Volume 3 Issue 2 December 2021

International Journal of Criminal Justice

KICJ Korean Institute of Criminology and Justice

INTERNAITONAL JOURNAL OF CRIMINAL JUSTICE

EDITOR IN CHIEF: Yoon, Jeongsook, Ph.D, Director, Crime Analysis and Survey Research Division, KICJ
ASSOCIATE EDITOR IN CHIEF: Yu, Jin, Ph.D, Deputy Director, International Cooperation Center, KICJ
MANAGING EDITOR: Kwon, Hyewon, M.A, Programme Officer, International Cooperation Center, KICJ

JOURNAL DESCRIPTION

The primary research areas of the journal are change of human behaviors, community response, and social system in the field of criminal law, criminology, criminal justice and psychology. We welcome research contributions that achieve: (a) improving knowledge and understanding of the etiology and trends of crime (b) utilizing theoretical frameworks and research methodologies in evaluation of criminal legislations and policies in different jurisdictions and (c) undertaking analysis and research on enacting and amending the criminal codes and legislations in response to changing or evolving crime trends with an eye towards improving the effectiveness of the judicial system and criminal policies.

International Journal of Criminal Justice

Contents

Invitation Article

The Modes of Mean(ing)s in Cybercrime Theorising, Analysing, Modelling and More

*M.R. McGuire.**
Senior Lecturer
Department of Sociology, Surrey Centre for Cyber Security
University of Surrey

Abstract

Developing a more rounded understanding of cybercrime is key to enhancing the ways in which we respond to it. This task has often been associated with the process of definition, though options here remain far from satisfactory. But defining cybercrime is one thing, attaching meaning to these definitions is another. In this paper I review some possible ways forward for adding greater depth and substance to what we mean we talk about cybercrime. I consider the role of data collection, theory and analysis in this context and question how helpful these have been in furthering our understanding of digital offending. I then evaluate what seems to be a third, promising option – the modelling of cybercrime activity, whether formally or informally. I suggest this provides a useful synthesis of theory, analysis and available evidence, as well as providing the basis for a more dynamic sense of cybercrime 'in action'. I conclude by setting out details of a recent research project where an economic model of cybercrime was developed. Some implications of this model for our understanding of cybercrime are outlined and reflections offered on the extent to which modelling might provide a useful way forward.

Keywords

Cybercrime, Definition, Meaning, Modelling, Cybercrime Economy

* Direct correspondence to Dr. Michael McGuire; m.mcguire@surrey.ac.uk
* http://dx.doi.org/10.36889/IJCJ.2021.006
* Received 7 December 2021; Revised 8 December 2021; Accepted 8 December 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 3-35

INTRODUCTION

We all know what we think we mean when we call an online crime a cybercrime. Or is it that we think we know what we mean? Or do we mean what it is we think we mean? Or is it somewhere in between? Confronted with these contrasting perceptions a tempting response has been to shrug one's shoulders and echo the words of the seminal K-Pop collective BTS, by saying, 'So what'? If some agree or some disagree with any particular interpretation of cybercrime why should this matter? For as BTS also argued, "if somebody call me right" and "somebody call me wrong" it may be best to just say "So what, let go".[1] Why, in other words should our interpretations of cybercrime have anything to do with framing responses to the problem? Shouldn't we just 'let go'?

To begin with it is obvious enough, as has been pointed out on several occasions (see McGuire 2019a), that there is nothing fixed about the act of calling a crime committed online a 'cybercrime'. It is not as if there haven't been plenty of other terminological options along the way. Why not 'online crime' for example? Or 'e-crime', 'computer crime' internet crime, 'techno-crime', 'digital crime' and so on? The fact that the term cybercrime is now sufficiently familiar and convenient for it to seem like a waste of energy in pursuing alternatives is not in itself a decisive reason to retain it. We may be "stuck with it" (Wall 2007, p.11) but force of habit does not constitute a final condition for assuming that it is any more meaningful (or serviceable) than the alternatives on offer. On the other hand – what's in a name and why would it be worth spending any more time in worrying about this? After all, surely it is the case that names have little bearing upon conceptualisations, or in establishing significance? There are perhaps two reasons why the terminological issue isn't entirely dead, even if it no longer seems very crucial. First is the conceptual baggage that comes with the term 'cybercrime'. That elusive prefix has often seemed like it 'adds something' extra to old fashioned crime – augmenting what has gone before with a frisson of the new or the mysterious. And we might (still) wonder whether this undermines effective understanding of it. Second, the term offers the tempting promise of universality - a rubric under which all the many and complex manifestations of human wrongdoing can be uniformly translated into the new space of the digital. The seeming ease with which the term has been imported across linguistic barriers so widely has reinforced this perception. For example, in Korea 'cyber' is saibeo

1) BTS-"So what" (2018)

(사이버), in Japan it is saiba, in Russia it is kiber (кибер), in Spanish ciber (netico), in Hindi saibar (साइबर) in Turkish siber and in Yoruba simply 'cyber' – and so on and so on.[2] Its presumed universality is even manifested within government circles where ministers often just say 'cyber' as their reference point to any kind of digital issue. But this seeming linguistic universality is at best a de facto one and may imply little more (as seems to be the case here) than a convenient replication of a familiar term.

Beyond the (ostensibly) minor issue of terminology lies the wider question of meaning. We may indeed think we know what we mean by the term 'cybercrime' but if its key criterion – the technology underpinning it – changes and mutates so quickly, can we be sure that our ideas are as stable as we imagine? For even if we could keep the technological element fixed across all its criminal manifestations this would still leave open the thorny question of how technology makes a crime a cybercrime, and what kind of level of causal dependency is at work here. I have dwelt at length on these questions elsewhere (McGuire 2007, 2019) but suffice to say here that they remain unanswered in any very satisfactory way.

At this point the question of redundancy raises its head. If its terminology is so questionable and its meaning so unsure, is a concept of cybercrime worth retaining at all? Why would we need it? After all, we know what crime is, irrespective of whether it is committed using a paper clip, a pocketknife or a PC. And isn't that enough? But whilst dispensing with the language of cybercrime has sometimes been an appealing option, it has never been seen through in any systematic way. The idea of cybercrime seems hard to relinquish, not just because this would seem to fly in face of popular wisdom but also because it ignores the facts on the ground. That crime using networked computers is happening seems indubitable. That it is significant, rising, causes harms to individual interests and may, on occasions, pose existential threats to society is hard to reject. And the fact that its modus operandi does seem to involve important variations on traditional criminal methods remains more than plausible. In what follows I will try to plot a way through this labyrinth of assumptions and find a way of accommodating them, whilst also suggesting a pragmatic way forward.

---

2) Two interesting exceptions here are Mandarin Chinese which has Wăngluò fànzuì (网络犯罪) and Arabic which has aljarimat al'iiliktrunia (الجريمة الإلكترونية - 'electric referred') as their transcription of e-crimes. Note however that both still invoke the technology as central. For example, wăngluò meaning "network (computing, telecommunications, transport etc)" and fanzui, crime (or committing one).

THREE RESPONSES

On the one hand then we have been landed with a seemingly indispensable criminological constant – one which has been regularly projected as amongst the greatest threats to the world today. At the same time, it appears to be something with conceptual foundations which lack clarity, depth or substance. Three ostensibly distinct ways of responding to this unsatisfactory state of affairs seem possible:

Sceptical Agnosticism: On this view, whilst the epistemic questions around the terms of meaning and reference of cybercrime may be interesting, they offer no real utility in dealing with cybercrime as an ongoing challenge. Thus, whilst there may be problems in how we think about digital/online/computer crime it is better to press on with gathering as much data as possible and not to worry too much about what this might all mean.

Cyber-Particularism: Conceptual/semantic questions about cybercrime may be problematic for developing a well-integrated approach towards it, but they do not prevent our understanding specific manifestations of online offending. The best response to any epistemic uncertainty is to therefore to keep a tight focus on *particular* cybercrimes, or elements of these – whether this involves the operation of online markets, online stalking or ticket fraud. By developing evidenced understanding of the particularities of online offending, the question of whether there are any useful connections or correlations between them can be postponed or ignored altogether.

Cyber-Universalism: In order to provide the most well-informed response to cybercrime, the epistemic challenges around meaning and conceptualisation are worth trying to overcome. This is best addressed by attempting to fix upon a universal conception of cybercrime. Such a framework is not just attainable but worth pursuing in its own right.

These responses need not be mutually exclusive or independent of each other. For example, one could easily be a cyber-particularist and maintain a focus upon more specific, empirically driven questions whilst retaining the belief that there is some

kind of unity behind the manifestations of online offending which are studied. Similarly, one could be a sceptical agnostic about the meaning of cybercrime or whether specific manifestations of online crime represent anything criminologically distinct whilst never ruling out that they might do. Finally, it is perfectly possible to hold, with the cyber-universalist, that there really is a clear and distinctive conceptual unity to the cybercrime construct whilst accepting that we can only ever find this in the particularities of its specific manifestations.

In other word, these three responses do not represent distinct decisions about the meaning of cybercrime, merely methods for managing best practice (whether as a researcher or a practitioner). What is clear though is that where there has been a decision to treat cybercrime as a real and unique evolution in crime and criminality the optimal response is going to conform with something like a cyber-universalist stance. This does not rule out a degree of agnosticism about what cybercrime actually entails, or that the best way to understand it is through the study of its specific manifestations. But, unlike the other responses, it *does* start with the assumption that cybercrime is something 'real' rather than ending with this. For this reason, it is this position I will assume in what follows, whilst also acknowledging the advantages of the greater caution represented by the first two positions.

Constructing a criterion for cybercrime

Cyber-universalism has tended to centre upon attempts to identify its most obvious and common characteristics. Since this has invariably involved the digital technologies upon which (it seems) to depend, providing a general definition of cybercrime has often resulted in formulations similar to what I will refer to as the 'C_{def}' Criterion:

$$C_{def} = \text{Cybercrime is (T-related) crime involving K}$$

Here T is the variable indicating the technological term to be inserted (digital; computer; network, or sometimes just technology); K refers to the *kind* of crime involved (i.e. stalking, fraud etc) and 'related' is a placeholder indicating whatever relation between T and the crime is considered to hold. This must clearly be some form of causal relation, though its level of determinism is variable and can be thought of in terms of necessary and sufficient conditions. Thus, at one end of the scale is causal *dependency* – indicating a necessary and sufficient relationship between the

crime and the technology whilst somewhere in the middle is causal *enablement* which indicates only a sufficient relationship (cf. Sloman et al 2009, McGuire and Dowling 2013, Salmon, 2020). That is, technology as non-necessary factor in the offending or, more simply still, that the crime could have been committed without it. Even weaker varieties of causal dependency involving the idea of a computer 'assisting' in the commission of a crime have also been invoked on occasions (Wall, 2014). Here computers are merely involved in some capacity (for example being used for a Google search), rather than as a tool central to the crime.

It is worth noting how the structure of C compares to formulations involving traditional crime. For example:

Rape is a crime involving sexual violence: R_{def} = (C, SV)
Fraud is a crime involving deception: F_{def} = (C, D)

The logical form of these criteria indicates a clear difference in that they involve a **two-place** predicate (C, *x*) whilst C_{def} requires a three-place predicate (Cdef = (C,T,K) to indicate that the relation between crime and victim is mediated. And what this suggests is that whilst standard conceptions or crime definitions are associated with a *direct* act of harm against another body or its interests, cybercrimes are not.

How necessary the technology place holder variable in definitions of cybercrime might be has been widely debated (cf. Wall 2007, McGuire 2018a). One reason for questioning this has been where T is substituted for N (referring to a network) as so:

$C2_{def}$ = Cybercrime is (N-related) crime involving X

Whilst it is true that contemporary networks are invariably seen as digital, this hasn't always been the case. Though traditional crime was a largely face to face business, it was also able to exploit certain network effects at times. Such networks might have been wholly socially centred - as in the explosion of new social connections made possible by 19th c urbanisation. Or they might have involved more constructed – though still physical – connections. As for example in the criminal exploitation of transport networks by the highwayman, the pirate and so on. I will return to considerations around connection shortly, but a more immediate question is whether *definitions* of cybercrime like the above also suffice to provide a *meaning* for cybercrime?

Constructing a meaning for cybercrime

The answer to this question appears to be no. A definition, though it can serve as a conceptual criterion, doesn't necessarily convey anything meaningful to us. That meaning and definition are not equivalent is easily shown in the way that a word like 'love' has no straightforward definition but carries a wealth of meanings. Conversely whilst it can be agreed that the following definition:

Copper = the name for the element with atomic number 29 represented by the symbol Cu

is true, it doesn't convey the many associations we attribute to copper (a shiny metal used in electrical wiring; a constituent of bronze; symbol for the 7th wedding anniversary – etc etc.). Thus, whilst definitions for cybercrime like C_{def} can be formulated, more is needed for them to say anything very substantive to us. Meaning used to be associated with reference – those objects or situations in the world to which a word refers. However, this was shown to be mistaken when it was realised that the *same* object can be referred to by words with *different* meanings (Frege, 1948). More generally, it is also clear that it is not possible to derive a semantics of cybercrime from purely syntactic considerations about definitions of terms or the rules governing their application (See McGuire, 2018a for an evaluation of the syntax/semantics distinction in relation to cybercrime). One suggestion for adding substance has been to acknowledge the role of context dependence and the contributions of both the social and the external world in determining meaning (Putnam, 1973). This certainly makes sense for our interpretations of cybercrime where contextual factors such as the techniques used by cybercriminal or the harms done by perpetrators against victims seem as essential to determining its meaning as any abstract definition.

A preliminary observation is that meaning constructions within cybercrime are consistent with at least two of the stances identified above. For example, cybercrime-particularists will look more towards the specific circumstances of what they have uncovered so that the meaning of cybercrime (for them) will tend to reside in their datasets and the observations made on this basis. By contrast, cybercrime-universalists will try to associate such observations within the more general pattern of cybercrime which they perceive. Not only does this emphasize that there is, as yet no general agreement about what is needed to make definitions of

cybercrime properly meaningful and that something additional is needed to plug into them. It also suggests that, as with the study of other social phenomena, other epistemic processes – most obviously *theory construction* are required for the pursuit of meaning. I will therefore begin here, before moving to the related process of *analysis* and finally my own suggestion for securing meaning – the process of modelling where both theory, data and analysis come together in fruitful ways.

Theory: Though the most obvious starting point for providing a meaning for cybercrime is to accommodate it within a theoretical framework of some kind, such frameworks have been far less developed than one might imagine. The application of *criminological* theories to cyber-criminality has been the most frequent strategy of this kind though, as suggested below, their use has sometimes been a little uneven. Far less common has been the development of new theory, tailored towards the novelty of cybercrime. This may be because it is still early days – cybercrime remains a relatively new phenomenon in the history of crime. Or it might just be that attention has been more preoccupied with empirical than with theoretical concerns.

Of the available theoretical positions which have seemed applicable to digital crime phenomena it is perhaps the routine activities approach (Cohen and Felson, 1979) which has found the widest favour. As far back as 2001 Peter Grabosky suggested this as one of the more promising theoretical directions (Grabosky, 2001) and there have been attempts to apply it to a range of cyber-offending contexts ever since (cf Reyns, 2017). For example, website defacement (Howell et al 2019); insider cybercrime victimisation (Williams et al 2018); spam distribution (Perkins et al. 2020) cyberstalking (Reyns et al., 2011); identity theft (Williams 2016); malware (Kigerl, 2021) and even cyberterrorism (Holt et al 2021). The appeal of routine activities as a way of providing meaning to cybercrime parallels its attractions in the context of traditional crime. By framing criminal acts in terms of their intersections between three key variables, the (suitable) target, an offender who is motivated in some way and the gaps provided by an absence of any effective guardian, a seemingly straightforward and flexible way is offered for understanding (and responding to) them. In turn, these 3 factors appear to translate across unproblematically into cybercrime contexts. For example, a motivated offender might be an advance fee phishing fraudster, a target the victims banking details and the failure to provide effective account security by the bank an absence of guardianship.

On the other hand, it is not clear that these often mechanical applications of a routine activities framework tell us very much about cybercrime that we don't already know. After all, it is trivially true that any crime involves a criminal or criminals. And irrespective of whether it is a digital or a terrestrial crime there is usually some kind of target or reward they are after - an objective made far easier where the means to stop them are lacking. Routine activities-based approaches have also been criticised for conflating the kinds of space available to criminals operating in physical contexts with those in digital contexts (Yar, 2005). The spatio-temporal compression (Harvey, 1990) which typifies online interaction means that time is not fixed (offending can be asynchronous) and the space between offender and target is usually not equivalent to what is feasible within traditional crime. In fact it is precisely these spatio-temporal differences that have led some to seek reasons for identifying meanings of cybercrime that transcend the resources of traditional criminological theory (see below).

Another theoretical approach which has often been invoked in trying to make sense of cybercrime is Social Control theory – the idea that offending results from low self-control (Hirschi, 1969, Gottfredson and Hirschi 1990). Poor self-control arises where there are few stakes in conformity, for example a lack of social attachments, limited ambitions/interests and minimal levels of belief in social institutions. Low self-control has been used to explain issues such as digital piracy (Moon et al 2010); cyber-victimisation (Nodeland, 2020) and hacking (Back et al 2018). There have also been attempts to show how control theory might apply beyond such frameworks (Donner et al 2014). Like routine activities-based approaches, there have been frequent claims of empirical corroboration for control theory when applied to cybercrime, though this has not always been borne out by studies which sometimes appear inconsistent with each other. For example Bossler and Holt (2010) took their use of the Grasmick et al. (1993) scale — (which measures low cognitive forms of self-control) — to suggest that low self-control could be associated with unauthorized password access and file tampering, But this conclusion was challenged by other researchers (Ngo and Paternoster, 2011) who found that low self-control had **no** significant effects on phishing or virus infection victimization when they used the same cognitive measure (see Louderback and Antonaccio 2021). It is also worth bearing in mind that if it were possible to show that control theory is able to cross the digital divide then this divide would cease to matter. Since Gottfredson and Hirschi's claim is that their theory provides a general approach to (all) crime, any search for the

meaning of cybercrime then becomes redundant, since there would be nothing ultimately very distinct about it.

Elsewhere, social learning approaches have also found some applications in the cybercrime context (cf Bowman & Freng, 2017), though examples are not extensive. Early studies looked especially at the way socialisation at college level sometimes persuaded young people to engage in cybercrime (Skinner & Fream 1997). And this theme has persisted, for example in the explanation of software piracy. Here the sharing of technical skills amongst young people and their gradual familiarisation with hacking communities was used to make sense of the spread of piracy and the perception that it is 'not real crime'. (Burruss et al., 2012). More widely, the use of social learning approaches to *predict* digital offending has also been proposed (Dearden and Pati, 2021).

Other applications of criminological frameworks to cybercrime have included Mertonian strain theory (Chism & Steinmetz, 2017); labelling theory (Turgeman-Goldschmidt, 2008, Payne et al 2019) and subcultural theory. The latter has found particular (though predictable) applications to hacking subcultures (Steinmetz, 2015, Collier et al 2021) and online forums (Bada et al 2021). However, surprisingly unexplored has the been the relations between subcultural formations and the impacts of online 'filter bubbles' – especially those implicated in the dissemination of crimes involving online hate or disinformation. Still less common have been the application of tested frameworks like white collar crime or youth gang crime to explain cyber offending characteristics (cf. Payne, 2018, Sela-Shayovitz 2012), and far more research is needed in such areas if more nuanced meanings of cyber criminality are to be drawn out.

By contrast more novel theoretical approaches to cybercrime have been few and far between. One more developed example is (so-called) space transition theory which suggests differences in behaviour where people move from physical to cyberspace – in particular the way that criminal tendencies which might be repressed within the physical domain are able to find expression within this extended digital medium (Jaishankar, 2008 Schmalleger & Pittaro, 2009). However, it is not clear whether this offers any more insights into cybercrime than what was identified with Suler's famous 'online disinhibition effect' (2004). Nor is it obvious whether the internet is always used for crime in the way the theory suggests (c.f Holt and Bossler p. 93) More radical uses of spatial concepts can be seen in the suggestion that what cybercrime 'is' - and

therefore what it ultimately means - is precisely to do with reorientations of spatial experience and the nature of social interaction that come with digital networks. The suggestion is that with these comes a wholly new kind of space - a 'hyperspace' - one that reflects the hyperconnected nature of contemporary life (McGuire 2007) and which produces *hypercrime* rather than cybercrime. However, these more radical interpretations of what cybercrime might mean have not yet been taken up very widely.

Whilst the examples cited here are certainly not only the theoretical frameworks which have been applied to cybercrime, they offer a fair representative selection of what has been tried. But a recurring problem in finding meanings for cybercrime in this way has been the rather fragmented applications of theory and the minimal agreement between scholars over which approach might be the most efficacious. And whilst theory is a useful tool, it can often seem a little remote from the facts on the ground. Perhaps more crucially, few of the theoretical frameworks which have been applied have had very much to say about the *technological* aspects of cybercrime. Aside from a few isolated examples, such as attempts to utilise actor network theory (Brown 2006, Van der Wagen & Pieters, 2015), serious engagement with what it is about digital technology which makes crime 'cybercrime' remains limited. Thus, in applying criminological theory it is unclear whether we understand the meaning of *cybercrime* any better or whether the outcome is, in the end, more about developing a better understanding of criminological theory.

Analysis – Another common way of providing a meaning for what we encounter in the social world is to break it down into component parts. This is the process of analysis, a process often contrasted with *synthesis* (where component parts are assembled into a kind of whole). Most physical science is analytic in this sense – physics finds meaning and understanding in the world by breaking down natural phenomena into elements and the forces acting upon them. Social science often aspires to the same thing but of course runs into the problem that its analytic components – human subjects – are not inert. Rather, they constitute a pre-existing intersubjectivity where meaning is indexical to individuals and therefore very hard to break down further into elements suitable for analysis. Within the cybercrime context, analysis has tended to take two forms – simple and complex. Its first, more simple application has usually involved straightforward *descriptive* analysis centred upon

quantities such as fraud prevalence, rises in DDos attacks and so on. More complex forms of analysis have included:

Mapping & logging analysis. Such approaches examine phenomena in the online crime world by gathering data about it and then attempting to break this down into indicative patterns and interrelationships. Since there is usually also a strong descriptive component to this approach - with an emphasis upon counting, accessing reliable datasets is essential. Some analyses of this kind have focussed upon causal correlations – for example the relationship between police interventions and the operations of dark markets (Décary-Hétu & Giommoni 2017); the effect of web takedowns on phishing (Moore and Clayton, 2007) or the impacts of education on cybercrime prevention (Bele et al 2014). Other studies have concentrated upon identifying and enumerating specific patterns of criminal activity such as the sale of drugs on social media (Moyle et al 2019); online image based abuse (Henry & Flynn, 2019); internet money laundering forums (Mikhaylov. and Frank, 2016) or the sale of personal information (Holt et al 2016). However, though such exercises are clearly valuable in establishing certain baseline indicators, it less obvious whether their greater focus upon finding the trees rather than the wood informs the meanings we draw from cybercrime very substantively.

Crime scripting analysis. Crime scripting involves a form of analysis which aims to break down crime events into their key stages to produce a kind of step by step 'script' of successful offending. The approach derives much from earlier precedents within the social sciences (see for example Abelson, 1976, Schank and Abelson, 1977) and was adapted for criminological analysis by Cornish (1994). It has been widely applied throughout the field since then (Dehghanniri & Borrion, 2019). Crime scripting has obvious appeal as a method for cybercrime analysis, with (at least) 24 scripting exercises recorded up to 2018 (Dehghanniri & Borrion ibid). For example, online data markets (Hutchings & Holt 2015) and internet trolling (Somer et al 2018). More recent applications have included online sex offending (van der Bruggan & Blokland 2020); online fraud (Junger et al 2020); SQL injection attacks (Leppänen, et al 2020) and sexual abuse via images (O'Hara et al 2020) amongst others. One problem is the degree of subjectivity in how the elements within a script (cast, props etc) are selected since this may compromise generalisation. And whilst crime scripting

contributes structure to our sense of 'what is happening' in specific cybercrime situations it is less clear that it provides the more nuanced interpretations or can demonstrate the wider significance of cybercrime events in terms preferred by a cyber-universalist.

Situational crime analysis Rather than focussing upon offenders or their motivations, situational crime approaches have concentrated more upon the background environment and how this might be doctored to reduce its appeal for criminal exploitation. Though this form of analysis has an overtly preventative rationale, its capacity to evaluate the cybercrime environment might also provide some resources for interpreting it. As with its applications to crime in general (see Clarke 1995), analysing cybercrime in situational terms essentially follows the routine activities approach by breaking crime events down into three key parameters – risk, opportunity and reward. For cyber criminality, environmental risks could include the strength of prevention processes like network security, where inadequacies then bring opportunities. For example, weak phishing controls or unpatched systems. Rewards might be purely financial – such as access to customer accounts, but could just as easily include, data, CEO emails, intellectual property and so on. Examples of situational crime analysis in the cybercrime context have included its application to online child pornography (Me & Spagnoletti 2005), information security (Hinduja & Kooi, 2013); the use of money mules (Kleemans & Leukfeldt, 2019); insider cybercrime (Willison & Siponen, 2009, Stockman, 2014), online piracy (Basamanowicz and Bouchard, 2011); cybercrime prevention (Brewer et al 2019) and cybersecurity in higher education (Back & LaPrade, 2020). Given its (relatively) long history a number of critiques have been raised against SCP-based analysis, any of which could also stand where it is applied in cybercrime contexts (cf. Wortley 2010). In particular, such analyses have often been charged with failing to consider displacement effects. Thus, an evaluation of a prevention measure as successful against cyber-attacks may overlook the fact that the hack or intrusion is then transferred or attempted elsewhere. There is also the problem that, since SCP analyses are more concerned with the circumstances of cybercrimes and how they unfold than with the offenders behind them, they are unable to detail the motivations behind any attack. This has some obvious drawbacks in the cybercrime context where one attack can often look very much like another from the outside. But suppose we have one

DDos attack mounted by a teenager seeking to demonstrate their skills, another by a cybercrime gang in search of 'Fullz' datasets and another still by a Nation state which aims to disrupt business activity. Being able to distinguish the intentions behind these Ddos attacks would seem to be an important factor in understanding them. Finding out who did it and why is likely to be just as valuable in determining meaning as identifying perimeter vulnerabilities. Certainly, it seems unlikely that providing for meanings for cybercrime can be wholly separated from acquiring a sense of the protagonists and their aims.

Social network analysis. Given that cybercrime can very plausibly be thought of *as* networked crime, (no network, no cybercrime), applying social network analyses appears to be a promising option. A wealth of potential insights and meanings seem likely to be drawn here by finding typical network structures or patterns within cybercrime activity. For example, better understanding of the ways in which illicit money is filtered through payment mechanism chains; clarifying who particular kingpins might be; finding distribution hubs and so on. Though SNA has not perhaps been applied as widely to cybercrime as might be expected, certain examples have pointed towards its potential going forward. Amongst these have been analyses illustrating the form and operation of hacker communities (Lu et al 2010); illicit activities on social media (Geetha et al, 2020); cyber-attacks on enterprise (Sarkar et al, 2019); cybercrime groups in China (Yip 2011); organised cybercrime (Leukfeldt 2015) and underground forums (Pastrana et al 2018) amongst others. However, an obvious concern with SNA based approaches is that whilst they are good on structure, they tell us far less about the *substance* of cyber-offending and this, as suggested above, seems to be an indispensable component of finding meaning in it. There is also a problem with potential triviality, in that almost any collection of elements can be interrelated to form a network Thus it is not always clear that SNA tells us anything particularly novel or surprising in more general terms about cyber criminality.

This catalogue of analytic approaches is by no means exhaustive. For example, there are also analytic tools available within other fields, most obviously psychology which look promising. Given the need to understand why cybercriminals think and act in the way that they do, psychological analyses of hackers (McAlaney et al 2019), of cybercrime victims (Van de Weijer & Leukfeldt, 2017), or the rationales of cybersecurity (Taylor-Jackson et al 2019) all seem likely to add to our understanding.

In isolation however analysis alone seems unlikely to deliver everything we need to develop effective interpretations of cybercrime. Taking something apart doesn't necessarily tell us how it works and certainly not what it signifies in wider social contexts. Combining analysis with theory might be a way of bridging this gap, though how remains uncertain. Overall, when evaluating the rather fragmented way in which both theory and analysis have been applied to cybercrime it is hard to resist the conclusion that these have been more like 'suck it and see' style exercises, than consistent or properly integrated programmes of study. For this reason, it may be that the third, modelling-based approach I will now consider, offers a more promising option for determining meaning in the longer term.

Modelling Cybercrime – an economic approach

Modelling aims to provide explanation in terms of models or simulations which create dynamical representations of clusters of activities at greater or lesser levels of detail and sophistication. I suggest it represents a more robust potential combination of theory and analysis in that the link between abstract (theoretical) frameworks and the way these are 'filled in' with data is far more transparent. Modelling in the social sciences have tended to pursue largely mathematical approaches, though there has been a shift towards agent based & game theoretic approaches more recently (Mershon & Shvetsova 2019). This has yet to find many applications within the cybercrime field, with some notable exceptions. For example, Onuchowska & Bernt (2019) utilised an agent-based approach to model malicious behaviour on social media whilst Basuchoudhary & Searle (2019) used a game theoretic model to highlight business responses to trade secret theft. Overall however, it has been within the cybersecurity field where we tend to see more of these kinds of models (see for example Rajivan et al 2013, Thompson & Morris-King, 2018 & Ashiku & Dagli, 2020).

More typically, modelling within cybercrime research has taken an informal 'heuristic' style approach. For example, Porcedda & Wall (2021) used an informal modelling approach to show how cyber-enabled data-crime influences cyber-enabled offending, whilst the use of non-mathematical modelling has also been seen in attempts to outline itemize the key features of a cybercrime 'ecosystem (cf. Broadhead 2018, Dupont 2019). Though these more informal approaches do not yet outline any consistent methodological approach, certain advantages can result where they are

conducted effectively. One benefit is to provide succinct yet dynamic snapshots of cybercrime 'in action', a useful counter to its often very static representations within many research approaches. Another is to provide a way of accommodating the various stances outlined earlier. For example, the fact that models can be applied directly to cybercrime scenarios without the need for a prior theoretical framework means that it is consistent with cyber-particularism. At the same time a cyber-universalist position can be supported by basing models upon theory and then testing to see how far data supports or refutes this.

To indicate some of the potential advantages of this approach to cybercrime and to conclude this discussion I will set out the contours of an informal modelling exercise conducted between 2018-21 (McGuire 2018b, 2019b, 2019c & 2021). This project had the initial aim of extracting some sense of how cybercriminals might spend their ill-gotten gains, but as it became apparent that other considerations needed to be built in to even pose this question it was soon obvious that something close to a model was under development – albeit one with uncertain boundaries and driven by a certain amount of educated guesswork. A first complication was that no estimate of the spending of cybercriminals could be made without knowing how *much* they have to spend. This in turn led straight to offending itself and the motivational backgrounds to this. Whilst motivations for cyber criminality may vary from revenge to sexual fulfilment, financial reward was the obvious motivation to explore in the context of understanding spending. When operationalised in terms of the pursuit of revenues, metrics could be derived from the key *methods* of generating revenues by cybercriminals which emerged. The research found a surprisingly wide range of activities here, from the more obvious varieties like fraud, through to more novel techniques such as selling advertising space on crimeware sites.

With agents directed towards various methods of revenue generation in place, other components of the model then began to emerge. For example, there are the targets and victims of such revenue generating schemes and in tandem with this the *quantity* of revenues cybercriminals are able to generate. Overlaid upon these variables were at least two further factors, both related to *where* these revenues go. Revenues may initially need to be moved around or concealed – so providing some sense of the connections between cybercrime activity and the wider field of (digital) money-laundering (Berghel, 2014. Albrecht et al. 2019). Finally, the ultimate point of disposal of the revenues need to be built in. This was found to take various forms,

from straightforward conversions into desirable commodities to more considered forms of disposal such as investment, or even their use in supporting further crime. Further complexity was added to the model by considering the kinds of *currencies* used to mediate the flow of revenue generation and transactions, with digital and crypto-currency the obvious tools driving these cycles. Some consideration was also paid to factors like production centres (where certain types of revenue generate activities are geographically focussed) and the size and type of criminal organisation involved in revenue generation.

One recognised advantage of models, especially in agent-based forms is that they are able to capture *emergent*, unexpected phenomena (cf. Bonabeau, 2002) – something not so easily accommodated within analytic or theoretical approaches. And what soon emerged from the model here was something close to an *economy* – a dynamic map of interactions amongst cybercrime (and other) actors based upon production, consumption and wealth generation. It also became apparent that this model of illicit digital relations conformed closely with economic patterns seen elsewhere within contemporary digital societies. For example, as traditional economic models based upon straightforward supply, demand and resource allocation have had to adapt to a more dynamic globalised world it is striking how the *movements* of wealth and the symbolic extensions of these (into data and so on) are now almost as important as the production of wealth itself. Thus, in the hyperconnected social world we inhabit the "power of *flows* takes precedence over the flows of *power*" (Castells, 1996, p. 469). Modelling cybercrime in terms of the very simple range of variables outlined above not only helped make this feature and its role as a wealth generator more obvious, but it was also able to illustrate the extent to which cybercriminality now feeds off the legitimate economy.

Understanding the meaning of crime through the lens of economics is not, in itself new of course. Becker's work in identifying seemingly useful correlations between the severity of punishment and a (rational) criminals' evaluation of how this compares to the benefits of violating the law represented an early foray into this kind of thinking (see Garoupa, 2014). Other applications of economic thinking have included attempts to apply theories of the firm and the dynamics of markets as a tool for understanding drug markets (Rottenberg, 1968; Moore, 1970; Fugii, 1975), or organized crime activity (Schelling. 1967; Rubin, 1973). Further studies have looked at the way economic theory in general might be useful in limited contexts (see for

example Orsagh, 1983). In a slightly different vein the Market Reduction Approach (MRA) (Sutton 1998, Sutton et al 2001) drew upon economic concepts around the market and market behaviours to develop a form of crime prevention based upon disrupting stolen goods markets.

Within cybercrime research itself economic thinking has most often tended to manifest itself within the 'cybercrime as a business' trope (Manky, 2013 NCSC 2017, Parise, 2019). However, the problem with this line is that it has tended to be more of an exercise in description than elucidation. We don't learn much, other than the fact that cybercrime activity sometimes resembles business activity by- for example – selling certain (illicit) commodities or being profit oriented. Worse, by simply seeing it as crime with economic *components* rather than as an integrated set of economic relations, a rather static portrait results. By contrast, modelling it more dynamically - as an integrated economy- more substantive insights related to the flows manifested within this economy and their interdependence become clearer. For example, by breaking down revenue generation into just 5 of the better evidenced modalities it was possible to build up a more connected sense of the key relationships in the flows connecting criminal profits, their destinations and what happens in between. In turn, this enabled some new insights into the modus operandi of cybercriminals and where cybercrime as a whole might be going.

Initial evaluation suggested that between 2018-19, activities in these five revenue categories were generating approximately:

Illicit/illegal online markets: $860bn per annum
Trade Secret/IP theft: $500bn per annum
Data Trading: $160bn per annum
Crimeware/CaaS: $1.6bn per annum
Ransomware: $1bn per annum

When totalled, these five categories implied that around $1.5 trillion in revenues is now available to cybercriminals annually.[3] And this, to be clear, was a fairly conservative estimate. Many other kinds of revenue generating activities were not considered and even within the five chosen categories estimates were always targeted

3) For details of how these and other estimates were arrived at, see McGuire (2018b, 2019b, 2019c, 2021)

towards the lower, rather than the higher revenue range. An obvious preliminary conclusion was that the size of the cybercrime economy is now very significant. Not only is it worth more than the total profits of the top 3 Fortune 500 companies, it also often matches or exceeds the GDP of many nation states (the annual GDP of Saudi Arabia is around $.75 as a comparison). Of course, some caution is necessary in interpreting agency here. There is no directed or collective synergy in the acquisition and disposal of these revenues, as there would be with an orthodox economic actor like a state or a company. Cybercrime actors tend not to share or jointly invest their profits. But the figures, no matter how undirected or provisional, provided several useful insights.

First, by indicating how much money is available to the cybercrime economy a firmer sense of the potential criminological significance of cybercrime was attained. Second by better understanding the relationships between cybercriminal activities and their revenues a more topographical, 3D picture emerged indicating where activity is most pronounced and what the key pulls of attraction for cybercriminals might be. And what was immediately striking here was that it was not so much the 'obvious' forms of cybercrime activity – such as ransomware attacks[4] - where the real money is being made, but in the more mundane activities associated with trading. Thus, the $860 bn in revenues being generated by illicit online sales clearly outstrips all others by a considerable amount. As a result, it might well be asked whether the sensible cybercriminal would be better off selling prescription drugs than trying to hack into a bank. The full implications of this imbalance are too complex to consider here[5] but there are clearly important questions about the focus of cybercrime activity to unravel as a result.

Third, by identifying this reservoir of illicit profits we can begin to draw

---

4) In 2020 it is estimated that known ransomware profits (i.e. those which got paid) came to around $370 million (Cimpanu, 2021). Though this represents an increase of over 300% increase over known 2019 earnings, it was below the estimated amount detailed in the Web of Profit research, probably because that also allowed for unreported payments. And it was still some way below the other revenue totals. Thus, whilst ransomware can be highly disruptive it is not necessarily the most profitable cybercrime activity. Nor any longer is it one of the safer ones. As ransomware attacks (especially the larger ones) have started to attract increasing attention from law enforcement and other agencies intervention and enforcement has begun to increase. See for example the recent arrest of members of the REvil ransomware group (DoJ 2021).

5) Though see my forthcoming (McGuire 2022) for some interpretations of what this might mean for cybercrime in the medium to long term.

inferences about where these are ending up and what that might imply. In particular, given these funds are illicitly generated, it is clear that a sizeable chunk of them will end up swilling around in the estimated 2 - 5% of global GDP currently circulating illegally around the world (around $800 billion - $2 trillion (UNODC 2011)). In this way, not only did the model help throw some additional light upon the murky world of money laundering, but insights into the contribution of digital deviance to this, most obviously in the use of bitcoin or other crypto currencies. Around $2.8 bn was estimated to have been laundered through cryptocurrency exchanges in 2019 (Chainanalysis 2020), so any additional steer on this is likely to prove beneficial in enhancing our understanding of the interweaving between the licit and illicit economies. Indeed, it raises many questions about how closely connected legitimate and criminal business activity now is – a point I will return to below. Finally, the modelling exercise also helped refine some of the questions about the modes of meaning around cybercrime which this paper is considering. For example, there have often been questions as to whether selling counterfeit or other goods through illicit markets should really be counted as 'cybercrime' in the truest sense. Yet if this contributes to the cybercrime economy in the way the model suggested, why wouldn't it?

Another way in which a modelling exercise like this can enhance our sense of what cybercrime might mean is by way of its flexibilities. Given the economic angle to the model, obvious sites for further analysis present themselves - not least other online contexts where trading activity can be discerned. One immediately interesting suggestion here was the challenge to assumptions that it is on the darknet where most economic cybercrime activity is conducted. Whilst there is clearly a substantial space for revenue generation provided by these 'hidden' markets, the so-called ''clear/open net" turned out have a far greater role in supporting the cybercrime economy. This was especially the case with social media platforms which appeared to be flourishing sites forcybercrime activity. Thus, it emerged that criminal revenues from fraud enabled by social media had increased by over 60% between 2017-2019 and certain activities - drug dealing most obviously - were being conducted within plain sight. One recent survey has suggested that 72% of young people have reported seeing illegal drugs advertised for sale on social media sites or apps every month (McCulloch & Furlong, 2019) and our research found that drugs were available for sale across a significant number of the platforms that were studied. And here too, received wisdom is not always reliable when such activity is modelled in more detail. For the research

again showed that it is in less spectacular activities where some of the real gains may lie. Thus, around $1.9bn was being generated through illegal pharmaceutical sales (i.e. prescription drugs) on social media – far in excess of the $290m or being made from the financial frauds enabled there. Nonetheless the fact that such frauds were being so openly conducted represents an obvious threat to social media users, as does the role of such platforms in generating around $138m from romance/dating fraud. Other categories of cybercrime revenue generation on social media were less predictable – for example around $250m being made from the distribution of Crypto mining malware. Also surprising was just how much common or garden cybercrime activity was going on, with 30-40% of the social media platforms inspected for the report having accounts offering some form of hacking service. The use of digital media for more traditional crime was also evident. For example, young people's readiness to use social media to communicate via provides an obvious angle for exploitation, so the 36% rise in the use of social media platforms between 2017-2018 to recruit money mules under the age of 21 was no surprise.

The value of an economically oriented model was also evident when extended to the more obvious site for cybercrime activity - the darknet. Credible estimations of revenues here have proved all but impossible to obtain given the numbers of active vendors and their reluctance to say very much about their operations. This means it is very hard to be sure how many transactions are successfully completed, let alone their total volume or value. However, since bitcoin or cryptocurrencies now represent an almost universal currency in dark market commerce, examining these transactions provides another method for obtaining a firmer grasp on how the darknet fits within the cybercrime economy as a whole. One study has suggested that the value of darknet trading had reached something like $1bn by 2019 (Chainanalysis, 2020). Whilst this doesn't tell us *what* is being traded, or what level of profit this represents, it does give us some insight into the revenues available through the darknet site for cyber criminality. And this in turn supports the conclusion alluded to above – the fact that it still lags behind revenues available from the clear net. Our analysis of the type of listings to be found suggested that around 25% of the total content involved items such as counterfeit goods - indicating again that it is old fashioned trading, rather than spectacular hacks which represent the bread-and-butter activities for cybercriminals. And this trade, fairly predictably, involves more familiar commodities rather than those which are overtly cybercrime related. Of the 70,000+ listings examined in the

research, 47% were related to drug or drug-related sales, while just under half (43%) were related to digital products like compromised bank accounts, malware, DDoS tools, or stolen card credentials. Six percent represented 'services' like hacking tutorials.

Also revealing was the fact that individual victims appeared to emerge as less of a target than enterprise and other social institutions within this trading environment. For example, where listings from drugs were excluded, we found that 60% of the digital products and services traded on the dark net represented direct opportunities to harm the enterprise. 15% of content could be associated with more indirect forms of harm to the enterprise (e.g. reputational damage). And of the vendors who were directly questioned at least 60% said they could offer access to more than 10 business networks; 30% offered access to between 5-10 and 10% were offering access to up to 5 networks. As might be expected - malware and DDoS/botnet tools represented the most frequent types of threat from the dark net in relation to network compromises; constituting an average of around 45% of listings examined (25% for malware and 20% for DDoS).

But perhaps the most telling indicator of the growing influence of the cybercrime economy is the way that nation states have become implicated within it. Whilst the threats posed by nation state attacks are now familiar enough, the role of the cybercrime economy in supporting and enabling their actions has been far less discussed. An analysis of nation state attacks between 2019-2021 was conducted suggesting that around 50% of them involved low budget, straightforward tools easily purchased on dark net, or other cybercrime markets. Around 20% involved more sophisticated custom-made weapons such as targeted malware or weaponised exploits, probably developed within dedicated state cybersecurity programmes. Crucially, many of these tools have themselves now been acquired and traded across darknet sites. For example, Eternal Blue - just one of the tools acquired from the US national security agency in the notorious 'Shadow brokers' hack has now helped compromise over 5 million computers worldwide; caused several billion dollars of losses to businesses and governments globally and generated in excess of $500 million in revenues for cybercriminals (Cf. Perloth & Shane, 2019) More recently, data stolen from multiple US government agencies during the SolarWinds hack has been reputedly advertised for sale on the dark net for over $1 million.

The interweaving of the cybercrime economy with the ongoing struggles in

cyberspace could be interpreted even more radically. Given the apparent dependence upon cybercrime activity on the part of some nation states (it could be argued that something like ‘cyberwar economies’ have emerged with nations profiting openly from the tools, services and revenues these illicit activities are now producing. One relatively well evidenced example here has been the case of North Korea (DPRK). Most experts believe that it has been able to combine methods of generating revenues from cybercrime with digital innovation. One approach has been bank robbery - albeit in contemporary forms like cryptocurrency theft coupled withransomware operations andmoney laundering. For example, a well evidenced set of cyberattacks on cryptocurrency exchanges in 2017 generated revenues equivalent to $571 million for the North Korean Lazarus APT group in that year alone. The group used phishing and other techniques to access the exchange, providing a useful way of supplementing the North Korean government’s limited access to foreign currency. Similarly, North Korean groups, probably government sponsored, were involved in a 2016 attack using SWIFT credentials from Bangladeshi Central Bank employees to engineer an $81 million transfer – one of a series of attempted heists from banks in South East Asia by the group. In 2018, the group switched their attention to ATM hacks, successfully engineering them into paying out millions of dollars on command using a specially adapted Trojan. A 2021 report by the UN has suggested that over $300 million generated by the DPRK in 2020 through cybertheft was used to fund its nuclear and ballistic missile programmes (Roth and Berlinger, 2021).

However, the benefits of the cybercrime economy are not restricted to smaller nations. For example, our analysis suggested that cybercrime related activities sponsored by China may now generate an equivalent of 10% of the value of its exports. Indeed, the increase in revenues for the Chinese economy is equivalent to total income from high profile exports like textiles (worth c$239bn to the Chinese economy in 2017). Similarly, the Russian economy now benefits from an additional $600m+ annually (at minimum) from carding operations alone, with cybercrime activities generating revenues around three times the value of arms/weapons exports for the Russian economy. And even where the economic activities are ostensibly legal, cybercrime is fuelling nation state GDP in significant ways. For example, Israel’s cyberwar economy benefitted by around $1.19 billion in 2017, with over 20% of global investment in cybersecurity being directed there.

Conclusions: Meanings in the modes of Cybercrime?

If the meaning of cybercrime amounts to nothing more than formulating a definition for cybercrime then, as this paper has suggested, not much can be concluded. Definition is not equivalent to meaning, so the standard way of characterising cybercrime as 'internet/digital/technology/etc crime', even if this were satisfactory (which I have argued it is not), doesn't begin to explain the depth and breadth of what (we think) it signifies. Gathering data, developing theoretical frameworks, or applying different forms of analysis seem like obvious ways of trying to bridge this gap between definition and meaning but each appears to be wanting in some way. In particular, simplistic exercises in applying established criminological theory or drawing upon recognised analytic tools has often seemed to be more about stamp collecting than providing genuine understanding. And the risk of intellectual noise arising from far too many attempts to apply far too many tools to find meaning is a real one confronting researchers.

If then cybercrime really is as novel or poses as much of a threat as is often held, the current situation represents a failure of the criminological imagination of the highest order. Too often the catastrophising of cybercrime has pushed researchers more towards finding 'interventions', 'disruptions' or 'solutions' than advancing explanation or finding meaning. But criminological understanding surely ought to be about more than providing a service industry for law enforcement or policy makers. At present, the best ways forward seem to be to attempt to carve out some form of synthesis between these options, perhaps in the form of models of greater or lesser rigour though even here reaching an optimal balance between the evidence and what we can say about this evidence remains uncertain.

Whilst this discussion has tried to pose some wider questions about the understanding of cybercrime it too remains very much within the confines of academic, rather than public discussion. This kind of insularity is of course a general problem for research, but we might wonder whether, in the context of what appears to a problem with such sweeping societal implications – extending from nation states down to teenage money mules – whether this is satisfactory. For what is never touched upon in questions of meaning is what cybercrime means to *others*? Here any duty of criminology to be 'public' (Loader & Sparks 2010) does not reside solely in making its findings palatable for policy makers, but accessible to everyone. Given current concerns about the way that public understanding of fact, truth and meaning is

being distorted in the mirror of digital mediation this challenge seems especially pressing. Finding a meaning for cybercrime surely also needs to properly represent its relevance to minority as well as to majority groups and to be far more culturally sensitive than it has been to date. But finding *that* kind of mode of meaning in cybercrime remains another story for another day at present.

References

Abelson R.P. (1976). Script Processing in Attitude Formation and Decision Making. In *Cognition and Social Behavior*. Edited by: Carroll JD, Payne J. Hillsdale NJ: Erlbaum.

Albrecht, C., Duffin, K.M., Hawkins, S. and Rocha, V.M.M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*.

Ashiku, L. and Dagli, C. (2020). Agent Based Cybersecurity Model for Business Entity Risk Assessment, *2020 IEEE International Symposium on Systems Engineering (ISSE)*, pp. 1-6,

Back, S., Soor, S & LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory, *International Journal of Cybersecurity Intelligence & Cybercrime*,1(1), 40-55

Back, S. & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence and Cybercrime*, 3(2), 25-47.

Bada, M., Chua, Y. T., Collier, B., & Pete, I. (2021). Exploring masculinities and perceptions of gender in online cybercrime subcultures. In M. Weulen Kranenbarg, & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing* (1 ed., pp. 237-257). Springer International

Basamanowicz, J. and Bouchard, M., (2011). Overcoming the Warez paradox: online piracy groups and situational crime prevention. *Policy & Internet*, *3*(2), pp.1-25.

Basuchoudhary, A., Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets, *Computers & Security*, 87

Bele, J, Dimc, M. Rozman D & Jemec, A. (2014). Raising awareness of cybercrime - the use of education as a means of prevention and protection, *10th International Conference Mobile Learning*

Berghel, H., (2014). The future of digital money laundering. *Computer*, *47*(8), pp.70-75.

Bonabeau, E. (2002). Agent-based modelling: Methods and techniques for simulating human systems, *Proceedings of the National Academy of Sciences* May 2002, 99 (suppl 3) 7280-7287;

Bowman, J. and Freng, K. (2017). Differential Association Theory, Social Learning Theory and Cybercrime,in Steinmetz, K. & Nobles, M. (eds) *Technocrime and Criminological Theory*, London Taylor and Francis

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A. and Maimon,

D., (2019). Situational Crime Prevention,in *Cybercrime Prevention* (pp. 17-33). Palgrave Pivot, Cham.

Broadhead, S. (2018) The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, *Computer Law & Security Review*

Brown S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2):223-244.

Burruss, George W., Bossler, Adam M. And Holt, T. J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. *Crime and Delinquency*, 59(5), 1157-1184

Chainanalysis (2020). Crypto Crime Report. Available at: https://go.chainalysis.com/2020-crypto-crime-report

Chism, K. & Steinmetz, K (2017). Technocrime and Strain theory in Steinmetz, K. & Nobles, M. (eds) *Technocrime and Criminological Theory*, London: Taylor and Francis

Collier, B. Clayton, R.,Hutchings, A. & Thomas, D. (2021). Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture, *The British Journal of Criminology*, 61, 5, 1407–1423

Cornish, D.B. (1994). Crimes as scripts. In: Zahm, D, Cromwell, P (eds) *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*. Tallahassee, FL: Florida Statistical Analysis Center.

Donner, C., Marcum, C., Jennings, W., Higgins, G. & Banfield, J (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy, *Computers in Human Behavior*, 34,165-172

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, *19*, 91–150.

Dearden, T.E., Parti, K. (2021). Cybercrime, Differential Association, and Self-Control: Knowledge Transmission Through Online Social Learning. *Am J Crim Just*

Dehghanniri H, Borrion H. (2021). Crime scripting: A systematic review. *European Journal of Criminology*. 18(4):504-525.

Dupont, B. (2019). The ecology of cybercrime in Leukfeldt, R. & Holt, T.J. (eds) *The Human Factor in Cybercrime*, London: Routledge

Garoupa N. (2014). Economic Theory of Criminal Behavior. In: Bruinsma G., Weisburd D. (eds) *Encyclopedia of Criminology and Criminal Justice*, Springer, New York, NY.

Geetha,S. P. Dinesh Kumar, G. Senthil Velan, D. Ali, S & Kanya, N. (2020). Big Data Analysis - Cybercrime Detection in Social Network, *Journal of Advanced Research in Dynamical and Control Systems*, 12,04, 147-152

Harvey, D. (1990). *The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change*. Cambridge, MA: Blackwell.

Henry N, Flynn A. (2019). Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence Against Women*. 25(16):1932-1955.

Hinduja, S. and Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, 26(4), 383-402

Hirschi, T. (1969). *Causes of delinquency.* Berkeley, CA: University of California Press.

Fugii, E. T. (1975). Heroin addiction and public policy, *Journal of Urban Econ.* 2:181-198.

Gottfredson, M., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grabosky, P. (2001). "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies* 10(2):243–249

Howell, C. Burruss, G., Maimon, D. & Sahani, S. (2019). Website defacement and routine activities: considering the importance of hackers' valuations of potential targets, *Journal of Crime and Justice*, 42:5, 536-550,

Hutchings, A, Holt, T.J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology* 55(3): 596–614.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information*. New York: Palgrave

Holt T.J., Turner N.D., Freilich J.D. &Chermak S.M. (2021). Examining the Characteristics That Differentiate Jihadi-Associated Cyberattacks Using Routine Activities Theory. *Social Science Computer Review*, 10

Jaishankar, K. (2008). Space Transition Theory of Cybercrime, in Schallmeger, F. & Pittaro, M. (eds) *Crimes of the Internet*, Upper Saddle River, N.J. : Prentice Hall, pp. 283-296

Junger, M., Wang, V. & Schlömer, M. (2020). Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. *Crime Science*9**,** 13

Kigerl, A. (2021). Routine activity theory and malware, fraud, and spam at the national level. *Crime, Law and Social Change* 76:2, pages 109-130.

Kleemans, E. & Rutger, E (2019). Cybercrime, money mules and situational crime prevention in Hufnagel, S. & Moiseienko, A. (ed) *Criminal Networks and Law Enforcement*, pp.75-89

Leukfeldt, E. (2015). Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions, *The European Review of Organised Crime* 2(2), 91-103

Leppänen, A., Toiviainen, T., & Kankaanranta, T. (2020). From a Vulnerability Search to a Criminal Case: Script Analysis of an SQL Injection Attack,

International Journal of Cyber Criminology, Vol. 14, 1**,** 63-80.

Louderback, E. & Antonaccio, O. (2021). New Applications of Self-Control Theory to Computer-Focused Cyber Deviance and Victimization: A Comparison of Cognitive and Behavioral Measures of Self-Control and Test of Peer Cyber Deviance and Gender as Moderators, *Crime and Delinquency*, 67, 3, 366-398

Lu, Y. Luo, X., Polgar, M & Cao, Y (2010). Social Network Analysis of a Criminal Hacker Community, *Journal of Computer Information Systems*, 51:2, 31-41

Manky, D. (2013). Cybercrime as a service: a very modern business, *Computer Fraud & Security*, Volume 2013, 6, 9-16

McAlaney, J., Kimpton, E. & Thackeray, H., (2019). Fifty shades of grey hat: A socio-psychological analysis of conversations on hacking forums, *CyPsy24: Annual CyberPsychology, CyberTherapy & Social Networking Conference,* 24-26 June 2019, Norfolk, VA, USA.

McCulloch, L. & Furlong, S. (2019). *DM for details: Selling Drugs in the Age of Social Media*, Volteface

McGuire, M. R. & Dowling, S. (2013). *Cybercrime - A Review of the Evidence*, HOS/11/047, Home Office

McGuire, M. R. (2007). *Hypercrime: the new geometry of harm*, London Routledge

McGuire, M. R. (2018a). Cons, Constructions and Misconceptions of Computer Related Crime: From a Digital Syntax to a Social Semantics. *Journal of Qualitative Criminal Justice & Criminology*, 6,2

McGuire, M. R. (2018b). *Into the Web of Profit: - Analysing the cybercrime economy* – Bromium: industry report

McGuire, M. R. (2019a). It ain't what they do, it's the way that they do it. Why we still don't understand Cybercrime' (in Leukfeldt, R. & Holt, T. *The Human factor in Cybercrime*, Routledge

McGuire, M. R.(2019b). *Social Media platforms and the Cybercrime Economy*, Bromium: industry report

McGuire, M. R., (2019c). *Behind the Darknet Black Mirror*, Bromium: industry report

McGuire, M. R., (2021). *Nation States, Cyberconflict and the Web of Profit*, Hewlett Packard: industry report

McGuire M. R. (forthcoming) *Platform Criminality and Post Crime*, London Routledge

Mershon, C and Shvetsova, O. (2019). *Formal Modelling in Social Science*. Ann Arbor MI: Michigan University Press

Mikhaylov, A. and Frank, R., (2016). Cards, money and two hacking forums: An analysis of online money laundering schemes. In *2016 European intelligence and security informatics conference (EISIC)* (pp. 80-83). IEEE.

Moon, B., McCluskey, J.D. and. McCluskey, C.P (2010). A general theory of crime and computer crime: An empirical test, *Journal of Criminal Justice*, 38 (4) pp.

767-772

Moore, M. H. (1970). *The Economics of heroin distribution***.** Croton-on-Hudson, NY: Hudson Institute.

Moore, T. and Clayton, R., (2007). Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*,pp. 1-13.

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). # Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*, 63, 101-110

NCSC (2017). Cybercrime: understanding the online business model, *National cybersecurity centre*. June

Nodeland, B. (2020). The effects of self-control on the cybercrime victim-offender overlap. *International Journal of Cybersecurity Intelligence and Cybercrime*, 3(2), 4-2

O'Hara, A.C., Ko, R.K.L., & Mazerolle, L. (2020). Crime script analysis for adult image-based sexual abuse: a study of crime intervention points for retribution-style offenders. *Crime Science* 9**,** 26

Onuchowska, A. and Berndt., J. (2019). Using Agent-Based Modelling to Address Malicious Behavior on Social Media, *ICIS 2019 Proceedings*. 24

Orsagh, T. (1983). Is there a place for economics in Criminology and criminal justice? *Journal of Criminal Justice*, 11. pp. 391-401

Pastrana S., Hutchings A., Caines A., Buttery P. (2018). Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum. In: Bailey M., Holz T., Stamatogiannakis M., Ioannidis S. (eds) *Research in Attacks, Intrusions, and Defenses*. RAID 2018. Lecture Notes in Computer Science, vol 11050. Springer, Cham.

Payne, B. (2018). White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both? *Criminology, Criminal Justice, Law & Society*, 19 (3), p.17

Payne, B.K., Hawkins, B. & Xin, C. (2019). Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes. *Am J Crim Just* **44,** 230–247

Perkins, R., Jordan Howell, C. Dodge, C., Burruss, G. &Maimon, D.(2020). Malicious Spam Distribution: A Routine Activities Approach. *Deviant Behavior* 0:0, pages 1-17.

Parise, J. (2019). Heads Up: Cybercriminals Are Businesspeople, *CFO* 2/8/2019

Porcedda, M. and Wall, D. (2021). "Modelling the Cybercrime Cascade Effect in Data Crime," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, 2021 pp. 161-177.

Putnam, H. (1973). Meaning and Reference. *The Journal of Philosophy*, *70*(19), 699–711.

Rajivan P, Janssen MA, Cooke NJ. (2013). Agent-Based Model of a Cyber Security Defense Analyst Team. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 57(1):314-318.

Reyns, B.W., (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), pp.99-118.

Reyns, B. W., Henson, B., Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38, 1149-1169.

Reyns, B. (2017). Routine Activity Theory and Cybercrime in Steinmetz, K. & Nobles, M. (eds) *Technocrime and Criminological Theory* London: Routledge

Roth, R. and Berlinger, J. (2021). North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report , *CNN*, 09/02/2021

Rottenberg, S. (1968). The clandestine distribution of heroin, its discovery and suppression. *J. of Poli. Econ*. 76: 78-90.

Rubin, P. H. (1973). The economic theory of the criminal firm, in Rottenberg, S. (ed) The *Economics of Crime and Punishment***,** Washington, DC: American Enterprise Institute for Public Policy Research.

Salmon, Wesley C.. "The Sufficiency/Necessity View". *Scientific Explanation and the Causal Structure of the World*, Princeton: Princeton University Press, (2020), pp. 185-190.

Sarkar, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. *The Cyber Defense Review*, 87–102.

Schank R, Abelson R. (1977). *Scripts, Plans, Goals, and Understanding*. Hilladale NJ: Lawrence Erlbaum Associates

Schelling, T. (1967). Economics and criminal enterprise. *The Pub. interest* 7: 61-78**.**

Sela-Shayovitz R. (2012). Gangs and the Web: Gang Members' Online Behavior. *Journal of Contemporary Criminal Justice*.;28(4):389-405.

Skinner, W. & Fream, A. (1997). A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*. 34(4):495-518.

Sloman, S., Barbey, A. & Hotaling, J. (2009). A Causal Model Theory of the Meaning of Cause, Enable, and Prevent. *Cognitive science*. 33. 21-50.

Somer, T, Tiido, A, Sample, C, Mitchener-Nissen, T (2018). Application of journey mapping and crime scripting to the phenomenon of trolling. In: *ICCWS 2018 13th International Conference on Cyber Warfare and Security*. Academic Conferences and Publishing Limited, 465.

Stockman, M., (2014). Insider hacking: applying situational crime prevention to a new white-collar crime. In *Proceedings of the 3rd annual conference on Research in*

information technology,pp. 53-56.
Steinmetz, K.F. (2015). Craft(y)ness: An ethnographic study of hacking. *British Journal of Criminology*, 55, 125–145.
Sutton, M. (1998). Handling Stolen Goods and Theft: A Market Reduction Approach. Home Office Research Study 178. Home Office. London.
Sutton, M., Schneider, J.L. and Hetherington, S. (2001). Tackling theft with the market reduction approach. *Home Office Crime Reduction Research Series* Paper 8.
Suler, J. (2004). The Online Disinhibition Effect, *Cyberpsychology & Behavior* 7(3):321-6
Thompson B, Morris-King J. (2018). An agent-based modeling framework for cybersecurity in mobile tactical networks. *The Journal of Defense Modeling and Simulation*. 2018;15(2):205-218.
Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker, International *Journal of Cyber Criminology*,2 (2): 382–396
UNODC (2011). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, *United Nations Office on Drugs and Crime*, October
Van der Bruggen M, Blokland A. (2021). A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb. *Sexual Abuse*. 33(8):950-974.
Van der Wagen, W. & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks, *The British Journal of Criminology*, 55, 3, 578–595,
Van de Weijer, S.G. and Leukfeldt, E.R., (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), pp.407-412.
Wall, D. (2007). *Cybercrime – The Transformation of Crime in the Information Age,* London :Polity
Wall, D. (2014). 'High risk' cyber-crime is really a mixed bag of threats, *The Conversation*, 14/11/2014
Williams, M., Levi, M., Burnap P. & Gundur, R.V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory, *Deviant Behaviour* 40:9, 1119-1131,
Willison, R. and Siponen, M., (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), pp.133-137.
Wortley, R. (1997). "Reconsidering the Role of Opportunity in Situational Crime Prevention." In: G. Newman, R.V. Clarke and S.G. Shohan (eds.), Rational Choice and Situational Crime Prevention. Aldershot, UK:Ashgate Publishing.

Wortley, R. (2010). Critiques of situational crime prevention. In B. Fisher & S. Lab (eds) Encyclopedia of Victimology and Crime Prevention. Thousand Oaks, CA: Sage.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. European Journal of Criminology, 2, 407–427.

Yip, Michael (2011). An investigation into Chinese cybercrime and the applicability of social network analysis. *ACM WebSci '11, , Koblenz, Germany. 13 - 16 Jun 2011.*

Invitation Article

Challenges Related to Fight Against Cybercrime. A Need to Strengthen International Cooperation

*Markko Künnapu**
Legal Advisor
Criminal Policy Department
Ministry of Justice of Estonia

Abstract

The objective of this article is to highlight the need for additional tools and frameworks for international cooperation. As the cyber threat landscape has considerably worsened in the last few years, in particular during the COVID-19 pandemic, law enforcement authorities worldwide need to take necessary measures to respond to this situation. As there are also new types of crime and modus operandi emerging, countries need to assess their legislative and organizational frameworks, and improve their capacities to detect and investigate these criminal offences. As most of the cases are of cross-border nature and electronic evidence needed for the investigations is stored in other countries, there is a greater dependence on international cooperation in conducting successful investigations. As traditional Mutual Legal Assistance measures don't provide the necessary speed and effectiveness needed to adequately address the cybercrime threat, additional tools need to be developed. So far the Convention on Cybercrime or Budapest Convention has been the only international legally binding treaty on cybercrime and electronic evidence. In order to provide additional measures to supplement the ones established in the Convention, officials have opened discussions about creating the Second Additional Protocol. Although the background work and preparations for the Protocol were conducted over the course of several years, the Protocol negotiations started officially in September 2017. In May 2021 the Cybercrime Convention Committee agreed on the conditions of the Protocol. The Protocol would complement the Convention and provide several new tools and measures for law enforcement authorities. These measures include inter alia Mutual Legal Assistance and disclosure of computer data in emergency situations as well as providing avenues for direct cooperation with Multinational Service Providers. The Protocol will be opened for signature in 2022 and hopefully implementing the measures listed in the Protocol will aid in the fight against cybercrime and increase the effectiveness of international cooperation. As the threats and risks related to cybercrime have increased over the years, it is also time for law enforcement to display a stronger response to this pressing issue.

Keywords

cybercrime, Budapest Convention, international cooperation, COVID-19

* Direct correspondence to Markko Künnapu, J.D; Markko.Kynnapu@just.ee
* This paper originally written by Mr. Markko Künnapu was presented at the keynote session of the Korean Institute of Criminology International Forum 2020 in Seoul, Korea
* http://dx.doi.org/10.36889/IJCJ.2021.007
* Received 22 October 2021; Revised 25 October 2021; Accepted 4 November 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 36-42

BACKGROUND

Governments as well as international organizations are reporting increased numbers related to cybercrime and other cyber-related threats. The current COVID-19 pandemic has brought about additional challenges for law enforcement authorities worldwide. Working from distance online and use of remote tools has increased peoples' vulnerabilities to being victims of cybercrime. Furthermore, lack of awareness about the threats and lack of sufficient preventative measures can facilitate cybercrime. Individuals, businesses and governments suffer more and more from different types of cybercrime.

Cybercrime has also changed in regards to its targets and potential negative impacts, in relation to the nature of its threats to national security, the economy, and political systems. This in turn requires an effective response from governments who need to take measures to prevent, detect and investigate cybercrime.

The current COVID-19 pandemic has already shown that cybercrime has the potential to become even worse, more aggressive, more complicated and more expensive to handle than its previous forms. We have also witnessed more attacks against governments and critical infrastructure, including against the health sector. This also means that the approaches and policies to tackle cybercrime must change accordingly to meet these new threats and trends.

Restrictions, limitations related to physical presence and meetings, and working remotely online have also brought about new threats and vulnerabilities in relation to cybercrime. These factors also have a negative impact on the operation of law enforcement authorities and judiciaries.

Problems related to creating measures to fight against cybercrime have arisen previously. However, the current situation and the complications related to the COVID-19 pandemic amplifies the gravity of these difficulties. This means that both businesses and individuals have increased expectations that governments will ensure safe and secure cyberspace and display effective responses to cybercrime. However, several different indicators reveal that only a small fraction of cybercrime offences are being reported and investigated.

CHALLENGES

There is a need for an effective joint response to cybercrime. Still in many countries legislative framework can be fragmented and capacities to detect and investigate cybercrime are low.

This needs to change and governments have different options to respond. First there needs to be strategic approaches and policies on how to improve capacities for the perpetuation and sustainability of proposed solutions. This includes strategies on cybersecurity and cybercrime, as well as necessary supporting legislative framework.

In regards to the criminal justice response to cybercrime, it is important to highlight substantive and procedural law as well as securing a legal basis for national and international cooperation.

There has to be sufficient capacity and competent and specialized institutions to investigate cybercrime and analyse electronic evidence, including digital forensics. Competent authorities need to have all the necessary resources to perform their duties. Law enforcement authorities and judicial authorities need to pay attention also to training. As technology is evolving and so do threats, it is of utmost importance to provide up to date training for all.

Cooperation has continued to be and will remain a key issue in tackling cybercrime. Most of the data or electronic evidence is currently being stored by private sector entities. There is a need for a legislative framework which would enable swift and smooth cooperation between the public and private sectors. Building trust and a culture of cooperation is relevant, because both sides have a respective role to play in fighting cybercrime. Law enforcement authorities should also consider officially signing cooperation agreements or memorandums of understanding in order to make public-private partnerships fully effective.

Most of the cybercrime offences and cyber-related threats are of cross-border nature. This means that legislative and organizational frameworks are not always sufficient if the sole focus is put on national level cooperation and reliance on domestic competent authorities.

Countries need to learn how to cooperate with each other in the most effective manner. However, this is the area that needs most attention in terms of effectively dealing with issues related to cybercrime. This requires a legal basis for cooperation, ensuring maximum availability of channels for cooperation, and achieving a mutual

agreement between parties about minimum standards. Without securing these conditions, cooperation would not work or would not be effective.

As most of the threats and incidents are of cross-border nature, governments cannot fight cybercrime alone. Even if a country adopts sufficient substantive and procedural law provisions, criminalizes cybercrime and provides necessary tools for law enforcement authorities, there is still an urgent need for international cooperation.

As cybercrime has become a cross-border phenomenon, victims, perpetrators as well as computer systems used may be located in different jurisdictions. This applies also to computer data or electronic evidence needed to investigate the case and identify the perpetrators.

This is often problematic, because countries have different views not only in regards to substantive law (what should be considered as cybercrime), but also often express differing opinions about how international cooperation should operate.

THE BUDAPEST CONVENTION

Every country needs to think about and analyze possible options in relation to this issue and how to improve both legislative frameworks and international cooperation.

Currently, there is only one international legally binding instrument on cybercrime and electronic evidence – the Convention on Cybercrime, also known as the Budapest Convention (The Budapest Convention on Cybercrime, 2001).

The Budapest Convention can serve as a model here, providing not only minimum standards on substantive and procedural law, but also a legal basis for cooperation. It is important to note that the provisions of the Convention can also address other criminal offences where electronic evidence is involved. The Convention uses language that is technology-neutral and can be applied to different types on cybercrimes.

The Convention can be considered an instrument on cybercrime and electronic evidence that has a global impact. Many countries have already joined the Convention, and even more have used it as a guide to develop or update domestic legislation, including substantive and procedural law.

The Convention is also being used on a daily basis for international cooperation and to exchange information. The Convention can be used to request preservation, production and real-time access of data from another party. In addition to mutual legal

assistance and cooperation between central authorities, it provides avenues for international cooperation through its 24/7 network and points of contact.`

2ND ADDITIONAL PROTOCOL

However, there is still room for improvement in order to ensure effective and timely access to electronic evidence that is being stored abroad, including “in the cloud.”

When speaking about electronic evidence, one has to think about its particular characteristics, in particular its volatile nature. Computer data can be copied, moved or deleted very fast and this may involve computer systems in multiple jurisdictions. It is often the case that the exact location of data remains unknown, in particular when law enforcement authorities face so-called darkweb investigations.

The prevalent issues that arise here are how to ensure timely access to data, how to secure it and how to obtain it. The Budapest Convention contains several procedural measures related to preservation, production and real-time access to data. However, as data moves fast across the borders, these measures alone might not be sufficient.

There are no boundaries for individuals in cyberspace and they can copy, move, and delete data as they wish, in particular when it comes to different cloud computing services. For law enforcement these boundaries still exist and rules and principles on international cooperation apply.

As existing or traditional mutual legal assistance frameworks were not designed to address electronic evidence and don’t provide necessary speed and effectiveness, additional tools need to be developed.

Consultations related to the Second Additional Protocol to the Budapest Convention have been ongoing for years. In September 2017 the Cybercrime Convention Committee started to draft and negotiate the text of the protocol. The main aim is to provide new measures and tools to obtain electronic evidence in addition to traditional mutual legal assistance. These tools would complement existing measures and would cover inter alia direct cooperation with multinational service providers, allowing for faster procedures in emergency situations.

In May 2021 the Cybercrime Convention Committee finally agreed to the text of the Additional Protocol. Although there are still internal consultations taking place at

the Council of Europe level it is expected that it will be adopted by the end of 2021 and opened for signature at the beginning of 2022. The Additional Protocol would be open for ratification for all State Parties to the Convention. This also means that in order to ratify the Protocol, a country needs to first become a party of the Convention (T-CY Protocol Drafting Group, 2021).In regards to the content of the Additional Protocol, it would provide for the following additional tools for law enforcement authorities.

First, it would provide a framework and new measures related to direct cooperation with service providers. These measures address both subscriber data and traffic data, which can be used instead of already available international cooperation measures. As practice has shown, law enforcement authorities request the most subscriber information and traffic data, so it is expected that cooperation would become faster and more effective by implementing this measure.

Special attention has also been paid to requests for domain name registration information and providers who offer domain name registration services. This would also enable enhanced cooperation and allow for easier and more efficient identification of registrants of a particular domain name.

Time and the need for fast responsiveness has always been a challenge for cross-border investigations, in particular in cases where electronic evidence is involved. Therefore, this protocol to establish new frameworks, measures and concrete deadlines for cooperation is unquestionably a huge step forward.

As we have already explained, mutual legal assistance frameworks and measures were not designed to address electronic evidence. Due to its volatile nature, electronic evidence requires a different approach and needs to be dealt with in a faster, more efficient manner.

For this particular reason the protocol also addresses mutual legal assistance and provides additional frameworks and legal bases for emergency situations. These measures include expedited disclosure of stored computer data, including content data as well as emergency mutual assistance.

Still, we need to bear in mind that countries and their legal systems are different. For this reason, the protocol would also provide flexibility. By allowing reservations and declarations, the protocol should satisfy the needs of all countries, in particular those countries who wish to have stronger conditions and safeguards in place. Therefore, certain differences concerning cooperation with individual countries could

remain.

Lastly, the protocol provides for rules that can be also found in other international instruments. These include rules on language that could be used for requests, potential for application of video conferencing, and use of joint investigation teams.

As in the Convention, the protocol pays much attention to conditions and safeguards, including safeguards related to personal data protection. We hope that the new protocol with its additional tools related to electronic evidence will make the fight against cybercrime more effective.

Information about the Convention as well as negotiations and public consultations on the 2nd Additional Protocol is publicly available for viewing at the Council of Europe's Cybercrime Convention Committee website (Cybercrime Convention Committee, 2021).

We hope that the protocol and the result of the years of work towards handling cybercrime will provide suitable measures for all parties involved, as well as necessary added value to the fight against cybercrime. As it is expected that the protocol will opened for signature at the beginning of 2022, this development can also be considered an important milestone at the international level. For example, as the European Union is still negotiating its electronic evidence proposal and United Nations is about to start work on a new instrument, it is crucial to have the text of the protocol already prepared and available for immediate use. Countries can use the protocol as guidance to adapt their legislative and organizational frameworks in order to have more effective responses to cybercrime worldwide.

References

Cybercrime Convention Committee. (2021). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Draft). Retrieved from "https://rm.coe.int/0900001680a42c4b"

T-CY Protocol Drafting Group. (2021). Protocol negotiations. Retrieved from "https://www.coe.int/en/web/cybercrime/t-cy-drafting-group"

The Budapest Convention on Cybercrime. (2001). T.I.A.S 131, E.T.S. No. 185. Retrieved from "https://www.coe.int/en/web/cybercrime/the-budapest-convention." Accessed 8 November 2021

The Effects of Investigator's Individual Factors on Investigative Decision Making: A Systemic Review

*Denis Lino**
Federal University of Pernambuco

Abstract

At the center of a criminal investigation is the ability of the lead investigator to identify all possible hypotheses, make sense of the information available and define appropriate investigative actions. These characteristics are usually dependent on what has been termed as investigative decision making, the process where an investigator analyzes the evidence and decides which actions to take. Previous research and reports have identified situational, organizational, and individual factors that may hinder or improve investigative decision-making. The present paper aims to identify which individual factors have been empirically tested concerning investigative decision making, and how they affect it. A systematic review was conducted, nine peer-reviewed papers were analyzed, and five factors were identified: Experience, Gender, Need for Cognitive Closure (NFC), Time-urgency, and Fluid Intelligence. Experience had mixed findings, suggesting that how officers developed expertise is more important than time on the job. Gender was only significantly related to investigative decision-making in a specific scenario. Low NFC, non-time-urgent individuals, and high fluid intelligence were related to effective investigative decision-making. Recommendations for the future academic development of the field, and how police forces can apply this knowledge are suggested.

Keywords

Criminal Investigation; Investigative Decision Making; Individual

* Direct correspondence to Denis Lino; denisvictorlino@gmail.com
* This study was financed in part by the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).
* http://dx.doi.org/10.36889/IJCJ.2021.008
* Received 8 October 2021; Revised 11 November 2021; Revised 7 December 2021; Accepted 15 December 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 43-67

INTRODUCTION

During a criminal investigation, there are dozens of decisions that investigators must make (Spanoudaki, Ioannou, Synnott, Tzani-Pepelasi & Pylarinou, 2019). In a situation where a body has been found, they may want to explore the idea that it was a fatal accident, a robbery has gone wrong, a murder, or a suicide. Each of these possible hypotheses will require the allocation of resources and time to be followed up. Investigators must decide who needs to be interviewed, which forensic experts need to be consulted to solve the case, if/when someone must be considered a prime suspect, if/when this suspect should be accused and detained, among other considerations. This process of making sense of the available information and deciding which course of action to follow from several possible options has been termed investigative decision making.

Unlike day-to-day decision making, such as which route to take from work, or which product to buy from the store, investigative decision making is extremely complex due to the high number of possible explanations for a single incident, the ambiguity and incompleteness of information available, and pressure from multiple sources to quickly solve every criminal incident (Rossmo, 2009). On top of that, the consequences of faulty investigative decision making are disastrous; several reports have identified how it has led to misallocation of scarce police resources and miscarriages of justice such as wrongful arrests and wrongful convictions (Rossmo & Pollock, 2019). Given its uniqueness and far-reaching consequences that affect those directly involved (e.g., investigators and suspects) and public trust in the criminal justice system, investigative decision making has gained increased attention from researchers and practitioners seeking to improve it and avoid pitfalls.

Many high-profile cases have highlighted how investigators fell prey to cognitive biases when making decisions, which hindered their investigative capacity and led to wrongful arrests or convictions (Simon, 2012). The most commonly identified bias in the investigative context is the confirmation bias, a phenomenon where people tend to search for evidence that confirms (rather than falsify) an initial belief, position, or opinion held (Rossmo & Pollock, 2019). Under confirmation bias, investigators may develop tunnel vision, a state in which they focus on a single specific suspect or narrative of what has occurred, seeking only confirmatory evidence while neglecting

or misinterpreting any competing evidence (Ask & Fahsing, 2018).

In addition to cognitive biases, heuristics may also negatively affect investigative decision making. While biases are erroneous thought patterns, heuristics are mental shortcuts that help us make sense of large quantities of information and make decisions more easily (McLaughlin, Eva & Norman, 2014). A type of heuristics is the satisficing heuristic, where people will search for as many available options as they can before settling for one that is "good enough" (Bendor, Kumar & Siegel, 2009). It has been found that investigators may use satisficing heuristics when making decisions, given that they search for possible explanations or suspects only until they find a "good enough" fit, after which they would then focus on finding incriminating evidence (Ask & Alison, 2010).

Although heuristics have been proven to lead to accurate outcomes most of the time, even when compared to statistical approaches, it can lead people on the wrong course sometimes (McLaughlin et al., 2014). Snook and Cullen (2009) made a case for the use of heuristics in investigative decision making; however, there has been no further testing of their accuracy and applicability in this context. Considering that one mistake in a criminal investigation may lead to the imprisonment of an innocent person, heuristics should be avoided before its applicability and consequences to investigative decision making are thoroughly understood.

In light of this, efficient investigative decision making must avoid relying on heuristics or falling to cognitive biases, but how can investigators develop the necessary skills or adopt the investigative mindset to thoroughly investigate every criminal incident and overcome these obstacles? Academics and practitioners have proposed some characteristics and actions on how to improve investigative decision making. Investigators must have an "open-mind" perspective when investigating any case, no matter how simple it may seem they must not jump to conclusions and consider every possible alternative for the incident (Lepard & Campbell, 2009). On top of that, they must make an effort to avoid biases and heuristics, such as considering the opposite to avoid confirmation bias and exhaustively investigating possible hypotheses to avoid satisficing (Ask & Fahsing, 2018). These characteristics and actions can be summarised in an investigative decision making style that considers all possible hypotheses and works towards falsifying (instead of confirming) each hypothesis, the hypothesis that cannot be falsified is the most likely to be true.

Unfortunately, it is not that simple, interviews with experienced investigating

officers and reviews of high profile cases indicate that are influencing effective investigative decision making (Ask & Fahsing, 2018; Spanoudaki et al., 2019; Rossmo & Pollock, 2019). These can be divided into three categories: organizational, situational, and individual. Organizational factors are those typical of policing or police forces' structure, such as training, work relations, policies, and guidelines. For example, some police forces require investigators to record all decisions made during a criminal investigation for future analysis of their decision making (Dando & Ormerod, 2017). However, it may lead investigators to avoid making decisions and let the case drift on because of anticipated regret, which can result in loss of important investigative leads due to the passage of time.

Situational factors are external influencers, an environmental feature, characteristics of the crime, or contextual variables during the investigation. A frequent situational factor of criminal investigations is time pressure as detectives often have to quickly solve their cases and move on to the next. Under time pressure, investigators' abilities to keep an open mind, generate competing hypotheses from the same information, and avoid impulsive conclusions are hindered. (Ask & Alison, 2010). Other situational factors include emotional impact caused by each case (e.g., an especially brutal murder or child sexual abuse) and media attention (Crego & Alison, 2004; Spanoudaki et al., 2019).

Individual factors are related to the personal characteristics of the investigator, such as their gender, experience, personality traits, and cognitive abilities. Studies on gender differences in decision making have identified that men performed better than women on tasks related to heuristics and biases, such as statistical reasoning and actively open-minded thinking (Toplak et al., 2016; Weller et al., 2018). On the other hand, men have also been found to process information selectively, ignoring potential risks as long as they achieve their goal, while women are more considerate of the benefits and risks of a decision (Byrne & Worthy, 2016). These differences generate ambiguous expectations as to how investigative decision making may be affected by gender because male detectives appear to be less susceptible to heuristics and biases. However, their decision making style is impulsive and inconsiderate of the negative consequences, which could lead them to make hasty judgments and jump to conclusions.

Experience is often cited by investigators as a predictor of good decision making (Spanoudaki et al., 2019). Experienced decision-makers are expected to make

decisions faster and achieve better outcomes because of the larger mental database of cases they have access to. They can assess a situation, compare it to previous scenarios and choose a course of action that worked in the past for a similar case (Klein, 1993). Research on medical decision making found that domain-specific experts generated accurate diagnoses sooner than non-domain-specific experts (Stolper et al., 2011).

Although experience indeed leads to faster and accurate decisions, it can also lead professionals to consider fewer hypotheses and rely on heuristics to solve problems. The same research on medical decision making found that doctors relied on "gut instinct" to select the correct diagnoses and, since they identified the correct hypotheses sooner, they also generated fewer hypotheses (Stolper et al., 2011). This highlights that more hypotheses do not necessarily mean better hypotheses and that experts often use satisficing heuristics. However, when investigators do not consider all hypotheses, they may fall under the influence of tunnel vision, which has well-known negative consequences (Rossmo & Pollock, 2019).

Personality traits such as time-urgency and the Need for Cognitive Closure (NFC) are also thought to influence decision making. Time-urgency refers to how people perceive the passage of time, time-urgent (vs non-time-urgent) people often perceive time to pass faster than it does, which affects how they perform in problem-solving tasks (Conte, Mathieu & Landy, 1998). Considering that external time pressure hinders decision makers abilities to consider multiple hypotheses and fall prey to cognitive biases, it is expected that internal time pressure (time-urgent individuals) will have similar effects. On the other hand, non-time-urgent individuals may be better equipped to deal with external time pressure, reducing its negative consequences on decision making.

NFC is a psychological term that refers to how people deal with certainty and ambiguity, it has been described as "the desire for a definite answer on some topic, any answer as opposed to confusion and ambiguity" (Kruglanski, 1990, p. 337). High NFC people are prone to attain closure as soon as possible, looking for any suitable explanation or solution for a problem. For that reason, they are more likely to seize and freeze on an early judgment of the situation. Low NFC people deal better with uncertainty and suspend committing to an early judgment, they are comfortable with searching for alternative explanations or solutions. In light of this, the "open-minded" characteristic of a good investigator is opposite to high NFC because these individuals

do not deal effectively with the uncertainty of considering multiple possible hypotheses for a criminal investigation, they will search for quick suitable answers that provide them closure, which could lead to confirmation bias.

It has long been recognized that intelligence is not a single construct but a combination of different types of intelligence. The Cattel-Horn-Carroll (CHC) model posits that intelligence can be divided into three strata, one that is general intelligence, a second that consists of broad intellectual capacities, and a third that encompasses narrow intelligence abilities (Primi, 2003). Fluid intelligence is part of the second stratum, it is a broad intelligence capability that refers to ones' ability to reason and solve new problems (McGrew, 2009). Research on fluid intelligence has identified that it is linked to performance in different settings, such as better academic performance (Colom et al., 2007; Ali & Ara, 2017), better performance on intellectually demanding video games (Kokkinakis, Cowling, Drachen & Wade, 2017), and solving complex problems (Tschentscher, Mitchell & Duncan, 2017). Considering that investigative decision making is, in essence, solving problems ("what happened", "how it happened", "who did it") and is intellectually demanding, it is expected that individuals who score high on fluid intelligence measures will perform better at investigative decision making tasks.

Even though situational, organizational, and individual factors have significant influence over investigative decision making, individual ones seem to moderate the effect of the others. For example, time pressure has significant detrimental effects on investigative decision making, but if the investigators are non-time-urgent, these effects are diminished. In addition, every investigator will be subjected to situational and organizational factors, but how much they will be affected by it will vary according to their characteristics. Considering the importance of individual differences and the plethora of individual factors that can, in theory, affect investigative decision making, the present paper aims to: 1) Identify which individual factors have been empirically tested concerning investigative decision making; 2) Analyse how these factors influence investigative decision making.

To achieve these objectives, a systematic review of the literature was conducted, given that it is the most reliable method for identifying, evaluating, and synthesizing the available scientific evidence on a given subject (Siddaway, Wood & Hedges, 2019). Furthermore, systematic reviews are particularly useful for informing practice and public policies. In this case, we as researchers, practitioners, and society need to

know which individual characteristics are connected to potentially better investigative outcomes. Virtually every police force in the world uses psychological assessment before admitting an officer into its ranks, especially if this officer is going to be responsible for conducting high complexity criminal investigations. Therefore, knowledge of which characteristics to look for or develop in investigating officers is essential to achieve a more complete and error-proof justice system.

Method

Systematic review protocol

A systematic search was carried out in four databases: PsycInfo, Microsoft Academics, PubMed, and *Periódicos Capes* (a Brazilian academic search database that encompasses over 48.000 journals worldwide). To identify every research that analyzed investigative decision making and potential individual factors influencing investigators abilities, the following descriptors were used: "Investigative Decision Making" AND (individual* OR personal*); "Police Decision Making" AND (individual* OR personal*); "Detective Decision Making" AND (individual* OR personal*). These Boolean operators were used to ensure that papers considering investigative decision making and either individual or personal characteristics were included in the present review, including any possible writing, derived from "individual" (e.g., individually, individuality) and "personal" (e.g., personality). The term "investigative decision making" was chosen because it is widely used by both researchers and practitioners to refer to the specific situation of making decisions when investigating a possible crime. However, to consider possible differentiation in terms used by researchers, "police decision making" and "detective decision making" were also used. Finally, no time cut was made to ensure that all available publications would be considered.

Inclusion and exclusion criteria

Publications were included if the full text was available in English and if it had been published in scientific journals and undergone peer-review. These criteria were used to ensure the quality and availability of the publications considered. Studies that

had not followed an empirical methodology, such as literature reviews were excluded. However, any publication that discussed the matter was analyzed in search of potential papers in the references that were not found through the databases. Only papers that a nalyzed individual or personal factors and their relation to investigative decision making were included. Finally, papers that addressed police or legal decision making in a different context than the process of a criminal investigation were excluded.

Selection process

According to this research protocol, a total of 690 studies were initially identified, of which 17 were collected through additional sources other than the scientific databases (analyses of references used in book chapters and papers on investigative decision making). After the initial assessment, 64 of them were excluded because they were duplicates present in more than one database or repeated documents in the same database. The title and abstracts of the remaining 626 studies were assessed, resulting in 21 papers being considered for further evaluation. Lastly, all 21 papers were read in full; however, only 9 of them met all inclusion and exclusion criteria. A flowchart of the systematic review process is presented in Figure 1.

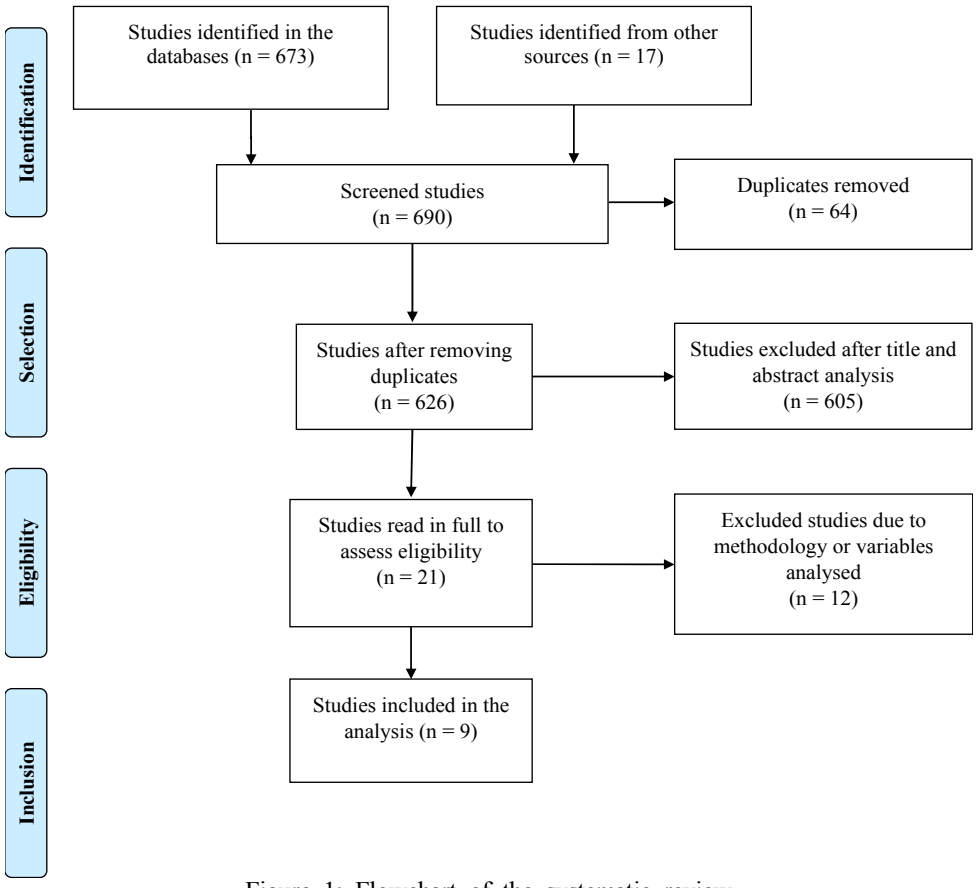


Figure 1: Flowchart of the systematic review

Results

Upon examination of all nine papers that met the inclusion criteria, it has been identified that they analyzed different variables or the same variables in different ways (Table 1 provides a summary of the nine studies). In these situations, a narrative synthesis is recommended because it analyses a collection of quantitative studies that used diverse methods, constructs, or relationships. This method of interpreting results from a systematic review synthesizes the results of individual quantitative studies and is useful to organize findings from different studies around the same subject, to understand how and why a variable has an effect over another (Siddaway et al., 2019).

Table 1: Summary of studies analyzing individual factors and investigative decision making

Research paper	Sample	Independent Variable definition/measurement	Study design	Study aims	Key findings
Expertise and decision making in the linking of car crime series (Santtila, Korpela & Häkkänen, 2004)	n = 33 (9 experienced car crime investigators; 9 experienced investigators of other crimes; 7 novice investigators; 8 no investigative experience). Finnish sample.	Experience defined of at least one year full-time as an investigator (and 5 cases of car crime investigation monthly for experienced car crime investigator); novice had less than 6 months experience as a full-time investigator.	Comparative design measuring participants' abilities to link car thefts together; ANOVA analysis.	Identify whether the experience was related to accurate linking of car crime series.	Experienced investigators with domain-specific knowledge performed better than laypeople in linking car thefts.
Motivational Sources of Confirmation Bias in Criminal Investigations: The Need for Cognitive Closure (Ask & Granhag, 2005)	n = 118 (50 criminal investigators and 68 undergraduate students). Swedish sample.	Criminal investigators had varying degrees of investigative experience (between 2 and 30 years), while undergraduate students had no investigative experience. NFC scale was used to measure NFC (Kruglanski, Webster & Klem, 1993)	Experimental design using manipulated case vignettes about suspect's guilt. Comparison according to experience and NFC. Regression analyses	Verify if NFC and experience moderated the effect of hypothesis perception over the strength of evidence against the suspect.	Investigators presented a "guilt bias" when compared to students. Students were more responsive to potentially exonerating information. Investigators with high (vs low) NFC were less likely to acknowledge evidence contrary to their hypothesis of guilty over the suspect.
Gender Difference or Indifference? Detective Decision Making in Sexual Assault Cases (Alderden & Ullman, 2012).	n = 328 criminal sexual assault cases involving adult female victims reported to a large Midwestern police department in 2003. No cases with multiple, victims, suspects, or investigating detectives were included.	Gender was coded dichotomously (male or female).	Case analysis using logistic regression.	Examine whether gender differences exist in detectives' arrest decisions in sexual assault cases.	Female detectives were significantly less likely to arrest suspects in sexual assault cases even after controlling for the influence of other factors shown to predict arrest.
The Effects of Subjective Time Pressure and Individual Differences on Hypotheses Generation and	n = 76 police officers from a rural UK police force. (n = 35 under time	Experience is defined by the years of domain-specific experience in crime investigation. Used Time	Experimental design manipulating time pressure. Regression analyses.	Examine whether individual differences moderate the effect of time pressure on the	Under time pressure, the experience did not moderate the number of hypotheses generated, time-urgent investigators had a

Research paper	Sample	Independent Variable definition/measurement	Study design	Study aims	Key findings
Action Prioritization in Police Investigations (Alison, Doran, Long, Power & Humphrey, 2013).	pressure manipulation; n = 41 control group).	Paradigm 1.0 (Dougherty et al., 2003) to measure time-urgency. Raven's standard progressive matrices are used to evaluate fluid intelligence (Raven et al., 2003).		number of hypotheses generated.	larger reduction in the number of hypotheses generated than non-time-urgent investigators. Investigators with high (vs low) fluid intelligence generated more hypotheses.
Homicide Detectives' Intuition (Wright, 2013)	n = 40 homicide detectives (10 Detective Constable and Sergeants; 10 Detective Inspectors; 10 Detective Chief Inspectors; 10 Detective Superintendent). British sample.	Experience defined according to rank	Card sorting procedure using crime scene photographs; Think aloud method to categorize and verify number and quality of inferences made. t-test analysis.	Examine the thought processes of detectives when first notified of a homicide; how they categorize and conceptualize different homicide crime scenes and whether the cognitive processes of experienced detectives differ from those less experienced.	Higher-ranking officers (Detective superintendent) made significantly more inferences than the others. Accuracy of inferences has no significant differences across ranks.
The Making of an Expert Detective: The Role of Experience in English and Norwegian Police Officers' Investigative Decision Making (Fahsing & Ask 2016)	n = 124 police officers (31 experienced officers and 30 novice officers from England, 32 experienced officers and 31 novice officers from Norway)	Experienced homicide detectives must have at least 10 years of experience as a detective, and currently, be in charge of major crime investigations. Novice officers must currently work as patrolling officers, have no more than 2 years of policing experience, and have no further education as detective.	Quasi-experimental design comparing the quality of investigative decisions made by experienced detectives and novice police officers in England and Norway Mixed ANOVA analyses.	Compare detectives' ability to generate investigative hypotheses and actions, as well as their vulnerability to investigative tipping points, across different qualification and training regimes and different levels of experience.	Experienced British investigators generated more hypotheses and investigative actions than inexperienced officers. However, the experience did not have a significant effect on a Norwegian sample.
Analyzing Decision Logs to Understand Decision Making in Serious Crime Investigations (Dando &	n = 60 decision logs randomly selected, which accounts for the decision making of 14 Senior	Experienced investigators had over five years of experience in leading investigations, while less experienced investigators had	Quantitative analysis to identify the number of hypotheses generated and qualitative analysis	Study decision making by detectives when investigating serious crime through the	Experienced investigators generated more hypotheses than inexperienced investigators.

Research paper	Sample	Independent Variable definition/measurement	Study design	Study aims	Key findings
Ormerod, 2017)	Investigating Officers. British sample	three years or less.	to consider the content of those hypotheses. ANOVA analysis.	examination of decision logs to explore hypothesis generation and evidence selection.	
In Search of Indicators of Detective Aptitude: Police Recruits' Logical Reasoning and Ability to Generate Investigative Hypotheses (Fahsing & Ask, 2017).	n = 166 newly recruited students at the Norwegian Police University College	Inductive and Deductive Reasoning skills measure by a cognitive aptitude test administered online by a recruitment company. The specific test is not mentioned. Non-significant variables are not explored.	Use of case vignettes to measure quantity and quality of hypotheses generated against independent variables. Multiple regression analysis.	Test if measures of inductive and deductive reasoning skills used for recruitment to the Norwegian police can predict recruits' ability to generate investigative hypotheses, and if these differences moderate participants' vulnerability to decisional tipping points.	Inductive and deductive reasoning abilities did not explain any of the variances in the generation of gold-standard hypotheses. Gender, age, previous higher education, or preference for future detective work were not related to the proportion of high-quality hypotheses.
The impact of individual differences on investigative hypothesis generation under time pressure (Kim, Alison & Christiansen, 2020)	n = 133 Korean detectives. (n = 66 under time pressure manipulation; n = 67 control group).	Used Time Paradigm 1.0 (Dougherty et al., 2003) to measure time-urgency. Raven's standard progressive matrices are used to evaluate fluid intelligence (Raven et al., 2003). NFC scale shortened version was used to measure NFC (Roets and Hiel, 2011). Experience is defined by the years of domain-specific experience in crime investigation.	Experimental design manipulating time pressure. Regression analyses.	Examine whether individual differences moderate the effect of time pressure on the number of hypotheses generated.	Under time pressure, experienced investigators generated hypotheses of higher quality but there was no significant effect on the number of hypotheses. High (vs low) NFC investigators generated significantly fewer hypotheses. Time-urgent investigators reduced the quantity and quality of hypotheses generated, while non-time-urgent investigator did not reduce their performance. Investigators with high (vs low) fluid intelligence had better performance in quantity and quality of hypotheses generated.

Demographic information differed across the included studies. The sample sizes varied from 14 to 166 participants, while there was one study, which did not allow to differentiate how many participants were considered (Alderden & Ullman, 2012). They analyzed 328 criminal sexual assault cases from police cases and investigatory files, but the same investigator could have been responsible for more than one case under analysis. The other eight studies, while delineating their participants, had different sampling methods according to the aims of their study. Some researchers used a sample of police officers and non-police officers (Ask & Granhag, 2005), others opted for varying degrees of experience among police officers (Dando & Ormerod, 2017; Fahsing & Ask, 2016; Wright, 2013), or a combination of both (Santtila et al., 2004), while some studies considered a homogeneous sample of police officers (Alison et al., 2013; Fahsing & Ask, 2017; Kim et al., 2020).

Demographic characteristics of the samples also varied according to country. A British sample was used, either completely or partially, in most of the studies (Alison et al., 2013; Dando & Ormerod, 2017; Fahsing & Ask, 2016; Wright, 2013), a Norwegian sample was used in two studies (Fahsing & Ask 2016; Fahsing & Ask, 2017) and each of the other four studies used samples from different countries: Finland (Santilla et al., 2004), Sweden (Ask & Granhad, 2005), USA (Alderden & Ullman, 2012) and South Korea (Kim et al., 2020). Most of the studies were conducted in European countries highlighting the need to expand research on the topic to other continents, particularly because different countries have different detective training.

Differences were also identified regarding the type of crime studied. Four different types of crimes were used to assess investigative decision making: Sex offenses (Alderden & Ullman, 2012; Alison et al., 2013; Kim et al., 2020), Homicide (Ask & Granhag, 2005; Wright, 2013); Missing person (Fahsing & Ask, 2016; 2017), Car theft (Santilla et al., 2004), and a single study used multiple crime types (Dando & Ormerod, 2017). Furthermore, sometimes researchers used real crimes as means to analyze decision making (Alderden & Ullman, 2012; Dando & Ormerod, 2017; Santilla et al., 2004; Wright, 2013), and sometimes they created a semi-fictitious case (Alison et al., 2013; Ask & Granhag, 2005; Fahsing & Ask, 2016; 2017; Kim et al., 2020).

Assessment of investigative decision making also varied across studies. Most of the studies considered either the number of investigative hypotheses generated, their

quality, or both (Alison et al., 2013; Dando & Ormerod, 2017; Fahsing & Ask, 2016; 2017; Kim et al., 2020; Wright, 2013). The other studies considered a specific decision made, such as whether two or more crimes were linked (Santilla et al., 2004), whether participants would acknowledge evidence contrary to their initial hypothesis (Ask & Granhag, 2005), or whether they decided to arrest a suspect (Alderden & Ullman, 2012).

It is interesting to note a shift in how investigative decision making has been studied, from a narrower perspective (a specific decision made in a specific scenario), to a broader one that considers other aspects of the investigation (generating multiple hypotheses), without missing on how accurate investigators are (quality of hypothesis). However, narrow studies are necessary to understand which variables influence important decisions in the course of an investigation, such as when to arrest someone, when to interview a suspect, which forensic experts to consult with, etc.

Eight different individual factors were analyzed by the studies included in the present review: Age, Experience, Fluid Intelligence, Gender, Inductive and Deductive Reasoning, Need for Cognitive Closure, Previous Higher Education and Time-Urgency. The experience was the most investigated individual factor as seven papers analyzed it. On the other hand, Age, Inductive and Deductive Reasoning, and Previous Higher Education were only analyzed in one study (Fahsing & Ask, 2017), while every other individual factor was studied in two different papers.

The studies that considered Experience used different measurements to define or analyze it. Some of them compared only police officers with the general public (Ask & Granhag, 2005), others used officers' rank as the measure for experience (Wright, 2013), while most researchers considered experience in terms of years on the job (Alison et al., 2013; Dando & Ormerod, 2017; Fahsing & Ask, 2016; Kim et al., 2020; Santilla et al., 2004). This issue of variable measurement was not identified with the other individual factors given that they are either straightforward (e.g., age) or have been measured using reliable psychometric testing (e.g., NFC).

There is a high number of individual factors that have been found to influence decision making in different contexts. These factors could, in theory, also influence investigative decision making; however, only eight of them have been empirically tested. Relying on theory is not necessarily bad but follow-up testing of such theories must be conducted to validate or refute them. In a first look, it seems that not many individual factors have been tested concerning investigative decision making but

empirical research on the subject has only started in the past two decades and only nine studies have endeavored to test it. In addition, there has been an increasing number of publications on the topic, nearly half of the identified studies were published in the last five years. Therefore, it is expected, from this increased attention, that researchers will continue to test other individual factors as well as try to replicate studies to verify if the findings are consistent.

Out of the eight individual factors empirically tested, only five had a significant effect on investigative decision making: Experience, Gender, Need for Cognitive Closure (NFC), Time-urgency, and Fluid Intelligence. Experienced investigators who were constantly dealing with car crimes were more capable of identifying crimes that were committed by the same offender when compared to the general population (Santilla et al., 2004). Investigators with more years of experience generated significantly more investigative hypotheses than investigators with fewer years of experience. This has been found under a quasi-experimental design using semi-fictitious cases (Fahsing & Ask, 2016), and an analysis of real decisions made during investigations (Dando & Ormerod, 2017). Using ranks to determine expertise in a laboratory analysis using real cases, Wright (2013) also identified that experienced officers generated more hypotheses; however, the accuracy or quality of them was not significantly different across groups.

Under time pressure, less experienced officers produced hypotheses of lower quality, which did not happen with more experienced officers (Kim et al., 2020). However, the number of hypotheses generated was not moderated by experience under the same circumstances, that is, experienced investigators under time pressure generate the same number of hypotheses as those with less experience, but their hypotheses are of better quality (Alison et al., 2013; Kim et al., 2020). Even though most of the results point to either a positive or null effect over investigative decision making, experience may have detrimental effects. Ask and Granhag (2005) found those police officers were more likely to perceive someone as guilty when compared to the general population even when presented with potentially exonerating evidence (Ask & Granhag, 2005).

Gender was only analyzed in two papers. The first used a quasi-experimental design and a missing person case to analyze the gender of newly recruited students to become police officers and their investigative hypotheses (Fahsing & Ask, 2017). Results showed no relation between participants' gender and the quality of hypotheses

generated. The second study analyzed criminal cases to verify if gender influenced investigators' decision to arrest a suspect of sexual assault (Alderden & Ullman, 2012). Its results identified that female detectives were significantly less likely to arrest suspects of sexual assault, even after controlling for common situational variables that influence this decision.

The need for Cognitive Closure was assessed in two different papers. In the study by Ask & Granhag (2005), high (vs low) NFC individuals were less likely to acknowledge evidence contrary to their hypothesis of guilty over the suspect, while Kim et al. (2020) found that high (vs low) NFC participants generated significantly fewer hypotheses under time pressure. Therefore, high NFC influences investigative decision making by preventing investigators to keep an "open mind", consider and generate multiple hypotheses, and avoid confirmation bias.

Time-urgency and fluid intelligence were analyzed by the same two papers, which used a sample of investigators and manipulated time pressure to verify if individual differences moderate its effect over investigative decision making (combined sample of 209 investigators from the UK and South Korea). Findings from both individual factors were consistent across studies. In a sample of British investigators, time-urgent participants had a larger reduction in the number of hypotheses generated than non-time-urgent investigators, while individuals who scored high (vs low) on fluid intelligence measures generated more hypotheses (Alison et al., 2013). In a sample of South Korean investigators, time-urgent participants reduced quantity and quality of hypotheses generated, an effect not found on non-time-urgent individuals, while high (vs low) fluid intelligent participants had better performance both in terms of quantity and quality of hypotheses generated (Kim et al., 2020). Therefore, it has been found that time-urgency and fluid intelligence have opposing effects over investigative decision making. Time-urgent individuals and those who score lower on fluid intelligence assessments reduce their performance in both quantity and quality of hypotheses generated.

In summary, each factor had its effect on investigative decision making. Experience had mixed findings. Some studies found that more experienced investigators had more effective decision making, while others found an inverted or non-significant relationship. Gender was found to be significantly related to a specific decision in a specific context (decision to arrest on sexual assault cases). High (vs low) NFC investigators produced significantly fewer hypotheses and were more prone

to confirmation bias. Time-urgency also had similar effects; investigators who were time-urgent produced hypotheses in lower quantity and quality under time pressure. Similarly, fluid intelligence was also found to be significantly related to effective investigative decision making, as individuals with high fluid intelligence produced better quality and a greater number of hypotheses.

DISCUSSION

The present paper set to identify which individual factors have been empirically tested in relation to investigative decision making, and how these factors influence investigative decision making. Through a systematic review of the literature, nine scientific papers were identified, which revealed that eight individual factors have been empirically tested, five of which had a significant impact on investigative decision making.

Despite the low number of studies, nearly all of them analyzed if experience had any effect on investigative decision making. Scientific theory and research point to an uncertain relationship between experience and decision making. On one hand, it is expected that experts will perform better than novices because they have a much greater mental database with relevant information about the task at hand (Alison et al., 2013). On the other hand, the experience can lead professionals to consider fewer hypotheses, rely on heuristics, and be more susceptible to confirmation bias.

The present review, unsurprisingly, found mixed results for the effect of experience. Some studies found that it played an important role in improving decision making, while others did not. Interestingly, one of the studies that used samples from two different countries achieved different results regarding the role of experience in investigative decision making depending on the country (Fahsing & Ask, 2016). It identified that experienced British detectives generated more hypotheses than experienced Norwegian detectives, and their hypotheses were also of better quality. The authors argue that differences in training were responsible for these differences in performance, even though both samples had the similar number of years of experience.

Considering the current findings, it would be wrong to condemn experience as a promoter of bad investigative decision making. It is more likely that experienced

officers will perform better than novices. However, only experience is not sufficient in leading to expertise and better performance. Fahsing and Ask (2016) suggest that a nationwide qualification program for investigators, mandatory training on the generation of hypotheses, consistent training, and procedural guides may facilitate this experience to be well developed over the years. Thus, police forces should invest in consistently training their investigators, providing supervision and feedback throughout their careers to develop experienced professionals that will perform at the highest level even under external negative influences such as media or time pressure.

It should be noted that there is a major methodological inconsistency around the definition of experience used by each paper. Nearly every one of them used a different method for considering experience, which hampers the direct comparison across samples. It is unknown whether the results would be the same if a study used a different definition, for example, considering years of experience investigating homicides instead of officers' rank. Therefore, readers must keep in mind how researchers have defined experience in their paper, while researchers must carefully select, and make explicit, the independent variables of the study.

Research on gender differences and general decision making pointed to ambiguous expectations in relation to the effects of this individual factor on investigative decision making, given that males are less susceptible to biases and heuristics, but also more likely to make hasty judgments (Byrne & Worthy, 2016; Toplak et al., 2016; Weller et al., 2018). The findings from both studies that analyzed gender do not provide an answer as to whether male or female detectives would have better investigative decision making. The only study that found a significant relationship between gender and investigative decision making did not investigate if female detectives also kept an "open mind" if they followed a confirmation bias, or even if the arrested suspect was guilty (Alderden & Ullman, 2012). Therefore, gender seems to have different effects on investigative decision making depending on the type of crime and context, but further research is needed to verify the replicability of and expand such findings.

Need for Cognitive Closure (NFC) was another salient individual factor identified in the present review to influence investigative decision making. Research on decision making has already identified that high NFC consumers used much faster decision making strategies, which relied on a small number of characteristics, while low NFC consumers took longer and analyzed more information to conclude (Choi et al., 2008).

In clinical settings, NFC has also been related to suboptimal information searching and decision making. Raglan et al. (2014) found that high NFC obstetricians/gynecologists often asked fewer screening questions about certain conditions, indicating that they could have searched further for treatable diseases. The results of the present systematic review corroborate this understanding. Even though NFC was only analyzed in two separate studies, both identified a negative relationship between NFC and effective investigative decision making.

One of the studies found that high NFC investigators had difficulty in modifying their perception of guilty even when presented with confronting evidence (Ask & Granhag, 2005), while the other study found that high NFC investigators generated fewer hypotheses under time pressure (Kim et al., 2020). As already pointed out, both of these outcomes can have devastating effects in the form of tunnel vision and miscarriages of justice. However, knowledge of this relation is quite beneficial because NFC can be reliably measured through the Need for Cognitive Closure Scale (NFCS), which has been validated in many countries (Kruglanski et al., 1993; Kossowska, Van Hiel, Chun & Kruglanski, 2002). Both studies under analysis used this scale, either in its full or shortened version (Roets & Hiel, 2011). Therefore, police forces should consider using the NFCS to recruit and select potential investigating officers, as well as identifying which officers require further training to prevent them from falling into the cognitive trap of need for closure.

There are different sources of pressure in the course of a criminal investigation, while some of them are occasional, such as media pressure in high profile cases, others are more frequent, which is the case of time pressure. There is never-ending pressure on investigating officers to solve crimes, when they solve one there are many others that need to be solved. The effects of time pressure may be moderated by how investigators perceive the passage of time, which is subjective, that is, there are individual differences in how people perceive the passage of time (Wittmann & Paulus, 2008). Time-urgent individuals feel time pressure much more overwhelmingly, regardless of the amount of time available.

Both studies that analyzed time perception and investigative decision making arrived at similar conclusions: time-urgent individuals had a significant loss in terms of quantity and quality of hypotheses generated under time pressure (Alison et al., 2013; Kim et al., 2020). In practical terms, when under pressure to quickly solve a case, some investigators may have worse performance due to their subjective

perception of time. Therefore, identifying time-urgent investigators and developing strategies to help them cope with this pressure without underperforming will likely lead to better investigative decision making and subsequent judicial process.

Finally, the last individual factor identified to lead to effective investigative decision making is fluid intelligence. In the present review, both papers that analyzed time-urgency also assessed fluid intelligence (Alison et al., 2013; Kim et al., 2020). They achieved similar results: investigators with high fluid intelligence generated more hypotheses and hypotheses of better quality when compared to those with low fluid intelligence. Criminal investigations are almost exclusively novel, each new case demands new investigative actions and, even though there are similarities among cases, it cannot be assumed that there are two identical crimes. Even homicide investigators with 20 years of experience on the job can find themselves dealing with new challenging cases daily, which requires them to adapt and direct the investigation accordingly.

In light of the novelty of criminal investigation, it would be important that investigators have the cognitive ability (high fluid intelligence) to adapt to each new case while maintaining high job performance. Like NFC, there is a reliable way, used by both studies, to measure fluid intelligence using Raven's standard progressive matrices (Raven, Court, & Raven, 1977). Therefore, police forces can measure their officers' fluid intelligence and identify who is best suited for investigative positions, who is more likely to achieve better results in novel cases, as well as who needs the training to develop fluid intelligence abilities.

While non-significant statistical results are not easily accepted by the scientific community in general, even leading to diminished chances of publication, they are a relevant source of data (Siddaway et al., 2019). In this particular context, understanding which factors are unrelated to investigative decision making can facilitate and direct the training and selection of future detectives. Considering that Age, Inductive and Deductive Reasoning, and Previous Higher Education were not shown to influence the quality of investigative hypotheses (Fahsing & Ask, 2017), police forces may want to reconsider minimum age, specific higher education requirements, or the use of psychological assessment of inductive and deductive reasoning to determine acceptance into police training.

Although researchers must select one or a couple of individual factors to analyze due to feasibility issues, all factors are simultaneously present when investigators make decisions. However, no research was identified that considered how multiple

individual factors interact with one another, and how this combination of factors can influence investigative decision making. Considering the main issues of a criminal investigation and circumstances that lead to miscarriages of justice, a combination of these individual factors may help prevent them.

LIMITATIONS

This systematic review was not without its limitations. First, the small number of studies identified and differences in methodology did not allow for a more comprehensive comparison among results. The biggest issue regards how investigative decision making was measured, some studies considered it in the form of hypotheses generation and their quality, while others focused on a more specific decision to be made (e.g., whether two crimes are linked). These issues, coupled with the small sample sizes, hinder result generalization. Furthermore, included studies consisted of only those that were published in peer-reviewed scientific journals, which makes the systematic review vulnerable to publication bias considering that non-significant findings are often rejected for publication. Finally, only studies published in English were considered, consequently, some papers on the subject may not have been included.

Implications for practice and policy

Because of the individual factors found to be related to effective investigative decision making, some actions can be taken to improve criminal investigations. Police forces should use reliable psychological tests (Need for Cognitive Closure Scale and Raven's standard progressive matrices) to recruit and select prospective candidates to become investigators. In addition, currently employed investigators could also be tested on these factors not to promote a working environment that excludes these officers, but to develop training programs designed specifically to build on these abilities. Finally, police forces around the world would benefit from developing a nationwide qualification program for investigators that includes training on generating hypotheses, while also developing procedural guides and frequently conducting refresher training courses to ensure that expertise is built on top of the experience.

Future research

At the academic level, there is still much to be understood about the individual factors relevant for investigative decision making. More research is needed to evaluate the effects of individual factors over investigative decision making in different types of crimes, samples from other backgrounds and nationalities may also lead to varying results due to differences in training and investigative practices. Developing more empirical evidence is necessary to replicate findings, identify other relevant individual factors and provide much more robust evidence to support the training and recruiting of investigators throughout the world.

Other factors that would be relevant to analyze are personality traits, such as those from the Big Five Model of Personality. Conscientiousness, for example, refers to how people regulate their impulses when engaging in goal-directed behavior, so it may influence how thorough investigators are in considering all possible hypotheses. Cognitive abilities such as crystallized intelligence may also be of relevance, especially considering that investigators attempt to solve problems (crimes) using learned knowledge from training and courses. Critical thinking has also been highlighted as a necessary skill for effective investigative decision making, given that it would allow investigators to be more aware of potential biases and avoid them, but no published studies testing the relation between the two variables were identified (Turvey, 2011). On top of that, future research should endeavor to analyze how multiple individual factors interact with each other to influence investigative decision making

Conclusion

Five individual factors were found to be relevant for effective investigative decision making: Experience, Gender, NFC, Time-urgency, and Fluid Intelligence. Even though these factors are not sufficient to ensure that a criminal investigation is conducted thoroughly and that mistakes or miscarriages of justice will never occur, they are mitigating factors. These factors are linked to investigators considering a wider variety of hypotheses for each investigation, which will reduce confirmation bias and tunnel vision. They are also likely to lead to crimes being more quickly solved, since they are linked to better hypotheses. Understanding how individual factors play a role in the outcome of criminal investigations will serve to guide police forces' recruitment and training programs.

References

Alderden, M. A., & Ullman, S. E. (2011). Gender Difference or Indifference? Detective Decision Making in Sexual Assault Cases. Journal of Interpersonal Violence, 27(1), 3–22. doi:10.1177/0886260511416465

Ali, S., & Ara, A. (2017). Intelligence as a determinant of academic achievement: A comparative study of high achievers and underachievers. International Journal of Humanities and Social Sciences (IJHSS), 6(6), 79-88.

Alison, L., Doran, B., Long, M. L., Power, N., & Humphrey, A. (2013). The effects of subjective time pressure and individual differences on hypotheses generation and action prioritization in police investigations. Journal of Experimental Psychology: Applied, 19(1), 83-93.

Ask, K., & Alison, L. (2010). Investigators' decision making. In P.A. Granhag (Ed.), Forensic psychology in context: Nordic and International Approaches (pp. 35-55). New York: Willan Publishing.

Ask, K., & Fahsing, I. A. (2018). Investigative decision making. In A. A. Griffiths & R. Milne (Eds.), The psychology of criminal investigation (pp. 52-73). London: Routledge.

Ask, K., & Granhag, P. A. (2005). Motivational sources of confirmation bias in criminal investigations: the need for cognitive closure. Journal of Investigative Psychology and Offender Profiling, 2(1), 43–63.

Bendor, J. B., Kumar, S., & Siegel, D. A. (2009). Satisficing: A "Pretty Good" Heuristic. The B.E. Journal of Theoretical Economics, 9(1), 1-36.

Byrne, K. A., & Worthy, D. A. (2016). Toward a mechanistic account of gender differences in reward-based decision making. Journal of Neuroscience, Psychology, and Economics, 9(3–4), 157–168. https://doi.org/10.1037/npe0000059

Choi, J. A., Koo, M., Choi, I., & Auh, S. (2008). Need for cognitive closure and information search strategy. Psychology and Marketing, 25(11), 1027–1042.

Colom, R., Escorial, S., Shih, P. C., & Privado, J. (2007). Fluid intelligence, memory span, and temperament difficulties predict academic performance of young adolescents. Personality and Individual Differences, 42(8), 1503–1514.

Conte, J. M., Mathieu, J. E., & Landy, F. J. (1998). The nomological and predictive validity of time urgency. Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 19(1), 1-13.

Crego, J., & Alison, L. (2004). 'Control and legacy as functions of perceived criticality in major incidents', *Journal of Investigative Psychology and Offender Profiling*, 1: 207–25.

Dando, C. J., & Ormerod, T. C. (2017). Analyzing Decision Logs to Understand

Decision Making in Serious Crime Investigations. Human Factors: The Journal of the Human Factors and Ergonomics Society, 59(8), 1188–1203.

Fahsing, I., & Ask, K. (2016). The making of an expert detective: the role of experience in English and Norwegian police officers' investigative decision making. Psychology, Crime & Law, 22(3), 203–223.

Fahsing, I. A., & Ask, K. (2017). In Search of Indicators of Detective Aptitude: Police Recruits' Logical Reasoning and Ability to Generate Investigative Hypotheses. Journal of Police and Criminal Psychology, 33(1), 21–34.

Kim, S., Alison, L., & Christiansen, P. (2020). The impact of individual differences on investigative hypothesis generation under time pressure. International Journal of Police Science & Management, 146135572090571.

Klein, G. A. (1993). A recognition-primed decision (RPD) model of rapid decision making. *Decision making in action: Models and methods*, 5(4), 138-147.

Kokkinakis, A.V., Cowling, P.I., Drachen, A. & Wade, A.R. (2017). Exploring the relationship between video game expertise and fluid intelligence. PLoS ONE, 12(11): e0186621.

Kossowska, M., Van Hiel, A., Chun, W.Y., & Kruglanski, A.W. (2002). The Need for Cognitive Closure Scale: Structure, Cross-Cultural Invariance, and Comparison of Mean Ratings between European-American and East Asian Samples. *Psychologica Belgica*, 42(4), pp.267–286. DOI: http://doi.org/10.5334/pb.998

Kruglanski, AW. (1990). Motivations for judging and knowing: Implications for causal attribution. In: E.T. Higgins and R.M. Sorrentino (Ed.), The handbook of motivation and cognition: Foundation of social behavior. Vol. 2. (pp. 333-368) New York: Guilford Press.

Kruglanski, A. W., Webster, D. M., & Klem, A. (1993). Motivated resistance and openness to persuasion in the presence or absence of prior information. Journal of Personality and Social Psychology, 65(5), 861-876.

Lepard, D. A., & Campbell, E. (2009). How police departments can reduce the risk of wrongful convictions. In D. K. Rossmo (Ed.), Criminal investigative failures (pp. 269-293). Boca Raton: CRC Press.

McGrew, K. S. (2009). CHC theory and the human cognitive abilities project: Standing on the shoulders of the giants of psychometric intelligence research. Intelligence, 37(1), 1–10.

McLaughlin, K., Eva, K.W. & Norman, G.R. (2014). Reexamining our bias against heuristics. Adv in Health Sci Educ, 19, 457–464.

Primi, R. (2003). Inteligência: Avanços nos modelos teóricos e nos instrumentos de medida. Avaliação Psicológica, 2(1), 67- 77.

Raglan, G. B., Babush, M., Farrow, V. A., Kruglanski, A. W., & Schulkin, J. (2014). Need to know: the need for cognitive closure impacts the clinical practice of obstetrician/gynecologists. BMC Medical Informatics and Decision Making, 14(1).

Raven, J. C., Court, J. H., & Raven, J. (1977). *Standard progressive matrices*. London, UK: Lewis

Roets, A., & Van Hiel, A. (2011). Item selection and validation of a brief, 15-item version of the Need for Closure Scale. Personality and Individual Differences, 50(1), 90–94.

Rossmo, D. K. (ed.) (2009) *Criminal Investigative Failures*. Boca Raton: CRC Press.

Rossmo, K. & Pollock, J. (2019). Confirmation Bias and Other Systemic Causes of Wrongful Convictions: A Sentinel Events Perspective. Northeastern University Law Review, 11(2), 790-835.

Santtila, P., Korpela, S., & Häkkänen, H. (2004). Expertise and decision making in the linking of car crime series. Psychology, Crime & Law, 10(2), 97–112.

Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to do a systematic review: a best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. Annual review of psychology, 70, 747-770.

Simon, D. (2012). In doubt: The psychology of the criminal justice process. Harvard, UK: Harvard University Press.

Snook, B. & Cullen, R. M., (2009). Bounded rationality and criminal investigations: Has tunnel vision been wrongfully convicted? In K. D. Rossmo (Ed.), Criminal investigative failures (pp. 69-96). Oxford, UK: Taylor & Francis

Spanoudaki, E., Ioannou, M., Synnott, J., Tzani-Pepelasi, C. and Pylarinou, N.R. (2019), Investigative decision making: interviews with detectives. Journal of Criminal Psychology, 9(2), 88-107.

Stolper, E., Van de Wiel, M., Van Royen, P., Van Bokhoven, M., Van der Weijden, T., & Jan Dinant, G. (2011). Gut feelings as a third track in general practitioners' diagnostic reasoning. Journal of General Internal Medicine, 26, 197–203.

Toplak, M. E., West, R. F., & Stanovich, K. E. (2016). Real-World Correlates of Performance on Heuristics and Biases Tasks in a Community Sample. Journal of Behavioral Decision Making, 30(2), 541–554. doi:10.1002/bdm.1973

Tschentscher, N., Mitchell, D., & Duncan, J. (2017). Fluid Intelligence Predicts Novel Rule Implementation in a Distributed Frontoparietal Control Network. The Journal of Neuroscience, 37(18), 4841–4847.

Turvey, B. (2011) Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 4th Ed. London, UK: Elsevier Science

Weller, J., Ceschi, A., Hirsch, L., Sartori, R., & Costantini, A. (2018). Accounting for Individual Differences in Decision Making Competence: Personality and Gender Differences. Frontiers in Psychology, 9. doi:10.3389/fpsyg.2018.02258

Wittmann, M., & Paulus, M. P. (2008). Decision making, impulsivity and time perception. Trends in Cognitive Sciences, 12(1), 7–12.

Wright, M. (2013). Homicide Detectives' Intuition. Journal of Investigative Psychology and Offender Profiling, 10(2), 182–199.

"Let's Not Go for That One!" Burglars' Perceptions of Alarms as Deterrents

*Seungmug (Zech) Lee**
PhD, Associate Professor
Department of Criminology and Criminal Justice
The University of Texas at Arlington

Abstract

Burglar alarms have been protecting residences and buildings for over 150 years. For most of this time, their utility in reducing the incidence of burglary has been based on anecdotal and intuitive notions. In recent decades researchers have established qualitative bases for the utility of residential alarms in the reduction of incidents in the United States. Camera systems have arrived more recently as anti-burglary protective measures. This study examines perceptions on the deterrence impact of alarms and other burglary-deterrent measures from 242 convicted burglars serving time in four Ohio prisons. The findings show that evidence of a residential burglar alarm, outdoor cameras, or surveillance equipment are powerful deterrent factors in the decision process of most actors.

Keywords

alarms; camera systems; burglary; crime mitigation

* Direct correspondence to Seungmug (Zech) Lee, Associate Professor at the University of Texas at Arlington; seungmug.lee@uta.edu
* http://dx.doi.org/10.36889/IJCJ.2021.009
* Received 11 November 2021; Revised 10 December 2021; Accepted 21 December 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 68-94

INTRODUCTION

Security is an indisputable necessity for human progress. We define security as the protection of assets from loss (McCrie, 2004) and without it, the safeness of people, possessions, freedom, and progress itself eventually will fail. Protection is advanced through many factors including the use of alarms. From times immemorial animals and human signaling cued the arrival or presence of unknown persons. In modern times mechanical and electronic alarms have contributed to the protection of people, commerce and industry, institutions, and government (Greer, 1991; McCrie, 2006; McCrie & Lee, 2023). In recent times cameras have been added to the residential armamentarium. This study primarily focuses on how alarms impact the to-burglar or not-to-burglar calculation of criminal risk-takers.

The first patent for alarm systems advanced by electro-mechanic technology in the U.S. was granted to Augustus R. Pope in 1853, in Somerville, Massachusetts, a Boston suburb. Pope's electronic alarm would sound a constant tone if a door or window were forced open without authorization. But five years later, without producing a commercial prototype, the patent was sold to Edwin Holmes of Boston, who saw the commercial possibilities of the protective system. Holmes moved his enterprise to New York City to further develop the system where signaling cable could be installed along with conduits for telephoning. By the early 20th century, the Holmes Burglar Alarm Company – and plenty of other alarm services businesses – were thriving across the nation for a growing commercial and industrial customer base (Greer, 1979; McCrie, 2004; Tilley et al., 2015). The large alarm companies concentrated on commercial, industrial, and government business: that was to change. Residential alarms could also include a visual component. During the urban crime rise starting in the 1960s, Marie Van Brittan Brown patented an electronic home security system that preceded the familiar door cameras of today. While the Brown patent of 1969 was never developed commercially, it has been cited in 35 U.S. patents since (Hilgers, 2021).

Despite the ubiquitous use of alarm systems in residential and commercial settings, research work on this topic has lacked quantitative analysis for most of its history (Cedar Rapids Police Department, 1971; Lee, 2008). Traditionally, alarm systems – also called burglar alarms – have been chosen to deter, detect, and induce a

response to burglary alarm conditions at residences, commercial settings, institutions, and government structures (Blackstone et al., 2020; Lee, 2008; Roth & Roberts, 2017). Separately, studies focusing on car alarms have also been published (Farrell & Brown, 2016; Farrell, Tilley, & Tseloni, 2014).

Residential burglar alarms are considered as a physical target-hardening protective measure to detect, deter, prevent, and signal the presence of burglars or the attempt of breaking into properties (Cedar Rapids Police Department, 1971; Clarke, 1997, 2002; Farrell et al., 2014; Hakim & Shachmurove, 1996; Scarr, 1973; Tseloni, 2014; Winchester & Jackson, 1982). Most of the previous research studies examined the impact of alarm systems on crime reduction, typically focusing on the overall burglaries, but not on the net effect of alarm systems. Those studies report that alarm systems produce a deterrent effect. The point of view of burglars themselves from those studies offers an insightful way of understanding the nuances of protection and strengthening security systems. Such studies that have been published indicate that the presence of alarm systems is not the sole factor in burglary target determination and that further research inquiries would be salutary (Clarke, 2002; Lee, 2008; Nee et al., 2019; Roth et al., 2018; Scarr, 1973; Vandeviver & Bernasco, 2020). However, most of the studies appear to focus on burglaries, but not on burglar alarm systems, which means alarm systems were considered as part of other home protection measures. The net impact of alarm systems on burglary reduction is rarely examined. The current study evaluates aspects of residential burglar alarms as a primary physical target-hardening protective measure to detect and deter burglaries.

LITERATURE REVIEW

Reactions to Burglaries

Lively research since the early 1970s has deepened understandings of burglars and their craft. General aspects of burglaries (Scarr, 1973; Shover, 1972) initially appeared, while studies during the 1980s and 1990s tended to focus on both general and specific aspects of burglars and burglaries with different research methodologies (Bennett & Wright, 1984; Buck et al., 1993; Cromwell & Olson, 2004; Hakim & Buck, 1991; Maguire & Bennett, 1982; Mawby, 2001; Nee & Taylor, 1988; Wright & Decker, 1994). More recent works continue to explore aspects of burglars and efforts

to deter and mitigate them (Lee, 2008; Roth, 2017; Roth & Roberts, 2018; Rothstein, 2020).

We know that certain factors influence a property owner or manager's decision to take multiple protective measures to protect their properties (Roth et al., 2018; Tilley et al., 2015). One deterrent measure is never enough. These protective modalities can be separated into two categories—behavioral precautions and physical security applications—which relate to the level of fear of crime and available burglary-resistance resources. Behavioral precautions take the form of constrained or avoidance behaviors or passive steps actions (e.g., leaving a radio on, keeping doors locked in the daytime, staying away from certain areas, and remaining inside after dark), while physical security includes a variety of precautions for home protection [e.g., keeping lights on, locking doors at night, having a dog, strengthening doors and their hardware, securing windows, installing an alarm system, closed-circuit television systems, and (more recently) carrying a cell phone connected to an alarm monitoring system that will alert the homeowner to a call at the door or an untoward event.]

Most studies report that physical security measures produce a sizeable positive effect to reduce the chance of burglary victimization (Bennett & Wright, 1984; Coupe & Blake, 2006; Cromwell & Olson, 2004; Hakim et al., 2001; MacDonald & Gifford, 1989; Roth, 2017; Roth & Roberts, 2017; Scarr, 1973), with a few exceptions; for example, with a dog's presence, there is no relationship with burglary victimization (Buck et al., 1993) or even higher burglary rates (Tseloni et al., 2004). But those exceptions seem to be inconsistent in different settings and circumstances.

Alarm systems remain a widely-adopted option to deter burglary victimization as a form of physical security at both residential and non-residential settings (Clarke, 1997, 2002; Farrell et al., 2014; Lee, 2008; McCrie, 2004, 2006; Rothstein, 2020; Scarr, 1973). A market research firm estimates that revenues for life safety and intrusion alarms in the United States reached $4.5 billion in 2019, the largest component for external security expenditures following contract security guard services (Freedonia Group, 2020).

Burglar Alarms as a Target-Hardening Adoption

Burglar alarms can be considered like occupancy proxies (e.g., dogs); that is, they are "non-human factors that substitute for residents by drawing attention to intruders" (Roth & Roberts, 2017, p. 126), rather than a solo, stand-along protective measure at

both residential and non-residential settings (e.g., commercial establishments, school properties, government buildings, churches, museums, etc.) (Bennett & Wright, 1984; Clarke, 2002; Mawby, 2002; Rothstein, 2020; Scarr, 1973). As noted earlier, burglar alarms have been considered crime prevention resources, together with other target-hardening adoptions in various research works employing different data sources (Bennett & Wright, 1984; Hakim et al., 2001; Hearnden & Magill, 2004; Lee, 2008; Maguire & Bennett, 1982; Nee & Meenaghan, 2006; Roth, 2017; Rubenstein et al., 1980; Wright & Decker, 1994).

However, burglars are not equally deterred by all target-hardening measures (Crowell & Olson, 2004; Wright & Decker, 1994). For example, the presence of dogs mostly produces a positive impact against burglaries (Bennett & Wright, 1984; Cromwell & Olson, 2004; Hakim et al., 2001; MacDonald & Gifford, 1989; Roth & Roberts, 2017; Wright & Decker, 1994), but a few counter-effects are reported as well (Buck et al., 1993; Tseloni et al. 2004). External lights and double locks on doors produce a deterrence (Tilley et al., 2015; Tseloni et al., 2017).

Regarding burglar alarms, empirical studies present a strong case that alarm systems are an effective mechanism for detecting and preventing burglaries (Cedar Rapids Police Department, 1971; Clarke, 1997; McCrie, 2006). The earlier studies in the 1970s and 1980s show that, though not many residences had alarms installed at those times, those with burglar alarms were less likely to be victimized and that burglars in the planning stages of their crimes ascertain whether an alarm is installed or not (Conklin & Bittner, 1973; Reppetto, 1974; Rubenstein et al., 1980; Scarr, 1973). Burglars themselves also generally reveal that they check whether alarms are in place among targeted properties before deciding to commit break-ins/burglaries and that, when encountered, they mostly try to bypass those once-considered-targeted properties (Bennett & Wright, 1984; Blackstone et al., 2020; Buck et al., 1993; Cromwell & Olson, 2006; Maguire & Bennett, 1982; Roth, 2017; Wright et al., 1995). Regardless, some professional and/or experienced burglars attempt to disable alarms or quickly complete burglaries before police respond (Clarke, 2002; Coupe & Kaur, 2005; Cromwell & Olson, 2004; Nee & Meenaghan, 2006; Roth et al., 2018; Wright & Decker, 1994).

Therefore, an alarm is an unfavorable factor in positive target selection (Bennett & Wright, 1984), and maybe regarded as a definite deterrent (Cromwell et al., 1991; Hakim et al., 1998), as well as a device to delay an attempt to enter an intended target

(Wright & Decker, 1994). Surveys in communities, including homeowners who were victims of burglaries, established the value of alarm systems in homes and businesses (Hakim, 1995; Hakim & Buck, 1991; Hakim, Rengert, & Shachmurove, 2001; Hakim & Shachmurove, 1996a, 1996b). Overall, their studies show that burglar alarms produce a net benefit and relate to lower odds of burglary victimization. For example, homes without alarms systems are, on average, 2.71 times, and commercial properties are 4.57 times at greater risk of being burgled than homes and businesses with an alarm installed. It is these less protected targets that burglars go for. Audible alarms cause burglars to escape before entry. Of all incomplete burglaries, 74.3% are thwarted by sirens or bells. In addition, the average value of property stolen from homes in which alarms are installed is 74% of that removed from homes without alarms. This indicates that burglars, though successful in breaking into properties, have less time available to commit burglaries at homes with alarms operating. Further, using mapping analysis, Lee (2008) established that the existence of burglar alarms reduces burglaries without displacing burglaries to nearby homes. Neighborhoods with a high density of alarm installations experience fewer burglary incidents occurred.

But British victimization surveys report a counter-intuitive finding that alarm ownership has no effect there and increased burglary risk, depending on other home security measures in place (Tilley et al., 2015; Tseloni et al., 2015). Nevertheless, most studies listed in the previous sections support the positive deterrent effect of burglar alarms.

Distinctive Methodologies with Analogous Findings

Over the last five decades, burglary, in general, has been a subject of research projects, and in particular burglar alarms have also been analyzed as a significant variable for enhanced property protection. Researchers have used distinctive methodologies for data collections and analyses to establish their findings but, by and large, reached similar conclusions that burglar alarms can be an effective burglary deterrent (Tilley et al., 2015).

One methodology to study burglary pursued here is to interview burglars at either correctional facilities or in post-release centers in their neighborhoods. The majority of the convicted burglars in studies by Maguire and Bennett (1982) (N = 40), Bennett and Wright (1984) (N = 300), and Nee and Taylor (1988) (N = 50) responded that they

would avoid homes with alarms installed and that an alarm would have deterred them from their most recent offense. Studies with videotapes and photographs shown to incarcerated burglars by Bennett and Wright (1984) (N = 40), Wright et al. (1995) (N = 47), and Roth and Roberts (2017) (N = 52) found that an alarm could be an unfavorable factor in target selection for burglary and that most burglars are deterred by alarms.

Some earlier studies used a secondary data source, mostly from police incident records. Conklin and Bittner (1973), Scarr (1973), Reppetto (1974), LeBeau and Vincent (1997), and Lee (2008) report that, generally, houses with alarms installed are less likely to be burgled and that, therefore, a burglar alarm can be selected as a means of preventing a burglary or reducing its costly impact.

Ethnographic studies, using mostly a snowball sampling technique common in the 1990s, focused on burglars' perspectives in understanding various aspects of burglaries and environmental or situational factors. These confirm previous research findings that burglar alarms are a deterrent and that burglars avoid houses with an alarm installed (Buck & Hakim, 1993; Cromwell & Olson, 2004; 2006, N = 30; Hearnden & Magill, 2004, N = 82; Wright & Decker, 1994, N = 105; Wright, Logie, & Decker, 1995, N = 47). Victimization surveys (Buck et al., 1993; Hakim et al., 2001; Miethe & Meier, 1990) also find that alarms are associated with a reduced risk of burglary.

Perhaps the most interesting research method is to apply an experimental design to test the true effect of alarm systems on burglaries or other crimes. Unlike other well-suited research designs (e.g., inmate interviews, surveys, ethnographical observations, video clips, and photographic showings, and secondary data sources), the experimental and even quasi-experimental research methods are rare in this subject area (Lee, 2008). The only notable experimental study was conducted by the Cedar Rapids Police Department (1971), a landmark research endeavor. Matched pairs of over 100 schools and businesses with previous burglary experience were selected in which one of the pairs in each case is given an alarm system that sounds directly at the police station. The other half remained as the control group. In the experimental endeavor, the findings are substantial in several aspects that: (1) burglar alarms had the effect of significantly reducing attempted offenses with about 55% in burglaries of business places as compared to only 8% for the control group; (2) arrests at the scene were significantly higher (31%) for sites with alarms, while only 6% of the cases in

the control group; (3) clearance rates were also higher for locations with alarms with 46% as compared to 27% for the control group and 31% citywide; and finally (4) schools with alarms installed experienced reduction in burglaries (75%), while less than a 25% reduction occurred among the schools in the control group (Cedar Rapids Police Department, 1971).

Another approach applying a quasi-experimental research design was conducted by Lee (2008) with the concepts of WDQ (weighted displacement quotient) and three nested concentric zones and GIS (geographic information system) mapping techniques, which makes possible a construct for three zones—the target zone with the houses where alarms are installed, a buffer zone next to the target zone, and a control zone next to the buffer zone. Such an approach to test the impact of alarm systems on residential burglaries employs a combination of a quasi-experimental research design, secondary data sources (e.g., police incident records, census data, and alarm permit records), and mapping analyses. The study presents a burglar alarm as a system used to detect the entry or attempted entry of an intruder into protected premises and to signal the detection to others, either locally or remotely. This demonstrates that a negative relationship exists between the presence of a hot spot for burglaries and the presence of a hot spot for alarm installation. It further establishes that the existence of burglar alarms reduces burglaries without displacing them to nearby homes (i.e., no spatial displacement is observed). Neighborhoods or street blocks with high residential alarm density experience fewer burglaries.

Key Issues over the Effectiveness of Burglar Alarms

Several important points should be assessed in determining the deterrent effect of alarms on burglaries. The first relates to the state of knowledge over the net effect of alarm system deterrence. Only in recent years have alarm systems received academic attention as part of burglars/burglaries studies and crime prevention evaluations combined with other security measures (e.g., dogs, window locks, door locks, and indoor and outdoor lighting). Different research methods (e.g., inmate/victim/household surveys, police data analyses, ethnographic studies with snowball sampling, observational studies, in-depth interviews, and experimental studies) are also used to examine the effect of protective security measures. But still too little is known of the net impact of alarm systems as a deterrent on burglaries mainly because of the dearth of independent assessments and experimental research endeavors. Other topics like

target selection or the motivation to commit burglaries have become major research topics and have reached criminology's first paradigm (Felson, 2017). Too few studies have demonstrated that alarm systems function as a strong deterrent against burglaries; even fewer consider the impact of camera systems.

Second, unlike most previous studies, a report based on British Crime Survey data suggests that alarm ownership has no effect or increases the risk of burglary victimization, depending on other home security measures (Tilley et al., 2015). This becomes Sherman et al.'s (2017) conclusion that evidence is still lacking using a five-point scale on what works best in mitigating residential burglary. This conclusion is based on just a few studies (conducted by the same researchers), in which the findings and arguments are provocative and call for further research endeavors while not negating findings from the Cedar Rapids Police Department.

Third, the positive effect of alarms in the prevention and control of burglaries can be offset by the high volume of false alarm activations (Blackstone, et al., 2020; LeBeau & Vincent, 1997; Rothstein, 2020; Tilley et al., 2015). Rates of false alarms are reported as high as 90% to 98%, and the factors that cause such high rates include faulty equipment, poor installation, and human errors or negligence (e.g., incorrect inputting keypad codes, roaming pets, helium balloons, or insects) (Blackstone et al., 2020; Hakim, 2001; LeBeau & Vincent, 1997; Sampson, 2011). This problem relates to a variety of negative consequences that can offset the net effect of alarm systems (e.g., withdrawal of prompt police response, increased fines for false alarms, or negative image of alarms by the public). Despite the problem of false alarms, burglar alarms remain established as a deterrent to a residential burglary.

Fourth, the issue of methodological approach is worth noting that, though assorted research methods as listed above have been used to assess the effectiveness of alarm systems on burglaries, causal experimental or quasi-experimental designs and new analytical tools should be selected to comprehend the net deterrent impact of burglar alarms like an experimental research design combined with mapping techniques (Lee, 2008). This study revisits the first issue; it endeavors to deepen an understanding of alarms' deterrent effectiveness independently from other security measures according to convicted burglars' perspectives of alarms and other deterrent measures.

METHODS

Survey Procedure

The research design for this study used a questionnaire survey focusing on burglars, discussing their crimes and implications for crime prevention. The researcher commenced by conducting an in-depth face-to-face interview with one convicted inmate at an Ohio state prison. After this interview, the researcher developed a survey questionnaire for the current study for use with a larger sample of convicted burglars incarcerated at Ohio state prisons. Among a total of 560 inmates (male = 440 and female = 120) who were convicted for burglaries, 242 usable surveys were collected for the current study in 2012. The return used rate of 43.2% is an average percent of what many prison studies produce (Gaes & Goldberg, 2004; Hensleyet al., 2000). All inmates were randomly selected from the initial sampling frame; the researcher visited the four prisons to administer and collect the surveys. The sampling frame of the potential inmates for data collection was incarcerated persons convicted for aggravated burglaries (including attempted aggravated burglary) and burglaries (including attempts), who were serving time among these prisons at the time of the survey.

The questionnaire employed a paper-pencil format. The initial questionnaire used for data collection covered various topics of criminal behaviors and crime prevention from the burglars' perspectives, including the effectiveness of various security measures (e.g., dogs, lights, locks, and alarms), burglars' decision-making processes (e.g., decision to commit crimes, target selection, method of entry, and items taken), and characteristics of burglaries (e.g., temporal classifications, co-offending pattern, and drug use). Of 70 questions in the survey, 13 related to alarm systems.

Research Questions and Variables

The current study examines the effectiveness of alarm systems on burglaries, in particular, focusing on the direct and net impact of alarms on the crime reduction aspect. Thus, three main research questions are as follows: (1) are burglar alarm systems a favorable/unfavorable factor among the convicted burglars in the course of target selection; (2) do burglar alarms produce a direct/net benefit in deterring burglaries; and (3) what is the contextual impact of burglar alarms on burglaries with

other home protection measures (e.g., dogs, cameras, and locks)?

Questions relating to burglar alarms in the survey are divided into three categories: contextual effect, direct effect, and handling attitude. The contextual effect of alarms on burglaries is measured alongside other security applications (e.g., the presence of a dog, cars in the driveway, types of doors and windows, and visible outdoor cameras), by two variables—types of items that burglars are concerned about when deciding whether to enter the target place and any peculiar physical feature to block burglars from proceeding to enter the premises.

The direct effect of alarms on burglaries is measured on four variables—target selection (dichotomous response—*yes, no*), frequency of alarm observation (three-scale response—*always, sometimes, never*), attitude toward an alarm found in the property (three-scale response—*always, sometimes, never*), a number of the property with alarms for burglars to attempt to burglarize (five-scale response—*all, more than half, half, a few, none*).

The last dimension, how burglars respond to an alarm they encounter, is measured by four variables—frequency of attempts to disable an alarm (three-scale response—*always, sometimes, never*), how successful the attempts were (dichotomous response—*yes, no*), whether to cut alarm wires before breaking into a property (three-scale response—*always, sometimes, never*), frequency of tools used to disable an alarm (five-scale response—*all, more than half, half, a few, none*).

Statistical approaches

The main analyses are based on descriptive and crosstab analyses. A series of questions related to burglar alarms are presented with summary tables and findings. SPSS 26 and Stata 16 software are used.

ANALYSES AND FINDINGS

Demographic and Criminal Characteristics

The initial questions in the survey, Tables 1 and 2, gather the 242 sampled inmates' demographic and criminal information characteristics. The average age of the incarcerated subjects is 30.4 years. Since the survey is administered among adult state prisons, minors under 18 years old are not included. About 53% of respondents are in

their 20s, with about 30% in their 30s. Burglaries are usually a criminal activity of young males. The second category of the "age" variable is the time of the inmates' first arrest (the first arrest is not necessarily for burglary). The average age of the first arrest is 23.4 years old, seven years younger than that of the incarcerated burglars. Age distributions of the first arrest by survey participants attest that 7% were first arrested at 13 years old or younger. High school ages, typically from 14 to 17 years, are 10%. Late adolescents, 18-19, represent about 20%; 44% were in their 20s, with only 15.7% 30 or older at the time of their first arrest.

Table 1. Difference between the current and first arrest of ages among the survey participants

Age category	*Current Age*		*Age of the 1st Arrest*	
	Frequency[a]	**%**[b]	**Frequency**[a]	**%**[b]
<=13	n/a	n/a	16	6.9
14-17	n/a	n/a	23	10.1
18-19	2	.8	46	20.1
20-24	68	28.1	55	24.0
25-29	60	24.8	46	20.1
30-34	47	19.4	20	8.8
35-39	23	9.5	13	5.7
40-44	18	7.4	9	3.9
45-49	16	6.6	2	.8
50-54	5	2.1	1	.4
>=55	3	1.2	0	.0
Total	242	100.0	229	100.0
Mean age	30.4		23.4	

[a] Total number (*N*) of each variable may not equal due to 13 missing cases of "age of the first arrest."

[b] Total percentages of each variable may not be exact 100 due to rounding off.

Table 2. Demographic characteristics of the survey participants

Variable	*Category*	*Frequency*[a]	*%*[b]
Sex	Female	65	27.0
	Male	176	73.0
	Total (N)	241	100.0
Race	Caucasian	162	67.8
	African American	59	24.7
	Others	18	7.5
	Total (N)	239	100.0
Marital status	Married	19	7.9
	Divorced	19	7.9
	Separated	11	4.6
	Single	172	72.0
	Others	18	7.5
	Total (N)	239	100.0

[a] Total number (*N*) of each variable may not equal due to the missing cases ranging from 1-3 cases.
[b] Total percentages of each variable may not be exact 100 due to rounding off.

Regarding "race," about 68% of the study subjects are Caucasian, with about 25% Black. "Single" marital status consists of 72%. In short, the current data from the convicted Ohio burglars show that burglaries are crime dominated by Caucasian males in their 20s, while the percentage of Caucasian males in the state is 81.7%, 4.0% Latinos, Blacks 13.1%, and other 1.2% (US Census Bureau, 2019).

Table 3 presents the study participants' arrest and conviction statistics. The first variable is the number of arrests for burglary, which shows that on average the participants have 2.1 arrest experiences and that about 51% of them have had just one arrest recorded before their current offense. About 87% of the respondents have had 1-3 arrest history incidents. The conviction history for burglary also coincides with that of the arrest. Almost 90% of the convicted respondents have had a pattern of 1-3 previous convictions before the current one.

Table 3. Number of arrests and convictions for burglary

	# of Arrest for Burglary		*# of Conviction for Burglary*	
	Frequency[a]	**%[b]**	**Frequency[a]**	**%[b]**
	6	2.6	7	3.0
	117	50.6	127	54.0
	56	24.2	58	24.7
	29	12.6	25	10.6
	9	3.9	6	2.6
	6	2.6	3	1.3
	3	1.3	2	.9
	3	1.3	4	1.7
	0	.0	1	.4
	1	.4	1	.4
	1	.4	1	.4
Total	231	100.0	235	100.0
Average	2.1		2.0	

[a] Total number of each variable may not equal due to the missing cases ranging from 6-10 cases.
[b] Total percentages of each variable may not be exact 100 due to rounding off.

Perceptions on Alarms as a Deterrent

Previous research studies assessed the extent to which burglar alarms influence offenders on their planning or target selection process. The assumption was that, once burglars decide to "go for" the properties to be burgled, an alarm does not seem to be a major deterrent in the course of executing the crime. Typically, the discussion of the deterrent effect of alarms tends to be consequential during the planning or target selection processes. Burglars may be aware of the presence of an alarm but either ignore it, because he or she, as an experienced offender, knows how to handle it (i.e., cut the alarm wires or disable its operation), or the burglar enacts unrestrained impulsive behavior. In this study, multiple questions need to be raised to ascertain aspects of burglars' perceptions to carefully determine the deterrent effect of alarms. For the current study, the questions are grouped into three categories—contextual effects, direct effects, and coping attitude. Regarding the perception of a general deterrent effect on burglaries, several questions were devised to ask directly about alarms' impact on decision making or to ascertain the impact in the context of other security measures.

Contextual Effects of Alarms

An "alarm" is included as one of the available contextual effects with other common features at and around the properties (e.g., a dog, cars in the driveway, types of doors and windows, outdoor cameras, lightings, nearby neighbors, presence of police patrol cars, the volume of traffic in the area, newspapers piled up in the yard, a mailbox full of mail, and security or no-trespassing signs). Two questions ask (1) types of security measures that the burglars are concerned about when deciding whether to burglarize the place; and (2) what particular feature may cause burglars to desist from acting (see Table 4). Both questions have multiple-checking items. These questions seem alike, but they are constructed to examine what factors might influence burglars during the planning and target selection process. In contrast, the second question underscores the peculiar features to stop burglars from executing steps to commit their crimes. Both inquiries are contemplated in the context of other protective measures.

The most frequent factor mentioned by the study sample in mitigating their desire to burgle was the presence of outdoor cameras or surveillance equipment (75.3%). The next most powerful contextual deterrent is direct occupancy of the residence (about 70.0%). The presence of an alarm comes next (69.7%). The contextual deterrent effect of the alarm systems is even higher than the presence of a dog (68.0%), cars in the driveway or parking lot (66.3%), a police officer parked nearby (62.4%), and closeness of the neighbors (55.1%). Three top-rated features relate to the presence of people at or around the house—residents at the house, police officers on the streets, neighbors, but if these people are not present, the use of other deterrents can produce desired results. Alarms are the most frequently checked features to stop burglars acting feloniously, higher than outdoor cameras or surveillance equipment (48.8%), cars in the driveway or parking lot (44.8%), a dog (41.3%), a security sign (28.5%), steel bars over the windows or doors (27.3%), indoor lights on (21.5%), beware of dog signs (19.2%), neighborhood watch signs (14.0%), and outdoor lights on (13.4%). Visible outdoor cameras and alarm systems are part of the blended security measures taken to protect properties and are exceeded only by direct occupancy indicators and a police officer parked nearby the streets.

Table 4. Contextual residential security deterrent factors (multiple checked items)

Variables	Checking Items	*N*[a]	%[b]
Types of things when deciding[c]	Outdoor cameras or surveillance equipment	134	75.5
	People are inside	125	70.2
	An alarm	124	69.7
	A dog	121	68.0
	Cars in the driveway or parking lot	118	66.3
	Police officer parked nearby	111	62.4
	How close the neighbors are	98	55.1
	The amount of traffic in the area	96	53.9
	Security sign	93	52.2
	Several possible escape routes	91	51.1
Deterrent factors not to burglarize[d]	Seeing people in the house	134	77.9
	Police officer parked nearby	120	69.8
	Seeing neighbors	106	61.6
	Noise coming from the house	108	62.8
	An alarm	92	53.5
	Outdoor cameras or surveillance equipment	84	48.8
	Cars in the driveway or parking lot	77	44.8
	A dog	71	41.3

[a] N is based on multiple responses with "types of things when deciding (1,900 responses) and "deterrent factors not to burglarize (1,045).

[b] Percentage is based on multiple responses.

[c] Other checking items not included in Table 4 are volume of people walking in the area (48.9%), distance from other houses or businesses (40.4%), indoor lights on (40.4%), a place to hide (38.2%), steel bars over windows or doors (37.1%), distance from a major road (36.0%), neighborhood watch signs (33.7%), types of doors or windows (33.7%), a beware of dog sign (33.1%), newspapers piled up in the yard (29.8%), outdoor lighting (28.7%), mailbox full of mail (28.1%).

[d] Other checking items not included in Table 4 are a security sign (28.5%), steel bars over the windows or doors (27.3%), indoor lights on (21.5%), a beware of dog sign (19.2%), no cover (e.g., bushes) (15.7%), neighborhood watch signs (14.0%), and outdoor lighting (13.4%).

Direct Effects of Alarms

The direct effect of alarm systems on burglaries underscores specific responses from other available security features by the burglars in the study. That is, how an alarm can influence burglars independently as a deterrent. A set of four questions address this issue: focusing on target selection, frequency of alarm observations, attitude toward an alarm on the property, and

perceptions of properties with alarms already installed (not "attempted burglary") (see Table 5). As noted previously, the alarm factor tends to matter to would-be burglars in two time-points: during planning and target selection steps and during the intervals between the arrival at the site and before entering the property when seeing an alarm. Once burglars successfully enter the property, the alarm seems not to be a

deterrent in the duration between the actual burglary commission and exit from the site. The former time-point is covered by the first two aspects: target selection and frequency of alarm observation, while the latter time-point is addressed by the last two aspects—attitude toward an alarm in the property and number of the properties with an alarm as possible burglary targets.

For the first question of alarm factor on target selection—*whether alarms make a difference to select a target*, 71.3 % of the responses go to "Yes – I prefer *not* to burglarize a place with an alarm" ("No" - 28.7%). For the second inquiry on the frequency of alarm observation—*how often to determine there is an alarm in the property before a burglary attempt,* responses divide into three checking items of "always" (33.3%), "sometimes" (47.7%), and "never" (19%). From the burglars' point of view, about one-third of properties are equipped with alarm systems and about 20% of the properties targeted for burglaries are not protected by alarms. Therefore, more than half of the properties – considering 47.7% of the "sometimes" category and "always" items together – seem to be protected by the alarms deter burglars from not choosing such properties. In short, an alarm can function as a deterrent during the initial stage of planning or target selection.

Table 5. Alarms as direct deterrents to a residential burglary

Variables	Checking Items	%	*N*[a]
Target selection	*Yes - Prefer not to burglarize a place with an alarm*	71.3	195
Alarm observation	*Always*	33.3	195
	Sometimes	47.7	
	Never	19.0	
Attitude toward alarms found	*Always attempt the burglary*	12.6	199
	Sometimes attempt the burglary	36.2	
	Never attempt the burglary	51.3	
Properties with alarms to burglarize	*All of them*	3.1	196
	More than half of them	8.7	
	Half of them	6.6	
	A few of them	35.7	
	None of them	45.7	

[a] N represents the sample size of each "questions" category and excludes the missing cases, which range from 42-46.

The other two questions relate to the second time-point after the decision to commit burglary, yet before deciding whether to enter the selected target (see Table 5). For the question of alarm factor on the attitude toward an alarm in property—*once decided to burglarize a place but learn that there is an alarm in the property, will you attempt the burglary?,* the survey participants respond as follows: "never" (51.3%), "sometimes" (36.2%), and always (12.6%). More than half of the burglars in this study succinctly express to "*never*" attempt to burglarize the property once they observe an alarm installed even though they select and decide to do so. On the other hand, 12.6% of the respondents say to "*always*" burglarize the targeted property even if an alarm is found. This finding indicates that about two-thirds of the even decisive burglars are substantially deterred by the mere presence of alarms (combining 51.3% of "never" and 36.2% of "sometimes).

The last question of the alarm factor concerns the number of properties with an alarm already installed for determined burglars to attempt breaking (see Table 5). A burglar might choose a target after weighing several factors in and around the property, including an alarm installed at the property after arriving at the site. Thus, that person, in a sense, is a determined burglar, knowing that the selected target has already an alarm. How forcefully alarms can deter this determined actor is a relevant issue. To the question of alarm factor on how many properties with an alarm the burglars attempt to burglarize, the responses are "none of them" (45.9%), "a few of them" (35.7%), "half of them" (6.6%), "more than half of them" (8.7%), and "all of them" (3.1%). About 46% of the convicted burglars answer that, though they are determined, they decide not to select properties with an alarm installed. Combined with the "a few of them" category, about two-thirds of the burglars are forcefully deterred not to burglarize the already chosen targets by the presence of alarms.

Handling Burglar Alarms

How do burglars respond to alarms? The majority of the survey participants perceive that an alarm is a decisive deterrent, discouraging substantial actors in the course of selecting or breaking into the properties with alarms installed. But such a positive effect of alarms by the determined burglar does not guarantee the protection of residences. In particular, for experienced or professional burglars, the presence of alarm systems at the properties can be just another annoying concern, either to simply ignore it or to deal with it by disabling it, then to deter them from executing the next

steps of their criminal activity. Several questions cover this topic, such as the frequency of attempts to disable an alarm, how successful the attempts were, whether to cut alarm wires before breaking into a property and the frequency of tools used to disable an alarm.

The first question is whether burglars attempt to disable an alarm when they encounter it on the property (see Table 6). The responses are "never" (79.8%), "sometimes" (11.9), and "always" (8.3%). With the previous questions of contextual alarm factors on target selection and alarm observation, most burglars are disinclined to act further by the mere presence of alarm systems. Besides occupancy indicators on properties and the presence of a CCTV system, alarms are the top-ranked security measure for convicted burglars to consider avoiding, more effective than dogs, security signs, bars over the windows or doors, indoor lights on, and signs warning about dogs. Additionally, about half of the convicted burglars express that they would "*never*" attempt to burglarize properties when they find an alarm installed. These observations coincide with this question of attempting to disable an alarm when they find it. Though it is not clear with the current data about whether the burglars continue to carry on burglary as planned or give up at this moment, about 80% of the responses indicate that burglars do not attempt to disable alarms on the properties. They are usually in a hurry to complete their work and may not possess the know-how to disable the alarm system.

The next question—*how effective they are in disabling an alarm*—provides some clues to such a high rate of 79.8% is attempting to disable an alarm (see Table 6). A dominant majority of the study participants check "no" (78.2%) that they are not effective in disabling an alarm, while 21.8% indicate "yes," assuming that the burglars know the presence of an alarm and have tried to disable it. Among the participants who check "yes," the question asks when they disable an alarm. Though the total number of the respondents is only 39 out of 179, the majority disables alarms "before" they are activated (61.5%), while 38.5% of them disable "after" being activated. This finding indicates that decisive actors who select targets and decide to commit burglaries tend to know that their target has an alarm installed and are prepared to disable the alarm before it is activated. They know how to do it. The other group may not recognize the presence of an alarm at the property but soon realize it once it is activated and successfully disabled. The second group assumes that they might think that an alarm may not be working or that it may be a dummy.

Another question asks about one specific but common method to disable burglar alarms—*cutting alarm wires* (see Table 6). The top category is "never" (78.9%), followed by "sometimes" (17.1%) and "always" (4.0%), which coincides with the previous question that presumably burglars who demonstrate that they *do not* effectively disable an alarm (78.2%) also *do not* attempt to cut alarm wires when they see them on the properties. Except "always" category (4%), when combined "never" (78.9%) and "sometimes" (17.1%), over 90% of the convicted burglars may not try to disable burglar alarms.

Table 6. Responses of how to handle an alarm

Questions	Checking Items	%	*N*[a]
Attempt to disable an alarm	*Always*	8.3	193
	Sometimes	11.9	
	Never	79.8	
Effective in disabling an alarm	*No*	78.2	179
	Yes – disable an alarm BEFORE activation	13.4	
	Yes – disable an alarm AFTER activation	8.4	
Cut alarm wires before entering in	*Always*	4.0	199
	Sometimes	17.1	
	Never	78.9	

[a] N represents the sample size of each "questions" category and excludes the missing cases, which range from 42-62.

The last question regards how to use tools to disable alarms (see Table 7). This is a contextual query with other items rather than a separate probe. The multiple-checkable items of tools burglars might use in this question include crowbars, screwdrivers, masks/disguises, bump keys, lock picking kits, window punches, hammers, bags/containers to carry the items stolen, electronic tools to disable an alarm, and mechanical tool(s) to disable. Multiple responses by the burglars in this study show that the top-ranked tools are: screwdrivers (54.9%), bags/containers to carry the items stolen (45.8%), masks/disguises (43.1%), and crowbars (38.9%). The mid-ranked tools are lock picking kits (20.1%), hammers (18.8%), and window punches (14.6%). Low-ranked tools include other disabling tools (11.8%), bump keys (10.4%), and electronic tools to disable an alarm (9.7%). The least favorable tool that convicted burglars might carry to commit burglary is an "electronic tool" to assist in disabling an alarm. This observation corresponds with the findings just above that about 80% of the convicted burglars rarely attempt to disable an alarm (79.8%), are not effective in doing so (78.2%), or hardly ever try to cut alarm wires before entering

the targeted properties (78.9%). Burglars largely endeavor not to interact with an alarm when they see it or spot its presence on or around the houses or properties. Thus, they may not need to carry any tools to assist them in disabling alarms. Further, in the event of an arrest, the presence of tools could imply a greater degree of preparation and lead to a stronger case for prosecutors.

These four questions demonstrate how burglars respond to alarms meant to deter them. The overwhelming majority of responses disclose that burglars are not only discouraged from choosing properties with alarms already installed during the stages of planning and selection, but also are deterred by the presence of alarm systems on the properties before entering them. Furthermore, burglars, though arrived at the pre-selected site, generally avoid attempting to disable an alarm or cut alarm wires. The exact reasons why they avoid or do not attempt to disable an alarm are not established.

Table 7. Frequency of types of tools used to commit burglaries

Tool Items	*N*[a]	%[b]
Screwdriver	79	54.9
Bag/containers in which to carry the items you obtain	66	45.8
Mask/disguise	62	43.1
Lock picking kit	29	20.1
Hammer	27	18.8
Window punch	21	14.6
Hammer	27	11.8
Other tool (s) to assist in disabling an alarm	17	11.8
Bump key	15	10.4
Electronic tool to assist in disabling an alarm	14	9.7

[a] *N* is based on multiple responses with 386 responses.
[b] Percentage is based on multiple responses.

DISCUSSION AND CONCLUSION

This study advances the scope of research on burglar alarms as effective deterrents to residential burglary by assessing the opinions of convicted burglars. A wide range of direct questions explored target selection and subsequent decision-making. The questions are grouped into three categories of alarm factors—contextual, direct, and handling attitude. The data are derived from responses of 242

convicted burglars at four Ohio state prisons. Burglaries are dominated by Caucasian males in their 20s, though Blacks are disproportionately present as actors. These burglars tend to have had long arrest histories and experience with the criminal justice system before their current convictions. Initial engagements in criminal behaviors start much earlier than conviction. On average, burglars in this study before incarceration had 2.1 arrests and 2.0 convictions, with almost 90% having 1-3 re-offending history of burglaries.

Camera systems were slightly more frequently mentioned as deterrents than alarms. Together, camera systems and alarms provide the two most frequently cited easily procurable electronic security measures to protect property from burglary, though having someone home and a police car parked nearby are even more powerful deterrents. As a residential security strategy, keeping someone at home or a police car nearby primarily as an anti-burglar strategy is not realistic options. Security systems require one-time purchase costs and modest monthly recurring monitoring fees. Monitoring can occur at a local office, a central station, on one's handheld, or a combination. Burglars understand the risks they assume if they choose to enter such premises.

Questions in this research centered mostly on the impact of alarms which function as a dissuasive during the initial stages of planning or target selection; about two-thirds of the burglars are forcefully deterred not to enact their crime in the presence of alarms. Furthermore, about two-thirds of the even decisive burglars are substantially deterred by the mere presence of alarms. The overwhelming majority of the burglars in this study deal with alarms, once arrived at the pre-selected site, by not disabling them but by acting and leaving more quickly than in facilities without such measures. Only a few actors cut alarm wires or otherwise disabled them.

A few research studies in the United Kingdom concluded that burglar alarms may have no net effect as a deterrent and that alarms can increase the risk of burglary victimization. However, the current study confirms most of the previous evidence that such alarms are a statistically valid preventative measure against burglaries. Burglar alarms and camera systems produce a true deterrent effect in the opinion of the respondents who have been convicted for this type of crime.

However, as seen in Table 4, depending on alarm systems exclusively as deterrent measures is unwise. Previous work on this topic since the early 1970s shows that in most cases an alarm can be more effective when combined with other protective

security measures, such as locks, better materials on doors and windows, grills over doors and windows, light inside and outside, dogs, and security yard signs. Camera systems now join these security measures. For further burglary mitigation evidence-based approaches, concentrating on burglary hotspots and social-economic and demographic analyses (Lee, 2010a, 2010b), might be productive.

Several limitations linked to the current study are worth noting. For example, the data source for this study came from the survey. Since the surveys were collected from the incarcerated inmates, the truthfulness of their responses cannot be verified. In particular, personal information (e.g., age, criminal history, arrest history, etc.) was not verified with police or courts records. In addition, since the surveys were collected from adult prisons, we do not know about the participants' criminal records as minors if any. This unknown gap can be a future research topic to explore furthermore about minor/juvenile burglars' perception of alarm systems and their deterrent effect.

Despite several limitations of the study, one significant aspect of the current study is that, unlike most of the previous studies which rarely treated a burglar alarm as an independent variable to access its deterrent impact on burglaries, this project examined the direct/net effect of alarm systems on residential crime prevention approaches, being separated from other home protection measures (e.g., camera systems, windows/door locks, light, and dogs). Alarm systems have technologically advanced and become more user-friendly control mechanisms (e.g., smart home security products). This study is one of the first examinations to scrutinize the direct impact of alarms based on the convicted burglars.

References

Bennett, T., & Wright, R. T. (1984). *Burglars on burglary: Prevention and the offender.* Hampshire, U.K.: Gower.

Blackstone, E., Hakim, S., & Meehan, B. (2020). Burglary reduction and improved police performance through private alarm response. *International Review of Law and Economics, 63*(1), 1-13.

Buck, A. J., Hakim, S., & Rengert, G. F. (1993). Burglar alarms and the choice behavior of burglars: A suburban phenomenon. *Journal of Criminal Justice, 21*(5), 497-507.

Cedar Rapids Police Department. (1971). *Installation, test, and evaluation of a large-scale burglar alarm system for a municipal police department.* Washington, DC: US Department of Justice, National Institute of Law Enforcement and Criminal Justice.

Clarke, R. V. (1997). Introduction. In R. V. Clarke (Ed.), *Situational crime prevention: Successful case studies* (2nd ed.) (pp. 1-43). Guilderland, NY: Harrow and Heston.

Clarke, R. V. (2002). Burglary of retail establishments. *Problem-Oriented Guides for Police Series* (No. 15). Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.

Conklin, J., & Bittner, E. (1973). Burglary in a suburb. *Criminology, 11*(2), 206-232.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology, 44*(2), 431-464.

Coupe, T., & Kaur, S. (2005). The role of alarms and CCTV in detecting non-residential burglary. *Security Journal, 18*(2), 53-72.

Cromwell, P. F., & Olson, J. N. (2004). *Breaking and entering: Burglars on burglary.* Belmont, CA: Wadsworth and Thomson.

Cromwell, P. F., Olson, J. N., & Avary, D. W. (1991). *Breaking and entering: An ethnographic analysis of burglary.* Newbury Park, CA: Sage.

Farrell, G., & Brown, R. (2016). On the origins of the crime drop: Vehicle crime and security in the 1980s. *The Howard Journal of Crime and Justice, 55*(1-2), 226-237.

Farrell, G., Tilley, N., & Tseloni, A. (2014). Why the crime drop? In M. Tonry (Ed.), *Why crime rates fall and why they don't.* Crime and Justice (Vol. 43) (pp. 421-490). Chicago, IL: University of Chicago.

Felson, M. (2017). Criminology's first paradigm. In N. Tilley & A. Sidebottom (Eds.), *Handbook of crime prevention and community safety* (2nd ed.) (pp. 22-31). New York: Routledge.

Freedonia Group. (2020). Safety & *security alarms, industry study #3784*. Cleveland, OH: Freedonia.

Gaes, G. G., & Goldberg, A. L. (2004). *Prison rape: A critical review of the literature.* Washington, DC: National Institute of Justice.

Greer, W. (1991). *A history of alarm security* (2nd Ed.). Bethesda, MD: NBFAA.

Hakim, S., & Buck, A. J. (1991). *Deterrence of suburban burglaries.* Cheltenham, PA: Metrica.

Hakim, S., Rengert, G. F., & Shachmurove, Y. (2001). Target search of burglars: A revised economic model. *Papers in Regional Science, 80*, 121-137.

Hakim, S., & Shachmurove, Y. (1996a). Social cost benefit analysis of commercial and residential burglar and fire alarms. *Journal of Policy Modeling, 18*(1), 49-68.

Hakim, S., & Shachmurove, Y. (1996b). Spatial and temporal patterns of commercial burglaries: The evidence examined. *American Journal of Economics and Sociology, 55*(4), 443-456.

Hearnden, I., & Magill, C. (2004). *Decision-making by house burglars: Offenders' perspectives.* London, UK: Home Office.

Hensley, C., Rutland, S., & Gray-Ray, P. (2000). Inmate attitude toward the conjugal visitation program in Mississippi prisons: An exploratory study. *American Journal of Criminal Justice, 25*(1), 137-145.

Hilgers, L. (2021). Who's there? The hardworking nurse who envisioned a new way to know who was at the door. *Smithsonian,* March, p. 20.

Holmes, E. (1990). *A wonderful fifty years.* New York: Holmes Protection. (originally published 1917)

LeBeau, J. L., & Vincent, K. L. (1997). Mapping it out: Repeat-address burglar alarms and burglaries. In D. Weisburd & T. McEwen (Eds.), *Crime mapping and crime prevention, Crime Prevention Studies* (Vol. 8) (pp. 289-310). Monsey, NY: Criminal Justice Press.

Lee, S. (2008). *The impact of home burglar alarm systems on residential burglaries.* (UMI Number: 3326964) [Doctoral dissertation, Rutgers University]. ProQuest Dissertations Publishing.

Lee, S. (2010a). Installation trends and characteristics of residential burglar alarms. *Journal of Applied Security Research, 5*(2), 176-207.

Lee, S. (2010b). Spatial analyses of installation patterns and characteristics of residential burglar alarms. *Journal of Applied Security Research, 6*(1), 82-109.

Letkemann, P. (1973). *Crime as work.* Englewood Cliffs, NJ: Prentice-Hall.

MacDonald, J. E., & Gifford, R. (1989). Territorial cues and defensible space theory: The burglar's point of view. *Journal of Environmental Psychology, 9*(3), 193-205.

Maguire, M., & Bennett, T. H. (1982). *Burglary in a dwelling.* London, UK: Heinemann.

Mawby, R. I. (2001). *Burglary.* New York, NY: Routledge.

McCrie, R. D. (2004). The history of expertise in security management practice and litigation. *Security Journal, 17*(3), 11-19.

McCrie, R. D. (2006). A history of security. In M. Gill (Ed.), *The Handbook of Security* (pp. 21-44). New York, NY: Palgrave Macmillan.

McCrie, R. D., & Lee, S. (2023). *Security operations management* (4th ed.). Cambridge, MA: Butterworth-Heinemann.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice, and criminal victimization: A test of a theoretical model. *Journal of Research in Crime and Delinquency, 27*(3), 243-266.

Nee, C., van Gelder, J. L., Otte, M., Verham, Z., & Meenaghan, A. (2019). Learning on the job: Studying expertise in residential burglars using virtual environments, *Criminology, 57*: 481-511. https://doi.org/10.1111/1745-9125.12210.

Nee, C., & Meenaghan, A. (2006). Expert decision making in burglars. *British Journal of Criminology, 46*(5), 935-949.

O'Shea, T. C. (2000). The efficacy of home security measures. *American Journal of Criminal Justice, 24*(2), 155-167.

Rengert, G., & Wasilchick, J. (1985). *Suburban burglary: A time and a place for everything.* Springfield, IL: Charles C Thomas.

Reppetto, T. G. (1974). *Residential crime.* Cambridge, MA: Ballinger.

Roth, J. J. (2017). A city-level analysis of property crime clearance rates. *Criminal Justice Studies, 30*(1), 45-62.

Roth, J. J. (2018). The role of perceived effectiveness in home security choices. *Security Journal, 31*(3), 708-725.

Roth, J. J., Lee, S., & Joo, J. (2018). The effect of community-level alarm ownership on burglary rates. *Journal of Applied Security Research, 13*(2), 160-171.

Roth, J. J., & Roberts, J. (2017). Now, later, or not at all: Personal and situational factors impacting burglars' target choices. *Journal of Crime and Justice, 40*(2), 19-137.

Roth, J. J., & Trecki, V. L. (2017). Burglary expertise: Comparing burglars to other offenders. *Deviant Behavior, 38*(2), 188-207.

Rothstein, S. J. (2020). *Temporal patterns for burglar alarms and police-coded burglaries* (Unpublished dissertation). Texas State University, San Marcos, TX.

Rubenstein, H., Murray, C., Motoyama, T., Rouse, W. V., & Titus, R, M. (1980). *The link between crime and the built environment: The current state of the knowledge* (Vol. 1). Washington, DC: US Department of Justice, National Institute of Justice.

Sampson, R. (2011). False burglar alarms (2nd ed.). *Problem-oriented guides for police series guide* (No. 5). Washington, DC: US Department of Justice.

Scarr, H. A. (1973). *Patterns of burglary.* Washington, DC: US Government Printing

Office.
Sherman, L. W., Strang, H., Mueller-Johnson, K., Weinborn, C., Valdebenito, S., McFadzien, K., & Strang, L. (2017). *Mobilising civil society against residential burglary: The evidence.* Somersham, UK: Cambridge Centre for Evidence-Based Policing.
Shover, N. (1991). Burglary. In M. Tonry (Ed.), *Crime and Justice: A Review of Research* (Vol. 14) (pp. 73-113). Chicago, IL: University of Chicago Press.
Tilley, N., Thompson, R., Farrell, G., Grove, L., & Tseloni, A. (2015). Do burglar alarms increase burglary risk? A counter-intuitive finding and possible explanations. *Crime Prevention and Community Safety, 17*(1), 1-19.
Tseloni, A., & Thompson, R. (2015). Securing the premises. *Significance, 12*(1), 32-35.
Tseloni, A., Thompson, R., Grove, L., Tilley, N., & Farrell, G. (2016). The effectiveness of burglary security devices. *Security Journal, 30*(2), 646-664.
Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands. *British Journal of Criminology, 44*(1), 66-91.
U.S. Census Bureau QuickFacts: Ohio (2019). https://www.census.gov/quickfacts/OH
Vandeviver, C., & Bernasco, W. (2020). Location, location, location: Effects of neighborhood and house attributes on burglars' target selection. *Journal of Quantitative Criminology, 36*, 779-821. https://doi.org/10.1007/s10940/019-09431-y.
Waller, I., & Okihiro, T. (1978). *Burglary: The victim and the public.* Toronto, Canada: University of Toronto Press.
Walsh, D. P. (1980). *Break-ins: Burglary from private houses.* London, UK: Constable.
Weisel, D. L. (2002). Burglary of single-family houses. *Problem-Oriented Guides for Police Series* (No. 18). Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.
Winchester, S., & Jackson, H. (1982). Residential burglary. *Home Office Research Study* (No. 74). London, UK: HMSO.
Wright, R. T., & Decker, S. (1994). *Burglars on the job: Streetlife and residential break-ins.* Boston, MA: Northeastern University Press.
Wright, R., Logie, R. H., & Decker, S. H. (1995), Criminal expertise and offender decision making: An experimental study of the target selection process in residential burglary. *Journal of Research in Crime and Delinquency, 32*(1), 39-53.

Crime-Terror Nexus: Assessing East Africa's Responses

*Mohamed Daghar**
Regional Coordinator, Eastern Africa
Enhancing Africa's Response to Transnational Organised Crime (ENACT) Programme
Institute for Security Studies

Abstract

There is growing international concern over the nexus between transnational organized crime, and terrorism – a significant, complex, and dynamic threat to global security. Considerable evidence from different regions in the world, such as South America and Sub-Saharan Africa, suggests that there has been greater collaboration between terrorist groups and transnational criminal networks in the trafficking of narcotics and arming of terrorist groups. Complex as implementing legislation and law enforcement operations are limited in capacity and dynamic as this nexus keeps changing. The burden of proof in convicting such crimes has remained challenging, with law enforcement often preferring to use penal code than anti-terrorism instruments. Thus the scale of this nexus has not been verified systematically by frontline state agencies and non-state experts. This paper assesses challenges, achievements, and solutions to address the nexus between transnational organized crime and terrorism in East Africa. In so doing, the report explores ways in which transnational organized crime and terrorism are linked. Addressing this linkage is a priority for many countries in East Africa, one of the regions most affected by terrorism and transnational organized crime in Africa.

Keywords

Transnational organized crime, terrorism, nexus, East Africa

* Direct correspondence to the author; mohamed.daghar@gmail.com
* http://dx.doi.org/10.36889/IJCJ.2021.010
* Received 28 October 2021; Revised 5 December 2021; Accepted 21 December 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 95-114

INTRODUCTION

There is growing international concern over the nexus between transnational organized crime and terrorism – a significant, complex, and dynamic threat to global security. Significant as evidence from different regions in the world, such as South America and Sub-Saharan Africa is suggesting that there has been greater collaboration between terrorist groups and transnational criminal networks in the trafficking of narcotics and arming of terrorist groups (De Castanedo, 2021; Jaitman & Machin 2016; Luhnow, 2014). Complex as implementing legislation and law enforcement operations are limited in capacity and dynamic as this nexus keeps changing. The burden of proof in convicting such crimes has remained challenging, with law enforcement often preferring to use penal code than anti-terrorism instruments.

Thus, this nexus scale has not been systematically verified by frontline state agencies, regional policing and prosecuting authorities, and other experts who are disseminating authoritative knowledge in this field.

The probability of terrorist groups benefiting from transnational organized crime and transnational organized crime benefitting from terrorist tactics may undermine affected States, specifically their security, stability, governance, and social and economic development.

Historically, studies (UNODC, 2018) show that transnational organized crime and terrorism differ in motivation, but their operational, organizational, and conceptual convergence continues to grow over the past three decades. In some regions in Africa, terrorists benefit from the criminal experiences of individuals they have recruited. These individuals provide expertise in counterfeiting documents and access to weapons and explosives. In other regions, terrorist groups financially benefit from direct involvement in the trafficking of arms, persons, drugs, and artifacts as well as from the illicit trade in natural resources, including gold and other precious metals and stones, minerals, wildlife, charcoal and oil; and also from kidnapping for ransom and other crimes including extortion, and bank robbery (GITOC, 2018; Shaw, 2017). Yet, in other regions, organized crime has employed indiscriminate violence against civil populations as a way to secure territorial influence (UNODC, 2018).

Therefore, identifying the links between terrorism and transnational organized

crime presents a unique opportunity in combating the two threats. However, the evidence on the phenomenon is still, at best anecdotal. Secondly, there are still no universally agreed definitions of organized crime and terrorism to guide the gathering and analyzing relevant information. These challenges are being exacerbated by local variations that shape how this nexus emerges and how it evolves. The nexus presents a point of organizational vulnerability to terrorist and transnational organized crime groups since knowing how, when and where the nexus emerges can be used as an effective policy tool (GCTF, 2021).

Between 2007 and 2017, with the crime-terror nexus dominating the agenda, the United Nations Security Council (UNSC) passed 1,113 resolutions and 387 (34.8%) referenced organized crime concerning the global conflict setting (GITOC, 2018). Some of the critical resolutions of this nexus are:

1. Resolution 2195 (2014) calls upon states 'to better understand and address the nexus between organized crime and terrorism as a threat to security and development.' (UNSC, 2014)
2. Resolution 2322 (2016) calls upon states to 'enhance cooperation to prevent terrorists from benefiting from transnational organized crime, investigate and build the capacity to prosecute such terrorists and transnational organized criminals working with them'. (UNSC, 2016)
3. Resolution 2370 (2017) urges Member States to 'strengthen, where appropriate, their judicial, law enforcement and border-control capacities, and developing their investigation capabilities of arms trafficking networks to address the link between transnational organized crime and terrorism.' (UNSC, 2017)
4. UN Resolution 2482 (2019) on terrorism and organized crime. (UNSC, 2019)

These United Nations (UN) resolutions have formed a basis of regional and national legislative frameworks that East African countries have since instituted. Already, some steps to address this threat have yielded positive results in East Africa. For example, the Eastern Africa Police Chiefs Cooperation Organization (EAPCCO) has shown strong involvement in the region. The UNODC and INTERPOL 'mentoring' seem to have brought in some promising initial results (EAPCCO CTCOE, 2021; UNODC, 2021).

Platforms such as the Global Counter-Terrorism Forum (GCTF) also assist

regions globally, including East Africa, to develop legislative and response capacities to combat this nexus. GCTF initiatives such as the Hague Good Practices on the nexus between Transnational Organized Crime and Terrorism (GCTF, 2021) serve as a possible guideline to countries in the East Africa region on how to deal with them this challenge by expanding both their legislation and practical responses. The GCTF has also developed a Policy Toolkit to operationalize the Good Practice document (GCTF & UNICRI, 2019).

This paper seeks to analyze a realistic assessment of challenges and achievements, and solutions that have been realized in addressing the nexus between transnational organized crime and terrorism in East Africa. In so doing, the paper seeks to explore how transnational organized crime and terrorism are linked. This is a priority for many countries in East Africa, one of the regions most affected by transnational organized crime and terrorism in Africa.

METHODOLOGY

Literature review

Linkages between different types of crime are not new. Internationally, the literature on the nexus between transnational organized crime and terrorism started growing robustly after the September 2001 attacks where Al-Qaeda carried out four attacks in the United States of America (USA). These quadruple attacks were sophisticated and coordinated internationally with the help of organized criminals who could infiltrate the national security and defense system of the USA.

In its 9/11 commission report (U.S. Government, 2004) the USA called for an increase in concerted efforts on counter-terrorism by calling for a ‘broader range of national security challenges in the decades ahead.’ Two decades later after the 9/11 attack, an enormous body of literature has grown on the nexus between transnational organized crime and terrorism.

A comprehensive review of existing literature was conducted for this paper. These included academic articles on terrorism, transnational organized crime and those specific to the nexus. 40 UNSC resolutions were perused through and four of the most important were analyzed concerning understanding the international approach to the nexus between transnational organized crime and terrorism. These include UNSC

2195 (2014), 2322 (2016), 2370 (2017), and 2482 (2019).

Many reports from international organizations such as the United Nations and the World Bank were equally reviewed, as well as many from non-governmental organizations across the world. Also included in the literature review were reports from civil society organizations and media articles.

However, it is noted that less literature still exists on the nexus between specific forms of transnational organized crime and terrorism. Most of the literature reviewed, compounded transnational crime as a whole with terrorism. To fill in this knowledge gap, the author drew into parts of the field research conducted by the organizsation he works for at the time of writing this research.

Field research

At the time of writing this research, the author worked for the Institute for Security Studies (ISS) ENACT programme. ENACT is a fully-funded European Union Programme and enhances Africa's response to transnational organized crime. It is implemented by the ISS, INTERPOL, and the Global Initiative against Transnational Organized Crime.

ENACT conducted an empirical study on the nexus between transnational organized crime and terrorism in Kenya and Uganda. The author was part of the team that conducted this research and uses some of the fieldwork data obtained for Kenya in this journal with full attribution to the ENACT programme. The field research interviewed law enforcement officers from the investigations department, anti-terrorism police unit, prosecution and judiciary.

Limitation of the Study

The study does not allude further to the pervasiveness of the specific types of transnational organized crime in the specific countries of East Africa. Thus, an indicator of countries with high criminality and other high or low response to these crimes does not allude further as the author noted that this may go beyond the scope of the study and its research question.

Further, considering the size of the criminal market in Africa and subsequently, in East Africa, the study does not delve into the specificities on the impact of this criminal market on the lives and livelihoods of its people. Though it is important to

first establish the impact this criminal economy has had on the residents of Africa and measure the resilience of African governments to protect its citizenry. This is an area of further research worth undertaking.

Contextualizing the nexus in East Africa: background

Countries in East Africa continue to face challenges of insecurity that hinder the region's governance, security, development and the practical application of the rule of law. These insecurity challenges emanate from armed, organized criminal and terrorist groups that operate transnationally.

However, over the last two decades, there has been an increase in these groups working together. In Uganda alone, for example, about seven groups are both terrorist and transnational organized criminal groups. These are the Allied Democratic Forces (ADF), the Lord's Resistance Army (LRA), al-Shabaab, Islamic State in Central Africa Province, Jahba East Africa, Force Obote Back Again (FOBA) and Kifesi.

Terrorist groups have influenced in the East Africa region even before the formation of the al-Shabaab. Osama bin Laden, the then leader of Al-Qaeda, was based in Sudan before the 1998 Nairobi and Dar es Salaam twin bombings. In the 1990s and in Sudan, Bin Laden formed the 'Islamic Army Shura' to develop new terrorist groups and form alliances with existing ones (9/11 commission report, 2004). From Sudan, Bin Laden coordinated with groups in Sub-Saharan Africa and those in Asia, including the Taliban in Afghanistan (Forest, J. 2011). It was evident that Bin Laden Shura managed to grow increasing admiration of terrorist groups in Sub Saharan and those already operating in Asia. For example, the Boko Haram operating in Nigeria, in its years of formation, referred to itself as the 'Nigerian Taliban' (Mohammed, S., Mohammed, Y.K. & the Nigerian State, 2011).

Bin Laden also set up the funding of these groups using existing global enterprises (9/11 commission report, 2004). This was the inception of the terrorist groups' cooperation with organized criminal networks. For example, to supply arms, terror groups in East Africa had to be connected to arms traffickers who already had robust global supply chains moving illicit firearms from countries such as Libya, Somalia and those in Eastern Europe (9/11 commission report, 2004). These criminal networks were well established using the political economy to canvas the movement of funds.

Terrorist groups had to form non-governmental organizations such as charities

and foundations as a decoy to pay for receiving illicit firearms from traffickers (9/11 commission report, 2004). This period in the 1990s witnessed the forging of cooperation between these two criminal entities.

Suicide bombers from terror groups moved across countries in the region by gaining fake passports facilitated by transnational organized groups. Even recently, in August 2021 (Reuters, 2021), a suicide bomber was arrested when he tried crossing into Uganda from Kenya with a fake South African passport that they obtained through an organized crime syndicate.

During this period, ADF, a predominantly terrorist group, started controlling several mines in the DRC along the Semliki river that cuts across to Uganda. ADF started charging taxes to both artisanal coltan, gold and tin miners who were each paying 1,000 Congolese francs as well as large miners in May-Moya, Beni territory (UN, 2011). The ADF benefitted from the most lucrative illicit trade was aiding the trafficking of timber from the DRC in collaboration with transnational organized crime networks (UN, 2011). With a connection in both DRC and Uganda, timber moved between these two countries to the other regions worldwide through the port of Mombasa in Kenya.

The most prominent terrorist group in East Africa is al-Shabaab, and just like the ADF, it is both a terrorist and a transnational organized criminal group. Al-Shabaab works with other criminal networks to gain funds to run its operations (Petrich, K. 2019). The group is deeply embedded in the smuggling of charcoal, arms and food commodities such as sugar, rice and powdered milk. As of late 2017, the UN Security Council stated that al-Shabaab continued to derive revenues from the illicit export of charcoal from Somalia (UNSC, 2017).

Also, in 2015 the UN-mandated Somalia and Eritrea Monitoring Group (SEMG) pointed out that the risk of al-Shabaab procuring illicit firearms remains (UNSC, 2015). The previous year, SEMG reports had obtained credible information from military intelligence sources that maritime vessels from Yemen delivered consignments of weapons and improvised explosive device (IED) component materials to al-Shabaab commanders at drop-off points on the Somali coast (UNCS, 2014). It should also be noted that the same routes used to smuggle sugar or cattle can supply weapons or move fighters. By integrating criminals who have pre-existing relationships and networks, al-Shabaab improves its operational agility (Petrich, K., 2019).

The distinctiveness of the nexus in East Africa

Terrorism is driven by ideology. In most instances, this ideology is either religious and/or political.

Financial gains drive transnational organized crime – massive profits. These profits are often moved through the political economy. For example, in 2009, the World Bank estimated that the profits gained from transnational organized crime in Africa and moved through the political economy stood at US$1.3 billion (ENACT, 2017). Two years later, in 2011, these profits grew by a 50% growth per annum, amounting to US$3.3 billion (ENACT, 2017).

Terrorism and organized crime are pretty distinct. In East Africa, terrorist groups are not many. The main ones are the al-Shabaab in Somalia and Kenya and the Allied Democratic Forces (ADF) operating in Uganda and the Democratic Republic of Congo (DRC). Transnational organized crime groups, however, are numerous with divergent interests in different sectors of the political economy. For example, in Kenya and Somalia, transnational organized crime groups have formed cartels in the food sector by smuggling sugar, rice, and milk powder from Somalia's Kismayo's port to Kenya (UNSC, 2017; Petrich, K. 2019). In South Sudan and Uganda, criminal cartels move timber such as teak trees planted in the 1940s that are being felled and transported for export to Asian countries through the port of Mombasa (Neumeister, C. & Cooper, S. 2019).

The type of violence used between terrorist groups and transnational organized crime groups also differs. There are four distinct criteria of violence used by terrorist groups. First is that terror groups target significant cities such as Kampala in Uganda and Kinshasa in the DRC. They also target large 'ungoverned' spaces where government presence is limited, for example, between and within the northeastern counties of Kenya, such as Marsabit and Garissa. Third, terrorist groups preponderantly target government personnel such as police and military officers and critical infrastructures such as telecommunication equipment and airports, as was the case with the Manda airstrip attack in Lamu, Kenya. Last and most important, there is a deliberate attempt of terrorist groups targeting civilians. As much as the terrorist groups insinuate that their target is government personnel and infrastructure, more so often, these groups have targeted civilians in almost all their attacks in East Africa. All significant attacks in Kenya, such as the Garissa University, DusitD2 and several

passenger bus attacks in Northern Eastern had civilians with the biggest casualties and fatalities.

The violence threshold of transnational organized crime groups is usually minimum, with less intensity to loss of lives and damage to property. The violence is also not indiscriminate but instead targeted. More often, the violence is between the transnational organized crime groups, and it can get as specific as targeting just particular players. There are no massive causalities involving third parties such as community members, as with terrorist attacks.

The continuum of the nexus in East Africa

A continuum is a condition where both terrorism and transnational organized crime are not different, but their motives and extremes are very distinct.

Reviewed literature (Roberts, I. 2021; Ryabchiy, K. 2018; Wang, P. 2010; Makarenko, T. 2010) suggests that terrorism is quite distinct from organized crime; there is a nuanced correlation between the two. The continuum between these two forms of crime plays out well in the East African region.

The interplay of this continuum is very similar in all the countries in the region, especially in Uganda, the DRC and Kenya. However, analyzing how the continuum plays out in all the countries in East Africa will be above the scope of this study. Thus, the author selected Kenya as a case study for the region to highlight some key findings.

The case study of Kenya

As mentioned in the methodology section of this paper, the ISS ENACT programme conducted empirical fieldwork research on the nexus between transnational organized crime and terrorism in Uganda and Kenya.

The ENACT study found out that these linkages are influenced by four factors, either independently or together. These are the necessity and circumstances for the actors to work together, having common goals at a particular point in time, complementing each other on a joint mission and having business relations on a specific product – whether licit such as food items or illicit such as firearms.

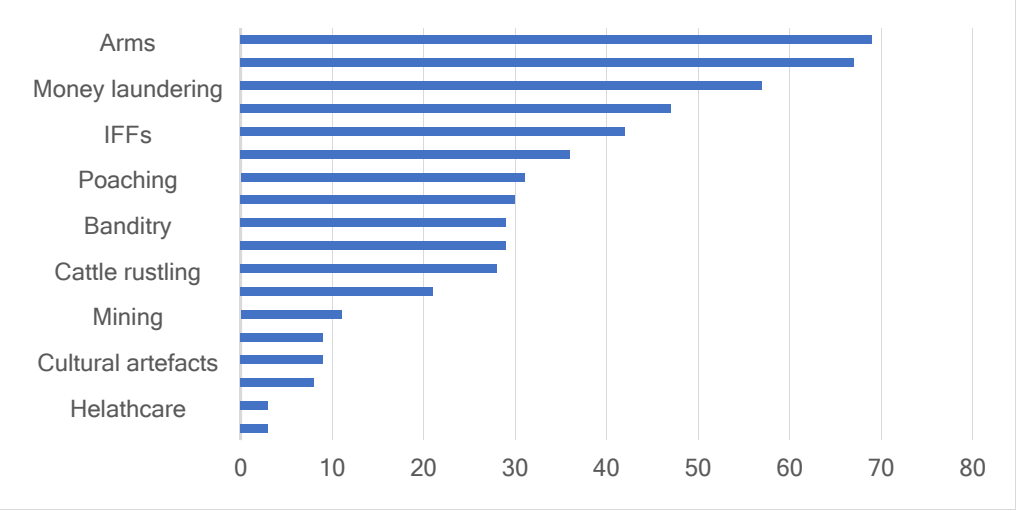
Respondents of the ENACT study indicated that the causes of terrorism and organized crime are communities' socio-economic vulnerabilities, lack of governance

in parts of the country, political marginalization and state excesses. Most respondents pointed out that the relationship between terrorist groups and organized crime networks is always excellent and becomes conflictual if one party crosses the other.

Most respondents also pointed out that while there is a distinction between organized crime and terrorism, it is increasingly becoming interrelated. This difference is based on the actors' common objectives and ideology and their group formation and types of violence used. While terrorism's objectives are politically inclined, organized crime is profit inclined. This vital distinction is critical for each type of crime, but the ENACT study indicates an increasing dependence of terrorism on profit-reliance and organized crime to the political economy. In most cases, this overlap has seen both criminalities converge on a mutually benefitting arrangement. Terrorist groups and organized crime networks meet virtually online through social media platforms. Physically, the two groups meet at places of worship, prisons, and public places like restaurants and markets.

90% of the respondents said that al-Shabaab is the biggest terror group Kenya faces, followed by the Islamic State. The al-Shabaab are increasingly commanding and shaping a political economy in their operations. Respondents suggested that al-Shabaab, stationed in Somalia and Kenya, work with organized criminal groups to move licit and illicit commodities between the two countries. These include illicit products like firearms that enter Kenya and licit ones like sugar and charcoal that enter Kenya illicitly by not paying duty. Despite the distinct objective and ideology of each form of crime group, the cooperation here was mutual as organized criminal groups use Somalia to ship products into Kenya, and al-Shabaab offers a safer passage of the products at an agreed fee.

Table 1. Cooperation between transnational organized crime actors and terrorists



Source: ISS ENACT research on the nexus between transnational organized crime and terrorists, 2021.

There is, however, distinction by the group formation and type of violence used in terrorism and organized crime in Kenya. While al-Shabaab remains the most extensive terrorist group operating in Kenya, organized crime groups are unknown by formation and names but believed to be many. Al-Shabaab use of violence is distinct, targeting major cities and large ungoverned spaces, mainly in the Northeastern counties of Kenya. Al-Shabaab violence targets both government personnel and critical infrastructure. As much as this form of violence is targeted, local communities become collateral damage. Organized crime groups are small and sporadic, targeting anywhere in the country but less intensity to loss of lives and damage to property.

Responses to the nexus: measures taken and challenges in Kenya

Legal framework and criminal justice system of terrorism and organized crime

In Kenya, a robust legal framework is in place for both terrorism and organized crime. The same frameworks have shared provisions that are often used in addressing the linkages between these two forms of crime.

The key terrorism legislation used is The Prevention of Terrorism Act, Act No. 30 of 2012. For organized crime, the legislations are; The Prevention of Organized Crime Act No. 6 of 2010; The Penal Code Cap 63 LoK; The Criminal Procedure Act Cap 75

LoK; Counter Trafficking in Persons Act, 2010; the Children's Act No. 8 of 2001 and the Proceeds of Crime and Anti-Money Laundering Act No. 9 Of 2009. Others include The Prisons Act, Cap 90 LoK; The Probation of Offenders Act Cap 64 LoK; The Extradition (Contiguous and Foreign Countries) Act Cap 76 LoK; and the Extradition (Commonwealth Countries) Act Cap 77 LoK.

Kenya is also a member of key international treaties and conventions and a partner of global efforts to counter both terrorism and organized crime such as the EAC, IGAD, AU, UNODC, GCTF and EAPCCO.

These legal frameworks are shared across the different government agencies of Kenya's criminal justice system. These entities are the police, the prosecution, the judiciary and the prisons. While some respondents had mixed reactions into the country's legislative framework with some pointing out that the country's criminal justice system is legislatively equipped to address the linkage between terrorism and organized crime, and others saying that such laws still need to be enacted.

The linkage between terrorism and organized crime: Experience of criminal justice actors

There are four primary government agencies involved in handling cases of terrorism and organized crime. These are the National Police Service (NPS), the Office of the Director of Public Prosecutions (ODPP), the Judiciary and the Kenya Prisons Service.

The National Police Service

It starts at several investigators and intelligence offices of the NPS. The Directorate of Criminal Investigations (DCI) is the body in charge of detecting crime, collecting intelligence and apprehending offenders of terrorism and organized crime. The key offices are the Anti-Terrorism Police Unit (ATPU), Transnational Organized Crime Unit, Anti-Narcotics Unit, and the Anti-Human Trafficking and Child Protection Unit. Other relevant DCI offices work on forensics, bomb and hazardous materials disposal, and land, bank and insurance fraud. The National Intelligence Service, a civilian agency, works with the National Police Service to address terrorism and organized crime cases.

Respondents from the NPS had investigated more cases of organized crime than

terrorism. The investigations of organized crime cases have a higher prosecution rate than those investigated for terrorism. For example, out of 10 investigated cases of orga nized crime, 6 had led to prosecution, three were ongoing and only one with no prosecution. On the other, out of 10 cases of terrorism, four had led to prosecution, two were ongoing, and four had led to no prosecution.

There were more significant linkages between human trafficking, arms trafficking, and illicit financial flows as forms of organized crime with terrorism. In an investigation of 10 case files, seven were linked to terrorism and organized crime, with the rest exclusive. The linkages were found on strategy and information, use of violence, ethnicity, funding, and use of similar money transfer channels.

These linkages had more tremendous implications as getting admissible evidence was a challenge due to the complexity of the crimes involved. In cases like these, the respondents also pointed out that interference during their investigations by interested parties dragged cases for long before being handed over to the ODPP. The interference was not explained further by the respondents. Officers also cited receiving security threats from interested parties when investigating such cases.

In addressing the linkages between terrorism and organized crime cases, the NPS offices collaborated with other government agencies through the multi-agency team approach through providing and sharing information and intelligence report.

Almost all investigators interviewed said that there was need for further and continuous technical assistance and training on terrorism and organized crime cases. This is because there is no consistency in training as these types of crime keep on evolving. Respondents pointed out that even though investigating organized crime cases is relatively direct, terrorism cases are complex, involving different planning, recruitment, radicalisation, profiling suspects, and tracing money flow. Now that there is increasing evidence suggesting the linkage of terrorism and organized crime, further technical assistance was also desired. Respondents also added a need for better coordination of actors in the criminal justice system in addressing cases of terrorism and organized crime.

Office of the Director of Public Prosecutions

Prosecutors prepare interlocutory motions to convert intelligence into evidence, search, seizure and custodial orders pending charging of suspects. Half of the

prosecutors interviewed on the ENACT study who were directly involved in terrorism, and organized crime cases were women. This indicates a more outstanding gender balance of men and women in prosecuting terrorism and organized crime cases.

Prosecutors interviewed pointed out that two had led to the conviction of four cases they were handling while the others were ongoing. Of these four cases, only one involved a juvenile, and one had been referred to witness protection. Mutual legal assistance had been requested for two of these four cases. The nature of this request was for preparing and presenting witnesses to testify via video link and requesting financial records from Vodafone South Africa.

Prosecutors pointed out that there is increasing evidence on the linkage between terrorism cases to organized crime. Most of these organized crime cases are human, arms and wildlife trafficking. For example, the weapons used in some of the wildlife trafficking offenses prosecuted in Kenya are supplied by a terror group. In cases like these, the decision to prosecute or discontinue the claim is based on law and sufficient and admissible evidence. In most cases, the terrorism burden of proof was lower unless in some exceptional cases where the terrorist group had turned to an organized crime network and executed the crime directly. Hence, the evidence used in the charge sheet was mainly from organized crime than from terrorism.

Half of the prosecutors interviewed pointed out that they are adequately trained in addressing terrorism and organized crime cases, with the other half calling for further training. Prosecutors pointed out that there is an institutional coordination system in place with other criminal justice actors in addressing linkages cases of terrorism and organized crime.

Kenya Prisons Service

Seven prison facilities, including a borstal institution, were sampled for this study. There were not many cases of prisoners serving a sentence of both terrorism and organized crime. For example, in one of the Men's prison facilities, a prisoner was convicted on a case in 2016/2017 that involved terrorism, poaching, and piracy. In another Men prison, there was a terrorist prisoner who was released and went back to Somalia. The released terrorist came back, and he was gunned down in Kilifi county. The prison assisted in tracking this released prisoner by using his visitor's information details. This also showed the need for collaboration between prisons and

other actors of the criminal justice system.

Rehabilitation/skills/disengagement programs for terror and organized crime convicts

Respondents pointed out that soft pieces of training are provided to organized crime prisoners. This includes playing cards, watching television, reading books and psycho-social support. For women prisons, these programs included bead working and weaving. Respondents pointed out that for a prisoner to attend a program, they must be interested in it of which most prisoners were not. Other training included computer and mechanics. But for example, like vehicle mechanics, the practical training is still using an old Bedford diesel engine instead of the new auto mechanics currently in place. When prisoners served their sentence and left the prison, this gained skill didn't help them much. Notably, in one prison, prisoners undergo Kenya formal school curriculum, and they had prisoners who had completed their Master's degrees.

For terrorism prisoners, respondents interviewed pointed out that the preferred program for terror convicts is disengagement and not deradicalization. Respondents explained that deradicalization focuses on having alternative programs offered to a terrorist. But it has never worked well. For example, the respondents pointed out that rolling out a masonry program for terrorist prisoners didn't work well. There is a need to disengage the prisoner first from terrorism and then introduce other programs that they might be interested in at a later stage. This is the reason why Kenya doesn't have deradicalization but disengagement programs in prisons.

Disengagement programs are conducted by the National Counter-Terrorism Centre (NCTC) through a 7-committee member composed of different stakeholders in the country.

Unfortunately, there were not enough tailor-made programs for the officers manning terror prisoners. Special training was pointed out as highly necessary.

Some programs were discontinued due to the risk they posed. For example, in a tailoring program, the prisoners used parts of the sewing machine, such as needles as weapons.

Terror prisoners do sports programs and only among themselves. Most were obsessed with religious programs as rehabilitation, but they knew more than the religious leaders such as imams and pastors sent to them. There is a gap as the rehabilitation is done by prison officers who know the fundamental part of religion. Respondents recommended having well-versed religious leaders offer spiritual

rehabilitation as prison officers have only the basic knowledge. Respondents pointed out that most terrorist prisoners accept their wrongdoing once in prison.

Handling of foreign prisoners

Some of these prisoners convicted of terrorism and organized crime were foreigners. For example, some Somali nationals were convicted for piracy and terrorism charges, and language barrier to their communication in prison. Other nationals from the East and Horn of African countries were convicted for human smuggling, especially to the Southern African countries with Kenya as a transit. These foreign prisoners, once released, were handed over to their embassies in Kenya.

Handling of recidivists prisoners

Terrorism and organized crime prisoners serve long terms, so they do not return once they leave. Most terrorist prisoners become targets by the terror groups on allegations of being informants. Due to this, some disappear, and it becomes difficult to track them. Others are assimilated back to society and start a different life. Respondents pointed out that a follow-up program with prisoners who are released is necessary.

Coordination of the prisons and other criminal justice actors

Respondents also pointed out a need for better coordination of information sharing between other actors in the criminal justice system and the prisons. The core mandate of prisons is just holding prisoners, but emerging issues call for more inclusivity of prisons in the criminal justice system. Prisons spend the most time with prisoners though most historical information of the prisoner is with the other actors of the criminal justice system.

Respondents also suggested a need for having a single command system of the criminal justice system. There is also a need to have a single-file system of prisoners shared across the criminal justice actors, including the prisons.

Prison equipment was still backdated and had not adopted the new equipment used for crowd control, manning prisoners, scanners, among others. For example,

most prisons used clubs to man the prisoners instead of electric shock gadgets, night visions, surveillance, listening devices, and phone jamming devices.

Prisoners are aware of these gaps and have exploited them to their advantage, for example, escaping, harming other prisoners, and allowing contraband goods inside the prisons.

CONCLUSION

The nexus is perhaps the biggest growing security threat that the East Africa region faces. Terrorist groups are increasingly controlling territories with vast resources, and this access has transformed the groups into an organized criminal network traversing different countries in the region.

Countries continue to combat terrorist groups using only hard anti-terror tactics such as the use of the military. In contrast, the groups continue to transform themselves into transnational organized crime groups. Responses must blend both hard and soft approaches that can include tracing the flow of money from these 'nexus' groups.

The burden of proof for terror cases has also remained a challenge for criminal justice system actors. Now with terrorists working with organized criminal groups, the burden of proof before the court of laws is even complex. Nexus cases should incorporate prosecution involved investigations at the onset, as the case of the Kenya Dusit2 terror attack suggested.

Countries in the region should also cooperate in the investigation and prosecution of nexus cases. The newly signed agreement on 15 October 2021 between Central and East African States on Police Cooperation and Criminal Matters is in force and can be used as a framework for cooperation. The Agreement has the provision of exchange and sharing of information and data, procedures for the handing over of suspected criminals, exhibits and foreign missions, and treatment of wanted and apprehended suspects.

Last, crime-proofing procurement processes could serve as a deterrence for terrorist groups infiltrating economic sub-sector such as the food industry. Rampant corruption, conflict of interest have enabled private sector corruption and these governance vulnerabilities are synergizing vectors for terrorists and organized criminal groups to nexus in perpetrating criminal activities.

References

De Castanedo, I.C. (2021). Narco Links Between South America And Africa. Grey Dynamics, April 15, 2021. https://www.greydynamics.com/narco-links-between-south-america-and-africa/

Eastern Africa Police Chiefs Cooperation Organization Counter-Terrorism Centre of Excellence (2021). https://eapcco-ctcoe.org/

Enhancing Africa's response to transnational organised crime (2017). Transnational organised crime in Africa. ENACT, 2017, https://enact-africa.s3.amazonaws.com/site/uploads/enact-brochure-eng.pdf

Forest, J. (2011). Al-Qaeda's influence in sub-Saharan Africa: myths, realities and possibilities, *Perspectives on Terrorism*, 5:3-4, 2011, 66.

Global Counterterrorism Forum (2021). Hague good practices on the nexus between transnational organised crime and terrorism. GCTF, https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2018/GCTF-Good-Practices-on-the-Nexus_ENG.pdf?ver=2018-09-21-122246-363

Global Counterterrorism Forum (2021). Resources and framework documents. GCTF, https://www.thegctf.org/Resources/Framework-Documents/Policy-Toolkits/Nexus-between-Transnational-Organized-Crime-and-Terrorism

Global Counterterrorism Forum and United Nations Interregional Crime and Justice Research Institute (2019). Policy toolkit on the Hague good practices on the nexus between transnational organized crime and terrorism, GCTF, https://www.thegctf.org/LinkClick.aspx?fileticket=GZAXnYJWfuQ%3d&portalid=1

Global Initiative against Transnational Organized Crime (2018). Organized Crime: A growing concern on the Security Council Agenda. GITOC, March 2, 2018. https://globalinitiative.net/analysis/scresolutions/

Jaitman, L. & Machin, S. (2016). Crime and violence in Latin America and the Caribbean: towards evidence-based policies. Centre for Economic Performance, London School of Economics and Political Science. https://cep.lse.ac.uk/pubs/download/cp461.pdf

Luhnow, D. (2014). Latin America Is World's Most Violent Region. The Wall Street Journal, April 11, 2014. https://www.wsj.com/articles/SB10001424052702303603904579495863883782316

Makarenko, T. (2010) The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism, 6(1), *Global Crime*, pp 129-145, 2010.

Mohammed, S., Mohammed, Y.K. & the Nigerian State: Historicizing the Dynamics of Boko Haram Phenomenon, Kaduna Journal of Liberal Arts 5(1), 2011, 30.

Nellemann, C.; Henriksen, R., Pravettoni, R., Stewart, D., Kotsovou, M.,

Schlingemann, M.A.J, Shaw, M. and Reitano, T. (Eds). 2018. World atlas of illicit flows. A RHIPTO-INTERPOL-GI Assessment. RHIPTO -Norwegian Center for Global Analyses, INTERPOL and the Global Initiative Against Transnational Organized crime. https://globalinitiative.net/wp-content/uploads/2018/09/Atlas-Illicit-Flows-FINAL-WEB-VERSION-copia-compressed.pdf

Neumeister, C. & Cooper, S. (2019). Money tree, teak and conflict in South Sudan. C4ADS, 2019, p6. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5df2b87d4c2e38505cf22725/1576188053567/Money+Tree.pdf#page=6

Petrich, K. (2019). Cows, charcoal, and cocaine: al-Shabaab's criminal activities in the Horn of Africa, *Studies in Conflict & Terrorism*. DOI, October 17, 2019, https://doi.org/10.1080/1057610X.2019.1678873

Reuters (2021). Ugandan military arrests man suspected of planning suicide bombing. Reuters, August 27 2021, https://www.reuters.com/world/africa/ugandan-military-arrests-man-suspected-planning-suicide-bombing-2021-08-27/

Roberts, I. (2021). An Unholy Alliance Links between Extremism and Illicit Trade in East Africa, Counter extremism, March 29, 2021, https://www.counterextremism.com/content/unholy-alliance

Ryabchiy, K. (2018) Rethinking the Crime-Terror Continuum in the 21st Century: Post-9/11 to the Present, *University of Pretoria*, 2018.

Shaw, M. (2017). Organised crime in Africa/Africa's changing place in the global criminal economy. ENACT, September 27, 2017. https://enactafrica.org/research/continental-reports/africas-changing-place-in-the-global-criminal-economy

UN Group of Experts on the DR Congo (2011). *Final report of the Group of Experts on the Democratic Republic of the Congo*, S/2011/738, p.29.

United Nations Office on Drugs and Crime (2018). Module 16: Linkages between organised crime and terrorism. https://www.unodc.org/e4j/en/organized-crime/module-16/key-issues/references.html

United Nations Office on Drugs and Crime (2021). Supporting the EAPPCO Regional Counter-Terrorism Centre of Excellence, https://www.unodc.org/easternafrica/what-we-do/terrorism-prevention/supporting-the-eapcco-counter-terrorism-centre.html

United Nations Office on Drugs and Crime (2021). UNODC and Eastern African Member States Joining Forces to Counter Financing of Terrorism and Links to Organized Crime, https://www.unodc.org/easternafrica/en/Stories/unodc-and-eastern-african-member-states-joining-forces-to-counter-financing-of-terrorism-and-links-to-organiz

ed-crimeunodc-and-eastern-african-member-states-joining-forces-to-counter-financing-of-terrorism-and-links-to-organized-crime.html
United Nations Security Council (2014). Letter dated 10 October 2014 from the Chair of the Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea addressed to the President of the Security Council, 13 October 2014.
United Nations Security Council (2014). Resolution 2195 (2014) / adopted by the Security Council at its 7351st meeting, on 19 December 2014. https://digitallibrary.un.org/record/785567?ln=en
United Nations Security Council (2015). Letter dated 9 October 2015 from the Chair of the Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea addressed to the President of the Security Council, 19 October 2015.
United Nations Security Council (2016). Resolution 2322 (2016) / Adopted by the Security Council at its 7831st meeting, on 12 December 2016. https://digitallibrary.un.org/record/785567?ln=en
United Nations Security Council (2017). Extending arms embargoes on Somalia, Eritrea, Security Council adopts Resolution 2385 (2017) by 11 votes in favour, 4 abstentions, SC/13065. UNSC, November 14, 2017, https://www.un.org/press/en/2017/sc13065.doc.htm
United Nations Security Council (2017). Resolution 2370 (2017) / Adopted by the Security Council at its 8017th meeting, on 2 August 2017. https://undocs.org/pdf?symbol=en/s/res/2370(2017)
United Nations Security Council (2019). Resolution 2482 (2019) / Adopted by the Security Council at its 8582nd meeting, on 19 July 2019. https://undocs.org/S/RES/2482(2019)
United States Government Information (2014). The 9/11 commission report: the foundation of the new terrorism, GovInfo, July 22, 2004, https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT-8.pdf
Wang, P. (2010). The Crime-Terror Nexus: Transformation, Alliance, Convergence, 6(6), *Asia Social Science*, 2010

Does Analysis of Competing Hypotheses (ACH) Really Mitigate Cognitive Biases? Practical Implications for Intelligence Analysts and Criminal Investigators

*Henrique Britto de Melo**
MSc program in Forensic Science (Universidade de Pernambuco - UPE)
Brazilian Academy of Criminal Sciences (ABCCRIM)

Abstract

This article discusses controversies about the Analysis of Competing Hypotheses (ACH) efficacy. The technique was developed by the Central Intelligence Agency (CIA) to mitigate cognitive biases and improve critical thinking, becoming one of the most popular analytical tools in the intelligence community. Despite its pervasiveness, ACH has some limitations and does not perform well in experimental tests. The findings suggest that the technique is not an effective way of mitigating analysts' biases and does not necessarily improve their reasoning. This might happen because of multiple factors (e.g. problems in implementing the technique, theoretical flaws, and vagueness of its instructions). However, this is not necessarily a reason to abolish the use of ACH in intelligence and investigative activities. With that in mind, the paper suggests some practical improvements that might lead to better results. These suggestions must be submitted to further experimental testing, which is related to the other aim of the article: to encourage the use of randomized experiments to test analytical techniques in the intelligence and investigative contexts.

Keywords

Analysis of Competing Hypotheses (ACH); Cognitive bias; Intelligence analysis; Investigative reasoning; Structured Analytic Techniques (SATs)

* Direct correspondence to Henrique Britto de Melo; henriquebrittodemelo@gmail.com
* http://dx.doi.org/10.36889/IJCJ.2021.011
* Received 16 October 2021; Revised 20 November 2021; Accepted 15 December 2021
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 2, December 2021, 115-129

INTRODUCTION

One important attribution of intelligence analysts in developing explanations for current situations and predictions about future scenarios (Dhami et al., 2019). To do that, they must generate plausible hypotheses based on the available data and then produce reports with their inferences. Despite seeming like an objective task, hypothesis generation is a difficult process because of the complex phenomena that analysts try to explain and predict. In addition, the available information is often fragmented and of questionable reliability. There is no precise way of predicting future events such as governors' decisions, military tactics, and criminal trends, for example. And on top of that, the intelligence activity involves other actors that might be working to hinder the information gathering, thereafter harming the subsequent analysis. This is another factor that makes intelligence analysis a complex job. This myriad of challenges is well described by Viale (2021):

> The task of analysis is made difficult partly because the human mind is limited in terms of attention, perception, memory, and processing capacity, and partly because the task itself can be extremely constraining and demanding. Indeed, there may be not enough relevant data or there may be large volumes of data, the credibility of data sources may vary, the data may be formatted in different ways (e.g., structured/ unstructured, textual/ visual/ audio), it may be ambiguous, unreliable, and sometimes intentionally misleading, and there may be time pressure and high stakes involved. This is further compounded by the lack of feedback which limits learning on how to perform analytic tasks.

Hypothesis generation can be cognitively challenging. As explained by Passmore et al. (2015), this is not a linear process and the analysts must revisit earlier inferences to change or discard them and generate new ones based on further discoveries. It is also important to notice that hypothesis generation and evidence-gathering feedback into each other. The inferences will guide investigations and will point to what path must be followed while the acquired information will serve as a filter to decide which hypotheses are "good" and which ones are not. However, this raises some questions: What makes an inference good or bad? How to distinguish them rationally and objectively? Such problems are the foundation of Structured Analytic Techniques (SATs). The term refers to several analytic tools that were developed to deal with

these and other challenges within the intelligence activity. According to Chang et al. (2017): "At their core, SATs are a set of processes for externalizing, organizing, and evaluating analytic thinking"

Theoretically, they can do that by helping users to display complex data in structured models, allowing them to manipulate, rearrange and interpret the information more efficiently. SATs can also make the process of hypothesis generation more transparent and open to scrutiny. This can be helpful to encourage group discussions about a specific line of thinking, to audit the analysis process searching for mistakes, and also to evaluate analysts' performance. In conclusion, the purpose of the SATs is to improve users' objectivity while making them accountable for the steps taken, which can theoretically be accomplished because of the externalization of thinking required by the tools. The use of a structured technique allows a systematic screening for reasoning errors and it makes it theoretically possible to retrace the steps taken by the analysts to see how they arrived at specific conclusions.

Currently, SATs are employed for a multitude of tasks, dealing with past, present, and future scenarios. They are used in a variety of endeavors such as criminal investigations, geopolitics, combating transnational organized crime, counterterrorism, and chemical warfare (Chang et al., 2017; Hart, 2014). One of the most known and taught SATs is the Analysis of Competing Hypotheses (ACH). Developed by the CIA, the tool is applied to mitigate cognitive bias and it is one of the most recommended SATs in the intelligence community (Coulthart, 2017; Whitesmith, 2018; Dhami et al., 2019; Jones, 2017). "Cognitive bias" refers to a series of inclinations in our reasoning that harm our objectivity and can lead to systematic errors. One of the most famous cognitive biases is confirmation bias, which is a tendency to focus on evidence that supports our existing beliefs and to give less attention to contrary information (Artner et al., 2016). This makes us more prone to see what we already believe to be true. According to the literature, analysts can present biases (Dhami et al., 2019), but this is not a well-understood phenomenon. The failure to generate hypotheses effectively and rationally discard them can damage further steps of the analytical process and lead to inaccurate conclusions, often leading to intelligence mistakes (Whitesmith, 2018). Therefore, it is necessary to understand these cognitive shortcomings to develop effective strategies for reducing bias in the intelligence reality.

ACH tries to deal with this problem with a systematic approach to inferential reasoning and users must follow an 8 step process (Jones, 2017):

(1) Identify hypotheses to be considered.
(2) List significant evidence and arguments.
(3) Use a matrix to analyze the 'diagnosticity' of evidence and arguments for each hypothesis.
(4) Refine the matrix, revising hypotheses or deleting non-diagnostic evidence and arguments.
(5) Draw tentative conclusions about the relative likelihoods of the hypotheses.
(6) Analyze conclusions for sensitivity to misleading or misinterpreted evidence.
(7) Report conclusions.
(8) Identify milestones for future observation.

These steps can theoretically help analysts avoid confirmation bias because the first recommendation is to identify multiple hypotheses that are consistent with the data. This could prevent them from pursuing a specific explanation of their preference. In addition, the guidelines propose a classification of hypotheses with a critical perspective, ranking them in terms of consistency. Finally, analysts must also seek ways of confronting the inferences with the reality to test which ones should remain being considered.

A central aspect of ACH is that users must seek to disprove their hypotheses rather than confirm them, a process called eliminative induction. The conjectures with fewer inconsistencies will then be rated as more plausible. Such an approach can allegedly antagonize the confirmation bias by pushing the analysts to be skeptical about their inferences. According to Mandel et al. (2018), the eliminative induction used in ACH may have been inspired by Karl Popper's idea that hypotheses falsification is important for the scientific method.

Despite being developed and usually used in the intelligence context, we can discuss possible applications of ACH in the criminal investigations scenario. Baechler et al. (2020) argue that intelligence and forensic activities must be seen as similar processes, concluding that there are no qualitative differences between intelligence and evidence. As they state, "both are a piece of information that has to be combined and put into perspective with alternative pieces of information to understand criminal problems, solve crimes and support decision-making at various levels". Houck (2020) describes similar challenges that both investigators and analysts must deal with: Limited or incomplete information; Unreliable, conflicting, or ambiguous information;

Denial and deception; Information in the context of volatile or unknowable social situations; Work within limited time frames; Collection of appropriate information and Identify information gaps.

Houck (2020) argues that criminal investigators can benefit from structured analytical techniques because they also face challenges regarding collecting, organizing, and communicating information. Major investigations involve several professionals from multiple areas of expertise in different agencies, so it becomes difficult to gather and transmit information effectively. The author recommends the use of ACH in criminal investigations since this line of work has so many similarities with intelligence activity.

Does ACH have scientific validation?

From an epistemological perspective, there are problems with the technique. As stated above, ACH proposes the use of eliminative induction because it allegedly mitigates confirmation bias by making users refute their explanations. However, the superiority of this approach has not been proven. There is no evidence that eliminative induction will reduce the probability of biased hypotheses being generated. According to Mandel et al. (2018), this might be the result of a misunderstanding of the falsification principle proposed by Karl Popper. This principle illustrates the impossibility of confirming a generalization such as the popular example of “all the swans are white”. One didn't examine all the swans in the world to make this statement and it takes only one black swan to refute this proposition. However, in the intelligence activity, there are rare situations when a generalization of this kind will be made and possibly refuted by a single event and/or information. In conclusion, there are several problems with trying to apply popper’s falsification principle to techniques such as ACH.

And how well does ACH perform in experimental evaluations? First, it is important to know that the number of experimental studies of ACH is small. With that in mind, we can analyze the scarce results found in scientific literature. Despite being one of the most popular analytical techniques in the intelligence community, ACH offers little evidence of its efficacy. A study conducted by Whitesmith (2018) found that the tool was not effective in reducing cognitive bias and serial position effects. Mandel et al. (2018) showed results pointing in the same direction. According to the researchers, the control group was more accurate at hypothesis development than the

group using ACH. Whitesmith (2020) reported no significant differences between groups using ACH and other methods such as serial order. Chang et al. (2017) showed that the technique was not effective in reducing confirmation bias in intelligence professionals. An experiment conducted by Maegherman et al. (2020) to test ACH did not show bias mitigation. Dhami et al. (2019) showed that the group using ACH was not more successful than the control group in choosing the right hypothesis in an experiment. The authors also gathered other sources stating that ACH is not effective in improving participants' reasoning.

Despite multiple sources showing that ACH is not necessarily an effective technique, these studies have several limitations. They generally have a small number of participants and in several cases, they don't even work in the intelligence field (Dhami et al., 2019). This leads to results with questionable statistical relevance (because of small samples) and no ecological validity since they are not examining real intelligence analysts' reasoning in most cases (Dhami et al., 2019). Some studies are using real analysts (Chang et al., 2017; Mandel et al., 2018) but they are scarce and suffer from the small sample problem. However, these limitations are not a sign that ACH should be used indiscriminately. In fact, to the knowledge of the author, no systematic reviews are supporting the technique and it lacks scientific validation.

From the practical perspective, ACH does not show how it would mitigate cognitive biases. Analysts are instructed to generate as many plausible hypotheses as possible, and then evaluate which ones have fewer inconsistencies to select them. However, the technique does not provide a detailed way of doing that. Users are not instructed on how they must develop inferences in the first place, and there is not a reference system to rank them (Mandel et al., 2018). If there aren't specific instructions on how to generate and filter hypotheses, users can still follow their own beliefs and biases when using the technique. For example, ACH's first step (Identify hypotheses to be considered) does not prevent analysts from generating inferences based on what they believe to be more realistic. In addition, they can fall within the search satisficing bias, which is a tendency to stop looking for alternative explanations once a plausible hypothesis is developed (Viale, 2021). In step 3 (Use a matrix to analyze the 'diagnosticity' of evidence and arguments for each hypothesis), analysts still can judge a piece of evidence that they believe to be strong as more diagnostic than other ones.

Another problem regarding the use of ACH is that analysts sometimes have to

provide statements with verbal probabilities such as " this scenario is highly probable". There are two main pitfalls with this practice: first, users may rank hypotheses as more probable if they can easily remember similar situations that occurred in the past (availability bias) (Viale, 2021). Second, it could be dangerous to communicate verbal probabilities without relying on actual statistical estimates. Since there isn't a consensus on terms such as "highly probable", they can have different meanings to different analysts (Dhami et al., 2015). How it is possible to categorize some phenomenon as "highly probable" without having quantitative data to support this claim? Probabilistic estimates need a previous quantification of a frequency to be useful here. Let's take the following case as an example: In a study conducted by Chopin et al. (2019), the authors found that sexual offenders left semen at the crime scene in 73,94 % of the cases. With this information, we can estimate that it is "very likely" that investigators will find semen in similar crimes within the region of the study.

Nonetheless, it is necessary to acknowledge that in several cases it's not possible to provide percentages in intelligence analysis. The circumstances of the job are complex and sometimes unpredictable, therefore hindering statistical analysis. But on the other hand, generating and ranking hypotheses without doing that gives plenty of space for a judgment based on prior beliefs and biases. This leads to another question: how the analysts judge what is more or less consistent? There is no unified definition of what this means in the intelligence context, and giving instructions to evaluate how consistent a hypothesis is can be dangerous if some delimitations were not made. Instead of saying exactly how analysts should assess consistency, the technique allows them to use their idiosyncrasies to decide what is consistent and what is not (Mandel et al., 2018).

As we can see, there are still multiple problems with ACH, which raise doubts about its scientific basis. To sum up, the claims made in defense of the tool and their respective shortcomings, a table is available below:

Table 1: Claims in favor of ACH and their respective limitations

Claim	Limitation
ACH can mitigate cognitive biases because it recommends the generation of multiple hypotheses	The technique does not specify how to generate the hypotheses and it allows analysts to make inferences based on their preexistent beliefs. The claim that ACH reduce cognitive biases lacks experimental validation
ACH mitigates confirmation bias by encouraging users to seek evidence that may disprove their theories instead of trying to confirm them (eliminative induction)	Eliminative induction does not prevent analysts from discrediting the weight of disconfirming evidence and focusing on the confirming ones
ACH makes it possible to identify cognitive biases because ideas are being put on a table, allowing peer review	Externalization of thinking can provide some degree of clarity about the reasoning process and subsequent peer review. However, it does not precisely show the steps taken in hypothesis development and ranking, making it difficult to track cognitive biases
ACH provides an objective way of judging hypotheses by ranking them according to their consistency with the evidence	There are no specific guidelines on how to evaluate the hypotheses' consistency and there is not a clear definition of what "consistent" means. Analysts can end up unconsciously using their own beliefs and biases to judge what is consistent with their hypotheses and what is not
Analysts trained with ACH perform better at developing hypotheses than those who weren't trained with the technique	There is little empirical data to confirm that. The scarce existent data indicate that analysts trained with ACH usually have an equal or slightly worse performance than those who weren't trained with the technique

Challenges in implementing debiasing strategies

The ACH and the other Structured Analytic Techniques can also be described as "debiasing strategies". This is an umbrella term that refers to all tools that are used to mitigate cognitive bias and enhance critical thinking. They are applied in several fields of knowledge, going from medical diagnosis (Croskerry et al., 2013) to criminal investigations (Fahsing et al., 2021). However, the efficacy of such techniques is at least dubious. This might happen because it's difficult to identify and target cognitive biases since they are not explicit (Fahsing et al., 2021).

According to Croskerry et al. (2013), the implementation of debiasing strategies

must walk a path full of obstacles: “from a state of lack of awareness of bias to awareness, to the ability to detect bias, to considering a change, to deciding to change, then initiating strategies to accomplish change, and finally, maintaining the change.” This lack of awareness and ability to detect one's own bias is often referred to as the “bias blind spot”, and it occurs without harming the individual's capacity to acknowledge bias in others (Viale, 2021). This represents a major challenge in debiasing strategies implementation because it's necessary to convince professionals that 1- they are susceptible to biases and 2- that they need to learn how to overcome them. Teaching them debiasing techniques might not work because there's no guarantee that users will adhere to the techniques and apply them correctly. In addition, we don't know how long the results of a technique will last, in the case of effectively reducing biases (Viale, 2021).

Debiasing strategies are often studied from a dual-thinking perspective. This approach considers that human reasoning manifests itself by 2 different processes, usually named system 1 and system 2 (Frankish, 2010). System 1 refers to a thinking process that is subconscious and intuitive, while system 2 is conscious, analytical, and goal-oriented. Since system 1 does not obey rules of logic and is a fast way of thinking that relies on intuition, it is often referred to as “the culprit” of reasoning errors because of an apparent proneness to biases.

To manage this problem, debiasing strategies try to make users more cautious about the first and spontaneous inferences that pop up in their minds since they can be a product of the “flawed” system 1. There are tools specifically developed to assess this problem (e.g. forcing techniques) that aim to make analysts “go further” in hypothesis generation, theoretically stimulating the analytical process of the system 2. This dual-thinking model has become pervasive in the scientific literature regarding cognitive bias, but there are some controversies with this approach. For instance, some scholars argue that intuitive and analytical thinking can occur simultaneously and systems 1 and 2 might not be categorically distinct. Opposing this duality, there is another view that considers a continuum with different degrees of both analytical and intuitive thinking, which undermines the idea that a reasoning process can fall under only one of these two categories (Viale, 2021).

It is also important to stress that some techniques can also generate other biases while trying to mitigate the targeted ones, causing iatrogenic effects. For example, trying to avoid overconfidence can lead analysts to be underconfident, harming their

reasoning in the opposite way (Viale, 2021; Chang et al., 2017). However, the literature assessing this collateral damage is scarce and this dual aspect of biases is often under-discussed.

Future directions

The use of a visual analytic technique such as ACH is not necessarily a problem. Literature shows that analyzing and manipulating visual information can be an effective way of thinking and solving problems (Passmore et al., 2015; Sunde, 2020) and there is evidence that considering competing scenarios can be an effective way to improve reasoning in some cases (Fahsing et al., 2021). However, it is necessary to conduct more studies about their implementation in investigative and intelligence scenarios. As stated in this article, ACH has several limitations and might not be ready to be used by intelligence analysts and investigators. Nonetheless, some directions can offer possible improvements for the technique. Some of these suggestions are described below:

Serious games - Some studies show that computer games can be a powerful tool to help with debiasing if they are specifically developed for that purpose (Viale, 2021). A study conducted by Morewedge et al. (2015) showed that a single intervention with a computer game was successful in reducing biases, and the reduction lasted for at least 2 months after the study. This research also used an intervention based on a video for another group, resulting in smaller debiasing effects. One important finding of the study is that the improvements in decision-making were extended to other contexts, showing that debiasing strategies might have effects in domains not related to the intervention. The efficacy of computer games might be caused by immediate feedback through dynamic interactions, which allow users to observe the consequences of their choices instantaneously. They also can mimic real-life situations, allowing users to think and make decisions that can help them outside the virtual landscape (Poos et al., 2017).

Structured investigative models - This has practical implications for both analysts and forensic scientists because, according to the authors, they are executing essentially the same tasks (i.e. collecting and assessing information to use it for explaining

events). This approach allows the use of structured models developed to aid police investigations, such as the Structured Hypothesis Development in Criminal Investigation (SHDCI), developed by Sunde (2020). The SHDCI is a step-by-step visual tool that also stimulates the consideration of opposite explanations for each inference. Users are instructed to create hypotheses and then frame them in opposite ways (e.g. considering that no crime was committed to counterbalance investigators' inclinations to think easier about criminal explanations). Nonetheless, these resources need further experimental testing as well. The SHDCI steps could theoretically be added to ACH's process, making its instructions more specific. For example, some questions developed by Sunde (2020) could guide the early stages of hypothesis generation: "What criminal offenses may have occurred based on the information in the case?"; "What other criminal offenses may have occurred?"; "What non-criminal circumstances may have occurred, based on the information in the case?"; "What could be reasons for him/her being innocent, based on the information in the case?".

Significance, reliability, independence, and patterns (SRIP) evaluation - Eck & Rossmo (2019) recommend the acronym SRIP to help analysts/ investigators to evaluate evidence more objectively. This might mitigate the lack of clear guidelines on how to judge information before using it to develop hypotheses. *"S"* stands for significance, which entails evaluating the probability of the evidence being present in that specific scenario (e.g. "what's the probability of the suspect's DNA being in the crime scene beyond he/she committing the crime? It could be there for other reasons?"). *"R"* refers to the reliability, which reminds the user of questioning how trustful the piece of evidence is. *"I"* stands for independence, or how derivative one piece of evidence is from the rest. *"P"* stands for patterns, a principle to remind users to analyze evidence by comparing it to the other pieces of information already gathered because it may be dangerous to evaluate something in a vacuum. The SRIP acronym is a more specific set of guidelines to evaluate data and can be added to the ACH to make it more clear. This tool can be particularly useful in helping analysts and investigators when they face new evidence and/or information. With this acronym, they can reason about the aspects of the facts and evaluate them in a more structured manner. Since ACH does not prevent users from disproportionately weighing new information, the SRIP tool could make this process more objective with its clear criteria for evaluation.

CONCLUSION

This paper showed some practical and conceptual limitations of the ACH and brought some suggestions for improvement. However, there must be a dialogue between researchers and intelligence professionals for the improvements to occur. In addition, this dialogue is necessary for developing more scientifically based analytical techniques, therefore making this cooperation paramount for the evolution of intelligence activity.

Despite several theoretical and practical pitfalls, some debiasing techniques are still used in intelligence analysis without systematic evaluation (Dhami et al., 2015; Coulthart, 2017; Artner et al., 2016). Intelligence professionals must be cautious about the claims of efficacy of the ACH and must develop stronger relationships with scholars to create and implement evidence-based analytical techniques. There is an alarming lack of research regarding SATs effectiveness in the intelligence context, which can potentially cause catastrophic repercussions. Since the intelligence activity deals with highly sensitive information about matters of national and international security, it is a paradox that the professionals analyze such formation using techniques that are not scientifically validated yet.

Despite some promising results, the future directions suggested in his article need more experimental evaluation. This type of research design is necessary to see what works in mitigating cognitive biases and improving critical reasoning. ACH and other SATs must be tested with experimental designs to evaluate their efficacy. Randomized controlled trials are an objective way of determining if an intervention has promising impacts because of how they use chance in their favor. They randomly separate participants into two or more groups, and then also randomly choose which group will receive the intervention and which one will not (control group). This is important to isolate the results from spurious influences, therefore showing that the differences found between the groups are probably due to the intervention (Prancan, 2002).

In addition, it is important to acknowledge that there is not a technique completely bias-free (Jones, 2017). The aim must be to gradually reduce the flaws of the tools used by analysts to optimize them *ad infinitum*. This is the core of the scientific method, which fits the intelligence activity because of the similarities between these fields. As stated by Dhami et al. (2015), intelligence analysis "involves generating and testing hypotheses and accurately characterizing the degrees of uncertainty in both the evidence and conclusions reached." This points to a need for a scientific approach to developing and testing analytical techniques in this field.

References

Artner, S., Girven, R. S., & Bruce, J. B. (2016). *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1408.html

Baechler, S., Morelato, M., Gittelson, S., Walsh, S., Margot, P., Roux, C., & Ribaux, O. (2020). Breaking the barriers between intelligence, investigation and evaluation: A continuous approach to define the contribution and scope of forensic science. *Forensic Science International*, *309*(309), 110213. https://doi.org/10.1016/j.forsciint.2020.110213

Chang, W., Berdini, E., Mandel, D. R., & Tetlock, P. E. (2017). Restructuring structured analytic techniques in intelligence. *Intelligence and National Security*, *33*(3), 337–356. https://doi.org/10.1080/02684527.2017.1400230

Chopin, J., Beauregard, E., Bitzer, S., & Reale, K. (2019). Rapists' behaviors to avoid police detection. *Journal of Criminal Justice*, *61*(61), 81–89. https://doi.org/10.1016/j.jcrimjus.2019.04.001

Coulthart, S. J. (2017). An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques. *International Journal of Intelligence and CounterIntelligence*, *30*(2), 368–391. https://doi.org/10.1080/08850607.2016.1230706

Croskerry, P., Singhal, G., & Mamede, S. (2013). Cognitive debiasing 2: impediments to and strategies for change. *BMJ Quality & Safety*, *22*(Suppl 2), ii65–ii72. https://doi.org/10.1136/bmjqs-2012-001713

Dhami, M. K., Belton, I. K., & Mandel, D. R. (2019). The "analysis of competing hypotheses" in intelligence analysis. *Applied Cognitive Psychology*, *33*(6), 1080–1090. https://doi.org/10.1002/acp.3550

Dhami, M. K., Mandel, D. R., Mellers, B. A., & Tetlock, P. E. (2015). Improving Intelligence Analysis With Decision Science. *Perspectives on Psychological Science*, *10*(6), 753–757. https://doi.org/10.1177/1745691615598511

Eck, J. E., & Rossmo, D. K. (2019). The new detective. *Criminology & Public Policy*, *18*(3), 601–622. https://doi.org/10.1111/1745-9133.12450

Fahsing, I. (2016). *The Making of an Expert Detective Thinking and Deciding in Criminal Investigations*. https://gupea.ub.gu.se/bitstream/2077/47515/1/gupea_2077_47515_1.pdf

Fahsing, I., Rachlew, A., & May, L. (2021). Have you considered the opposite? A debiasing strategy for judgment in criminal investigation. *The Police Journal: Theory, Practice and Principles*, 0032258X2110388. https://doi.org/10.1177/0032258x211038888

Frankish, K. (2010). Dual-Process and Dual-System Theories of Reasoning. *Philosophy Compass*, *5*(10), 914–926. https://doi.org/10.1111/j.1747-9991.2010.00330.x

Hart, J. D. (2014). *The Analysis Of Competing Hypotheses (Ach) In The Assessment Of Chemical Warfare Activities*. National Defence University.

Houck, M. M. (2020). Improving Criminal Investigations with Structured Analytic Techniques. *Advanced Sciences and Technologies for Security Applications*, 123–159. https://doi.org/10.1007/978-3-030-41287-6_7

Jones, N. (2017). Critical epistemology for Analysis of Competing Hypotheses. *Intelligence and National Security*, *33*(2), 273–289. https://doi.org/10.1080/02684527.2017.1395948

Lockhart, J. J., & Satya-Murti, S. (2017). Diagnosing Crime and Diagnosing Disease: Bias Reduction Strategies in the Forensic and Clinical Sciences. *Journal of Forensic Sciences*, *62*(6), 1534–1541. https://doi.org/10.1111/1556-4029.13453

Maegherman, E., Ask, K., Horselenberg, R., & Koppen, P. J. (2020). Test of the analysis of competing hypotheses in legal decision-making. *Applied Cognitive Psychology*, *35*(1). https://doi.org/10.1002/acp.3738

Mandel, D., Karvetski, C., & Dhami, M. (2018). Boosting intelligence analysts' judgment accuracy: What works, what fails? *Judgment and Decision Making*, *13*(6), 607–621.

Morewedge, C., Symborski, C., Scopelliti, I., & Quinn, M. (2015). Debiasing Decisions: Improved Decision Making With a Single Training Intervention. *Behavioral and Brain Sciences*, *2*(1), 129–140. https://doi.org/DOI: 10.1002/acp.3738

Passmore, P. J., Attfield, S., Kodagoda, N., Groenewald, C., & Wong, B. L. W. (2015). Supporting the Externalisation of Thinking in Criminal Intelligence Analysis. *2015 European Intelligence and Security Informatics Conference*. https://doi.org/10.1109/eisic.2015.35

Pherson, R. H., & Heuer, R. J. (2021). *Structured Analytic Techniques for Intelligence Analysis* (3rd ed.). SAGE Publications.

Poos, J. M., van den Bosch, K., & Janssen, C. P. (2017). Battling bias: Effects of training and training context. *Computers & Education*, *111*, 101–113. https://doi.org/10.1016/j.compedu.2017.04.004

Prancan, K. (2002). *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Houghton Mifflin Company.

Rassin, E. (2018). Reducing tunnel vision with a pen-and-paper tool for the weighting of criminal evidence. *Journal of Investigative Psychology and Offender Profiling*, *15*(2), 227–233. https://doi.org/10.1002/jip.1504

Sunde, N. (2020). Structured Hypothesis Development in Criminal Investigation: A method aimed at providing a broad and objective starting point for a criminal investigation. *The Police Journal: Theory, Practice and Principles*, 0032258X2098232. https://doi.org/10.1177/0032258x20982328

Viale, R. (Ed.). (2021). *Routledge Handbook Of Bounded Rationality* (1st ed.).

Routledge.
Whitesmith, M. (2018). The efficacy of ACH in mitigating serial position effects and confirmation bias in an intelligence analysis scenario. *Intelligence and National Security*, *34*(2), 225–242. https://doi.org/10.1080/02684527.2018.1534640
Whitesmith, M. (2020). *Cognitive Bias in Intelligence Analysis - Testing the Analysis of Competing Hypotheses Method* (1st ed.). Edinburgh University Press Ltd.

International Journal of Criminal Justice

114 Taebong-no, Seocho-gu, Seoul, 06764, Republic of Korea
https://www.kic.re.kr/international/

Printed in Seoul, Korea
31 December, 2021

ISSN 2713-5152

CALL FOR PAPERS

International Journal of Criminal Justice

AIM AND SCOPE

The International Journal of Criminal Justice (IJCJ), a biannual and peer-reviewed English journal published by Korean Institute of Criminology and Justice (KICJ), facilitates comprehensive analysis and evidence-based research on crime trends in order to make a contribution to national policies for crime prevention and criminal justice policies.

The IJCJ will share academic and practical views from home and abroad and play a pivotal role as an international academic forum for domestic and foreign criminal polices.

SUBMISSION DETAILS

- Manuscripts should be written in English and should be no more than 10,000 words in MS word.
- Please provide an abstract which should be no more than 200 words in length and a maximum of 5 key words.
- All papers should identify all authors and provide their contact information such as phone numbers, full postal addresses, email addresses, affiliations and so on.
- Authors should ensure that they have written entirely original works, and should not publish manuscripts describing essentially the same research in more than one journal.
- Honorarium (USD 2,000 or KRW 2,000,000) will be paid when papers are accepted for publication.
- All manuscripts must be submitted to the managing editor at ijcj@kicj.re.kr.

AREAS

International Journal of Criminal Justice (IJCJ) invites papers from many different realms of criminology and criminal justice at both regional and global levels. Any issues related to criminology and criminal justice will be welcomed such as:

Community Sanction, Corrections, Corruption & White Collar Crime, Crime Prevention & Protection, Crime Trends, Crime & Deviance, Criminal Investigation, Criminal Law & Policy, Criminal Procedure, Cybercrime, Drug, Terrorism & Organized Crime, Economic & Corporate Crime, Information, Technology & Forensic Science, Juvenile Delinquency, Juvenile Justice, Penology, Police & Policing, Violent Crime.

International Journal of Criminal Justice

KICJ Korean Institute of Criminology and Justice

9 772713 515003 09
ISSN 2713-5152