist for steps required in designing and carrying out the security intervention; as a gap-analysis of our existing understanding; to learn from failure and success; as a training tool for practitioners to support structured thinking about crime prevention; and as a way of encouraging communication and collaboration between security professionals with a range of backgrounds and disciplines. Therefore, the 5Is is '*an advanced framework for capturing, consolidating and sharing knowledge of good practice in crime prevention. It aims to improve performance, scope and delivery of that practice locally, nationally and internationally, enabling smarter responses with reduced resources (Ekblom, 2011)*'.

Ekblom (2014) covers in detail what knowledge of crime prevention (here translated to security interventions) should incorporate. When specifying what we need to know he identifies seven key characteristics of relevant knowledge including: a local understanding of identified security problems; an understanding of what works; an understanding of who should be involved in implementing security interventions; an understanding of appropriate timings to intervene; an understanding of how to target and distribute resources an understanding of context and local ethical and cultural meanings of security; and an understanding of how to translate this knowledge into practice. The 5Is can is therefore a set of tasks devised to deliver effective security interventions broken down as intelligence; intervention; implementation; involvement and impact. Each is briefly considered below.

Intelligence refers to the need to understand the local nature of the security challenge identified. What are the causes of this, what is the local context, what problem exactly is the intervention attempting to address? In this sense Ekblom aligns with the principles of Ratcliffe's (2008) definition of intelligence drawn from policing, which suggests a need to distinguish between data (observations and measurements of indicators); information (data translated into understanding local relevance); knowledge (an understanding of local mechanisms); and intelligence, that used knowledge to guide action. Any theoretically driven response to an identified security issue requires a detailed understanding as to the nature of the identified security issue.

Intervention relates to the design and planning of the identified action as a response to the intelligence gained in the previous step. This may include an overall intervention strategy, and a set of distinct individual interventions subsumed within this. These are often referred to as layered interventions. Fundamentally, intervention is about how to block, weaken or deflect the causes of criminal events, or alternatively put, how to frustrate the intentions and actions of offenders. There are likely to be multiple considerations here including: pre-planning, steps required to take the intelligence to an intervention; the organisation structure and local context of delivery; and the design process of the intervention itself. An important stage here is the theory behind the proposed interventions, why should it work, and what are the outcomes it expected to achieve.

Implementation relates to the process of putting identified interventions into practical action, and incorporates the input of resources, and the processes of delivering an output leading to an intervention including planning, management, organisation, monitoring and quality assurance of the actions. Implementation goes hand in hand with involvement in the 5Is process and this considers the persons involved with delivering a security intervention.

Involvement considers the mobilisation of organisations and individuals to deliver an intervention, including partnership working. Indeed, Ekblom considers involvement and mobilisation as a key component the 5Is, and, after all, no security intervention is likely to succeed without the will and skill of those implementing it. Ekblom highlights the use of the CLAIMED steps for mobilisation (Ekblom, 2011) which comprise: **C**larifying roles and tasks; **L**ocating appropriate preventive agents or persons; **A**lerting relevant persons to the identified security challenge or issue which may include offenders; **I**nforming them of potential consequences of harm of their actions; **M**otivating them to change their or others' behaviour; **E**mpowering them to make change which may include resource support; and, **D**irecting them to standards and rules that they should adhere to. Understanding implementation and involvement can be considered as central components of any process evaluation as outlined previously in this chapter.

The final task outlined in 5Is is *Impact*, which may include intermediate impacts and more long-term outcomes of an intervention. To what extent has a security intervention achieved its outcomes, and how attributable are any changes identified to that intervention? In the 5Is approach impact is considered to include process evaluation and outcome evaluation, and thus Ekblom suggests that understanding the 'how' of implementation and involvement (process) are a necessary part of identifying the extent to which an intervention had a casual impact in responding to the security challenge identified. Indeed, it could be argued that realistic evaluation and the 5Is are complementary frameworks for evaluating security interventions, and it is this harmony that this chapter now begins to unravel.

Combining Realistic Evaluation and the 5Is?

The 5Is framework Ekblom (2011) outlines a set of steps for each of the 5Is, and it is useful here to draw from the specific elements of these and how they complement and support a realistic evaluation approach. When breaking down the tasks involved in the *Intelligence* component of the 5Is, these include: an understanding of the geographical and social context of the security problem and an understanding of the type of security challenge and previous patterns of susceptibility; the tactics employed to bypass or overcome security; the timing and spatial pattern of previous incidents if applicable; and the local physical and social environs within which these have occurred. Further consideration includes the data, information, and knowledge used to understand the local security challenges; and an assessment of the possible significant harmful consequences that could occur because of exploitation of a security vulnerability. Translated into realistic evaluation, these are all issues that support a contextual understanding of the security issue and are required to develop a theory-based approach to identify possible appropriate solutions for the specific security situation identified. Here there is clearly duality with realistic evaluation in terms of drawing from theory and understanding context within realistic evaluation.

A further consideration of the steps used in the design of the *Intervention* phase of the 5Is, which is effectively the design of the appropriate response to the security issue identified in the previous intelligence stage. What intervention, or set of interventions are likely to be most appropriate to address this? This draws on a theory-based approach and in some ways is like using logic models which in simple terms can be considered each of the steps required to achieve change drawn in a flow diagram (Seratt, 2017). However, realistic evaluations and the 5Is approaches require a greater level of detail that spells out for each step the C- M-O process. This should include a specification of the intended inputs, outputs, and outcome metrics of an intervention, and how the generative mechanisms of change will achieve these outcomes given local and fluid context. A clear overlap between 5Is and realistic evaluation here is the necessity to use consistent and clear terminology (Ekblom and Sidebottom. 2008), and several examples can be identified where the security field has not articulated or used a clear glossary of terminology in its approach. Two of the 'big three' possible errors in evaluation design are theory failure and implementation failure. Clearly intelligence and intervention are crucial to getting the theory right. However, if an appropriate theory is used to inform an intervention, but the tasks are not clearly articulated and explicitly specified for the security professionals and partners who will likely have a diverse background of disciplines, then the potential for implementation failure grows exponentially. This applies to the likelihood an intervention is not carried out as prescribed or implemented within the appropriate context it was designed for. For reference the third failure to avoid is measurement failure, whereby the research design is not sensitive to detect changes, or the scale of the intervention does not enable change to be detected within its wider context.

When considering *Implementation* necessary steps include; the targeting of appropriate security action; tailoring of the intervention to specific local context; possible cycles of action; and management, planning and organisation of an intervention. In addition, *Involvement* requires a consideration of tasks carried out by organisations, individuals and partnerships, the mobilisations of each of these, any constraints and challenges for mobilisation; local climate of acceptance for security measures; accountability; capacity building; and communication. A key role within the 5Is is process evaluation, which is discussed by Ekblom as part of *Impact* but is highlighted here as it is effectively an understanding of *Implementation* and *Involvement,* the involvement of people and organisations supporting the intervention. Steps for these include to: identify the extent to which each task of the intervention was achieved; examine if the task was delivered to an appropriate quality; identify levels of involvement in each task and the specific role of each individual, organisation and or partnerships;

and, to understand any problems or obstacles faced and how these were overcome. When considering how these integrate into a realistic evaluation, it is pertinent to recall that this generative causality model seeks to identify specific conditions or readiness whereby the mechanisms of change can be successful. Indeed, the realistic evaluation framework suggests mechanisms are generally more attributable to human agency (involvement) than the mechanics of a security intervention (implementation – e.g., the kind of material used for a security door) but that both need due consideration. Here there is clear mutual synergy between the two frameworks given the prominence of context and readiness for change.

The final strand of the 5Is is *Impact*, sometimes referred to as outcome evaluation. Steps for this include identifying: the extent to which the intervention achieved its aims and objectives, generally measured by the outcome metrics; any changes in intermediate and ultimate outcomes; how attributable these are to the intervention; the sustainability of the intervention; and an understanding of context delivered and main 'ingredients' necessary for the success of the intervention. These latter two require careful elicitation from the process evaluation hence Ekblom's inclusion of process evaluation within Impact. Again, there are parallels with realistic evaluation as these *Impact* steps could all be written as steps to understand the CMO process. Moreover, Pawson and Tilley (1994, 1997) suggest that realistic evaluation requires: a pragmatic approach to identifying appropriate data collection methods; a pluralist approach to the selection of methods incorporating both quantitative and quantitative approaches; and that these should be appropriate to the hypotheses tested for evaluation.

Insert Figure Two about here

A Hypothetical Worked Example

The following is based on a fictitious scenario, and the author is not aware of this bearing resemblance to any currently identified case study, and it is purely co-incidental if this is the case. The scenario is around the distribution and supply of Covid-19 vaccinations, and an identified loss of vials at a regional distribution centre. The challenge is therefore how to secure these vials without disrupting the supply chain process.

Using Figure 2, the first stage of designing and evaluating a security intervention - using the realistic evaluation and 5Is approach - is *Intelligence*. What data, information and knowledge are available to understand the local problem. Where are the losses occurring, is there a pattern to this, when and where is this happening, what is the (likely) modus operandi of the offender, what is the scale of the problem, and what is the local context where it is happening. It is identified from analysis of data that loss occurs on regular basis consistent with shift patterns, but due to the number of staff involved in the logistics of the Covid-19 vaccination vials distribution, there are over 100 persons whose shift timings can be linked to this pattern. Moreover, due to staff wearing facemasks and the lack of CCTV cameras it is extremely difficult to use these to detect loss. The cameras were installed for previous products which were larger hence there are fewer than needed, several blind spots exist, and cameras are positioned inappropriately. Therefore, whilst insider threat is a distinct possibility, it is not the only loss as incidents have been recorded both at the distribution warehouses and on attacks to individual trucks distributing these to local vaccination centres. However, the loss on freight vehicles is at a smaller scale, less frequent, and more sporadic and no clear patterns here can be identified. This is all key information to understand the local context of the loss of vials.

Drawing from theoretical principles, the next step in Figure 2, suggests there are two distinct issues that need security interventions. The first is loss or theft of vials at the distribution centre itself, and the second is loss on local freight during transport. It is not known if these are linked; there is a strong possibility of insider threat given there are access controls in place at the distribution centre, and that interceptions targeting virus vials on moving vehicles is likely to require some pre-planning by offenders in terms of an awareness of the route and timing of delivery to local vaccination clinics. This suggests information on the logistical operations may not be secure. It is identified that a situational approach (Clarke, 1995) may be an effective approach to securing the vial stores in the warehouse distribution centre, the information on freight routes and timing of deliveries, and for adding improved security to the freight vehicles themselves. The loss of vials is considered an opportunistic threat, exploiting vulnerabilities that have arisen from the need to distribute vials rapidly during a pandemic. Therefore, interventions drawn from opportunistic explanations of theft are considered most appropriate.

Step three is to design the interventions. It is evident there are three security vulnerabilities to address: loss of vials at regional distribution warehouses; possible insider sharing of route planning; and vulnerability of the freight used whilst in transit to deliver vials to local vaccination clinics. In discussion with local operators and drawing from the evidence on situational crime prevention the following interventions were identified as appropriate. Intervention One is wireless controlled access at warehouses linked to operator provide mobile phones with biometric security for each individual user. Intervention Two is for ‘security by obscurity’ – direct sharing of routes through encrypted wireless transfer to share each route only with the drivers of that vehicle to non-personal satellite navigation devices which are sent ten minutes before the delivery starts. Route planning occurs on secure devices and each route request is logged. External communication is removed from these route planning PCs except for transfer of final route information. Intervention Three is to add tracking devices and covert panic alarms linked directly to local police operators to freight vehicles, and to ensure drivers only park in secure parking which is linked to their navigation device, and locked trailer doors requiring controlled access via GPRS and inaccessible during routes. They can only be activated at end point.

The CMO configurations for each of these are described only briefly here as this is a scenario-based example. Firstly, controlled wireless access has been added to the regional warehouses. The mechanism of change is that entry and exit is timed, there is biometric linkage of access to individual mobile devices, and NFC technology allows movement to be tracked within the warehouse. Moreover, the warehouse is broken down into smaller subsections with the same wireless controlled access so users will need to always carry their device. Direct communication and training are provided to all staff requiring access, and any theft or loss will be narrowed down to a small number of persons due to these multiple tracking systems. Previously card/fob entry was used but not linked to individual persons and these could easily be lost and swapped, so the intervention should not slow down operational logistics. For Intervention Two the context is the security of the route planning information, which is electronic. Additional layers of security have been added to restrict potential leaking of this information, with a secure point to point transfer between route planner and driver the only possible communication from these devices. This mechanism will stop unauthorised sharing of this information. The final security added is to freight itself on the journey (context) and the mechanisms of change are to increase efforts required to intercept vehicles through GPS tracking of journeys, alarms linked to local police systems, and GPRS locking of freight that can only be opened at end-delivery points. The outcomes are a reduced level of vial loss.

The next stage of this process is to evaluate implementation and involvement, and this would be done to understand if the mechanisms of change were triggered within the context of each of the three proposed solutions. It can be considered as part of a process evaluation of the interventions. Where 5Is is useful here is that is separates implementation from involvement as detailed previously. It is argued this is akin to the realistic evaluation process of examining the mechanisms of the intervention and the role of human agency in this. For each intervention, a detailed breakdown is needed in terms of what was delivered, and when. How were staff mobilised to engage with this? What obstacles were faced? How were they resolved? This detailed picture is necessary if outcomes are to be linked to the activation of a set of mechanisms within the context within which they were applied; and for this to be replicable.

The final stage is to assess if the outcomes were realised. That is, has there been an overall reduction in the number of vial losses? This could be further examined within each of the three contexts, including loss at warehouse, unauthorised sharing of route information, and loss of vials from vehicles. It is noted here that this is a multi-layered strategy; thus, there is a need to try and identify which of the interventions were successful, and the extent to which this can be attributed to the intervention. One of the challenges is identifying whether it was protection of route information, or extra security of vehicles which was the effective mechanism for reducing loss from vehicles in transit. One method to separate these two is to analyse whether attacks on vehicles were still happening post implementation, but these were less successful – suggesting unauthorised sharing of information was still occurring. A range of statistical tests may be considered, and the evaluation designer needs to consider the least biased approach when attempting to account for the counterfactual. What would have happened if the interventions were not introduced? In some instances, quasi-experimental design may be possible, and this should be considered at the intervention design stage. If so a range of tests could be considered including propensity score-matching, interrupted time series analysis, regression discontinuity design and difference in difference regression. If appropriate controls are not possible alternative approaches may be to use pre and after intervention data, triangulated with the findings of the process evaluation. if there is evidence for the occurrence of a particular process/mechanism that is necessary for the successful outworking of logic model, that strengthens and sharpens the evaluation findings. Likewise, impact in the *absence* of a particular conjectured mechanism can rule out the latter's substantive contribution and guide the choice of/search for alternative mechanisms. All of which is useful knowledge for intelligent replication of the action in other contexts and/or for related problems

Conclusion

This chapter has advocated for the security profession to adopt a more systematic approach to evaluation to support the currently weak what works evidence base. Many evaluations likely remain unpublished and inaccessible, therefore several opportunities for learning and replication are missed. The chapter also suggests that use of a combined approach, utilising realist evaluations with the 5Is as a complementary and systematic approach to do this. In doing so this chapter offers a potential framework whereby security practitioners can: think methodically about interventions they design and why they might work linked to theories of change; try to understand the context and setting of the situation they are trying to address; can consider the steps taken in the intervention and those involved in delivering it; and consider an up-front rather than retrospective evaluation design that attempts to identify not only whether an intervention was successful, but also the mechanisms by which this change was brought about. The 5Is also supports dissemination of this knowledge and considerations of the replicability of this intervention to other contexts and situations.

Recommended readings

The most comprehensive account of realistic evaluations is Pawson and Tilley (2007): Pawson, R., & Tilley, N. (1997). Realistic Evaluation. London: Sage.

For a detailed discussion of the 5Is framework see Ekblom (2011): Ekblom, P. (2011) Crime Prevention, Security and Community Safety Using the 5Is Framework. Basingstoke: Palgrave Macmillan.

For overviews of evaluations see the HM Treasure Magenta Handbook (2020): HM Treasury (2020a) The Magenta Book: HM Treasury guidance on what to consider when designing an evaluation; and for additional discussion of realist evaluation see the supplementary guide: HM Treasury (2020b). Magenta Book 2020. Supplementary Guide: Realist Evaluation.

References

Blamey A, Mackenzie M. Theories of Change and Realistic Evaluation: Peas in a Pod or Apples and Oranges? Evaluation. 2007;13(4):439-455

Brown J, Belur J, Tompson L, McDowall A, Hunter G, May T (2018). Extending the remit of evidence-based policing. International Journal of Police Science & Management. 20(1):38-51.

Bullock, K. and Ekblom, P. (2010) ‘Richness, retrievability and reliability – issues in a working knowledge base for good practice in crime prevention’. European Journal on Criminal Policy and Research, 16, 29-47.

Bullock, K., & Tilley, N. (2009). Evidence-based policing and crime reduction. Policing, 3(4), 381-387.

Burns-Howell, T. and Pascoe, T. (2004). Crime Prevention Evaluation: A Realistic Framework Based on Experience and Reality. *Criminology & Public Policy*, 3: 527-534.

Clarke, R. (1995). Situational Crime Prevention. Crime and Justice, 19, 91-150.

Dezember, A., Stoltz, M., Marmolejo, L., Kanewske, L., Feingold, D, Wire, S., Duhaime, L. and Maupin, C. (2020). The lack of experimental research in criminology—evidence from Criminology and Justice Quarterly. Journal of Experimental Criminology https://doi.org/10.1007/s11292-020-09425-y

Ekblom, P (2006) ‘Good practice? Invest in a Framework!’ Network News, Spring 2006. Chester: National Community Safety Network.

Ekblom, P. (2011) Crime Prevention, Security and Community Safety Using the 5Is Framework. Basingstoke: Palgrave Macmillan.

Ekblom, P. (2018). ‘From threat to debt… or, there is mechanism in my madness’. In G. Farrell and A. Sidebottom (Eds) Realist Evaluation for Crime Science: Essays in Honour of Nick Tilley. Milton Park: Taylor and Francis. 58-75.

Ekblom, P. (2014). 'Securing the knowledge' in M.Gill (ed.) The Handbook of Security (2nd Edn). Basingstoke: Palgrave MacMillan

Ekblom, P., and Pease, K. (1995). Evaluating crime prevention. In: M. Tonry, D. Farrington (eds.), Building a Safer Society: Strategic Approaches to Crime Prevention London/Chicago, University of Chicago Press, pp. 585–662 Crime and Justice: A Review of Research, vol. 19

Ekblom, P and Sidebottom, A. (2008) ‘What do you mean, ‘Is it secure?’ Redesigning language to be fit for the task of assessing the security of domestic and personal electronic goods.’ European Journal on Criminal Policy and Research, 14:61–87

Gill, M., & Turbin, V. (1999). Evaluating ‘realistic evaluation’: Evidence from a study of CCTV. In R. V. Clarke (Ed.), *Crime Prevention Studies*: Vol. 10 (pp. 179–199). Monsey.

Gilmore B (2019). Realist evaluations in low- and middle-income countries: reflections and recommendations from the experiences of a foreign researcher. BMJ Global Health; 4:e001638

Goldstein, H. (2018) On problem-oriented policing: the Stockholm lecture. Crime Science 7, 13.

HM Treasury (2020a) The Magenta Book: HM Treasury guidance on what to consider when designing an evaluation.

HM Treasury (2020b). Magenta Book 2020. Supplementary Guide: Realist Evaluation. [Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/879435/Magenta_Book_supplementary_guide._Realist_Evaluation.pdf]. Last Accessed: 5th May 2021

Hinkle, JC, Weisburd, D, Telep, CW, Petersen, K. Problem-oriented policing for reducing crime and disorder: An updated systematic review and meta-analysis. Campbell Syst Rev. 2020; 16:e1089.

Johnson, S.D., Tilley, N. & Bowers, K.J. (2015). Introducing EMMIE: an evidence rating scale to encourage mixed-method crime prevention synthesis reviews. Journal of Experimental Criminology 11, 459–473

Leone L. (2008) Realistic Evaluation of an Illicit Drug Deterrence Programme: Analysis of a Case Study. Evaluation. 14(1):9-28.

Marchal B, van Belle S, van Olmen J, Hoerée T, Kegels G (2012). Is realist evaluation keeping its promise? A review of published empirical studies in the field of health systems research. *Evaluation*.18(2):192-212

Mirzoev T, Cronin de Chavez A, Manzano A, et al (2021) Protocol for a realist synthesis of health systems responsiveness in low-income and middle-income countries. BMJ ; 11:e046992

Pawson, R. and Tilley, N. (1994). What works in evaluation research? British Journal of Criminology, 34(3), pp.291–306.

Pawson, R., & Tilley, N. (1997). Realistic Evaluation. London: Sage.

Quintans, J. R., Yonekura, T., Trapé, C. A., & Soares, C. B. (2020). Realist evaluation for programs and services in the health area: an integrative review of the theoretical and methodological literature. Revista latino-americana de enfermagem, 28, e3255.

Ranisavljević, D. and Hadžić, M. (2016) "Realistic Evaluation of the Ratio: Loan-To-value – The Key to Minimising the Credit Risk" Economic Themes, vol.54, no.3, , pp.449-468.

Ratcliffe, J. H. (2008). Intelligence-led policing. Cullompton, Devon: Willan

Salter, K.L., Kothari, A. (2014) Using realist evaluation to open the black box of knowledge translation: a state-of-the-art review. Implementation Sci 9, 115

Serrat O. (2017) Theories of Change. In: Knowledge Solutions. Springer, Singapore

Smith, J., Li, D. & Rafferty, M. (2020) The Implementation Research Logic Model: a method for planning, executing, reporting, and synthesizing implementation projects. Implementation Science 15, 84

Solymosi, R., Cella, K. & Newton, A (2018). Did they report it to stop it? A realist evaluation of the effect of an advertising campaign on victims' willingness to report unwanted sexual behaviour. Security Journal 31, 570–590.

Taylor-Dunn H. (2016). The impact of victim advocacy on the prosecution of domestic violence offences: Lessons from a Realistic Evaluation. Criminology & Criminal Justice. 16(1):21-39.

Tompson, L. Belur, J., Thornton, A., Bowers, K.J., Johnson, S.D., Sidebottom, A., Tilley, N. & Laycock, G. (2020). How Strong is the Evidence-Base for Crime Reduction Professionals? Justice Evaluation Journal. 4:1, 68-97

Weiss C (1997). How Can Theory-Based Evaluation Make Greater Headway? *Evaluation Review*. 21(4):501-524.

Wiebe, D. (2021). How can paths be risky. Paper Presented to International Seminar Series: Risky Places for Crime. [Available online]. https://play.kth.se/media/Risky+PlacesA+How+paths+can+be+risky.+Professor,+Douglas+Wiebe./0_21glhmqe Last accessed 8th May 2021.

Zelle, R. Rieke, C. Plappert, C. Krauß, D. Levshun and A. Chechulin, (2020). SEPAD – Security Evaluation Platform for Autonomous Driving, 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), pp. 413-420

Figure 1: A Schematic of the Realistic Evaluation Approach

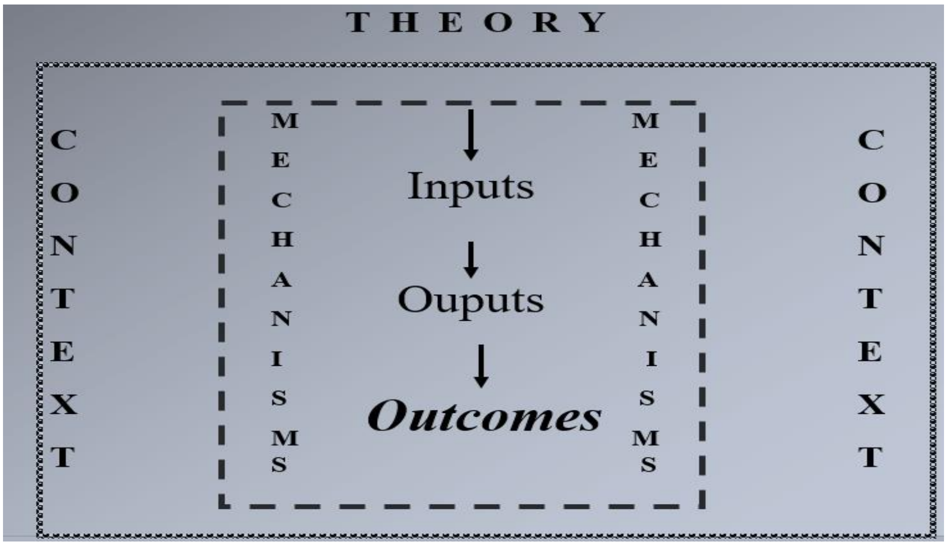
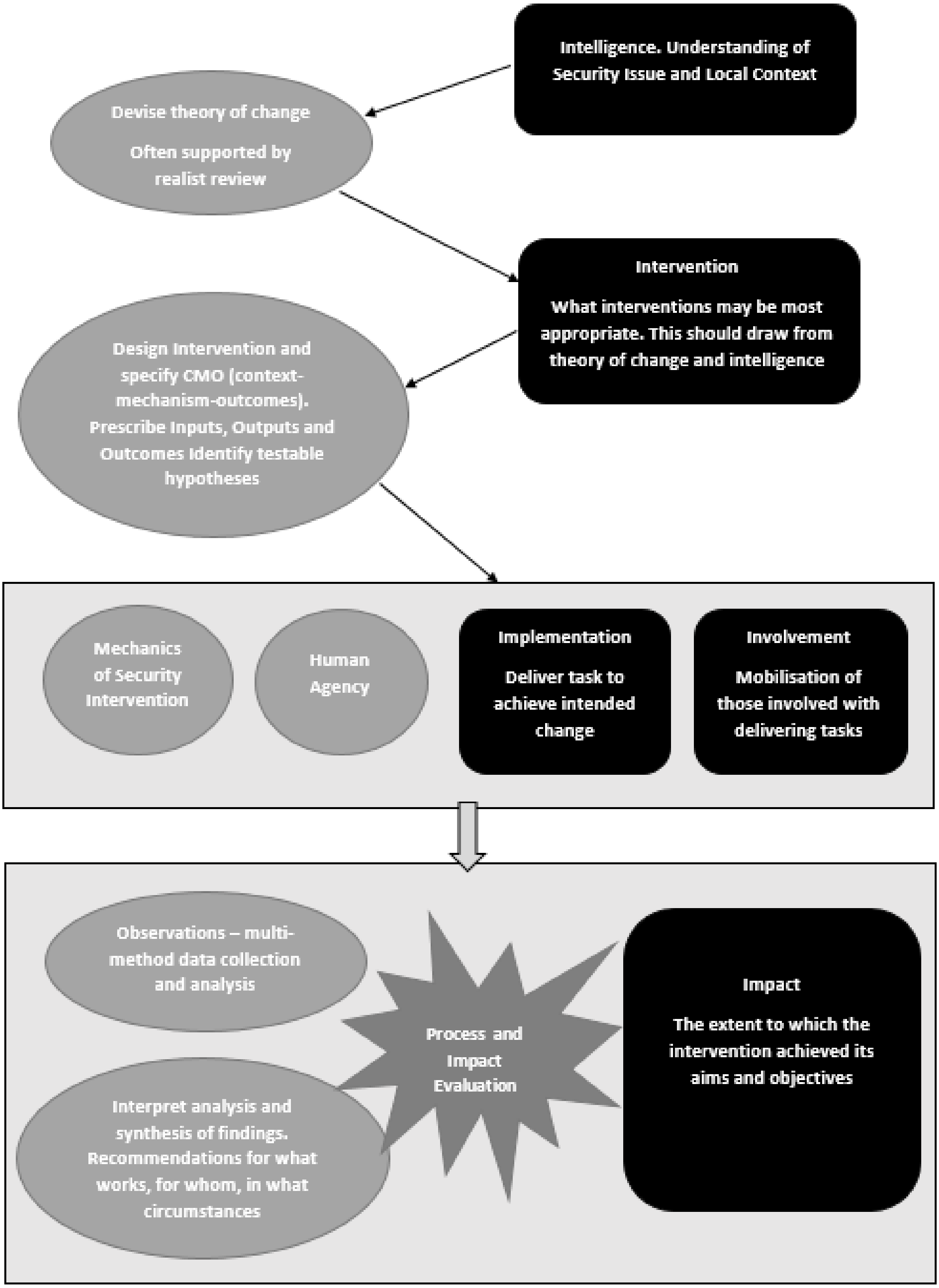


Figure Two: The duality between Realistic Evaluation and the 5Is



Intelligence. Understanding of Security Issue and Local Context

Devise theory of change

Often supported by realist review

Intervention

What interventions may be most appropriate. This should draw from theory of change and intelligence

Design Intervention and specify CMO (context-mechanism-outcomes). Prescribe Inputs, Outputs and Outcomes Identify testable hypotheses

Mechanics of Security Intervention

Human Agency

Implementation

Deliver task to achieve intended change

Involvement

Mobilisation of those involved with delivering tasks

Observations – multi-method data collection and analysis

Process and Impact Evaluation

Impact

The extent to which the intervention achieved its aims and objectives

Interpret analysis and synthesis of findings. Recommendations for what works, for whom, in what circumstances