# Out of Control? Using STAMP to Model the Control and Feedback Mechanisms Surrounding Identity Crime in Darknet Marketplaces

Ben R. Lanea\*, Paul M. Salmona, Dennis Desmonda, Adrian Cherneyb, Adam Carleyc, Adam Hulmea, and Neville A. Stantonad

aCentre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Maroochydore DC, Queensland, 4558, Australia. Email: [blane@usc.edu.au](mailto:blane@usc.edu.au) (Ben Lane), [psalmon@usc.edu.au](mailto:psalmon@usc.edu.au) (Paul Salmon), [ddesmond@usc.edu.au](mailto:ddesmond@usc.edu.au) (Dennis Desmond), [ahulme@usc.edu.au](mailto:ahulme@usc.edu.au) (Adam Hulme)

bSchool of Social Science, University of Queensland, Brisbane, Queensland, 4000, Australia. Email: [a.cherney@uq.edu.au](mailto:a.cherney@uq.edu.au) (Adrian Cherney)

cDepartment of Home Affairs, Adelaide, South Australia, 5000, Australia. Email: [adam.carley@homeaffairs.gov.au](mailto:adam.carley@homeaffairs.gov.au) (Adam Carley)

dTransportation Research Group, Civil, Maritime and Environmental Engineering and Science Unit, Faculty of Engineering and the Environment, Boldrewood Innovation Campus, University of Southampton, Southampton, United Kingdom. Email: [n.stanton@soton.ac.uk](mailto:n.stanton@soton.ac.uk) (Neville Stanton)

\*Please address correspondence to Ben Lane, Centre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Locked Bag 4, Maroochydore DC, Queensland, 4558, Australia. Email: [blane@usc.edu.au](mailto:blane@usc.edu.au)

# Abstract

Darknet marketplaces have emerged as a facilitator of identity crime and trading. This study aimed to (1) understand the entities and control and feedback mechanisms that influence identity crime prevention and occurrence on the darknet in the Australian system and to (2) comprehensively identify the implications of control failures across all system levels. The Systems-Theoretic Accident Model and Processes (STAMP) was used to develop an identity crime control structure in consultation with subject matter experts and then the Systems-Theoretic Process Analysis (STPA) was applied. The STPA identified 310 risk states, resulting from control failures and which were associated with the range of agencies, organisations, and individuals present across system levels. As darknet marketplaces rapidly evolve, alignment between these entities is necessary to enable agile system responses. STAMP and STPA have promise in understanding the potential for intervention across all system levels in preventing societal issues such as identity crime.

*Key words*: Darknet, identity crime, Systems Theoretic Process Analysis.

**Abbreviations**

STAMP = Systems-Theoretic Accident Model and Processes

STPA = Systems-Theoretic Process Analysis

TOR = The Onion Router

CAST = Causal Analysis based on STAMP

# Out of Control? Using STAMP to Model the Control and Feedback Mechanisms Surrounding Identity Crime in Darknet Marketplaces

**1. Introduction**

Identity crime is a serious problem in Australia and internationally. It includes the theft or use of another person’s personal identifying information, such as driver’s licence number, credit card details, and/or name (Allison, Schuck, & Lersch, 2005; Australian Federal Police, 2019). Potential uses of such information include credit card fraud, in which stolen credit card details are used to make purchases; bank account fraud, where personal bank accounts are accessed and drained; and credit fraud, in which loans, phone plans, and other assets are secured based on the victim’s credit rating (Copes, Kerley, Huff, & Kane, 2010). One in four Australians report being a victim of identity crime and, in a 12-month period during 2015 and 2016, identity crime resulted in an estimated financial loss of $2.65 billion nationally (Jorna & Smith, 2018). Victims lose assets ranging from thousands of dollars up to their entire lifesavings. In addition to financial losses, such crimes have behavioural, psychological, or emotional consequences, such as discontinued use of Internet-based services and feelings of shame, stress, or worry (Watson, Lacey, Kerr, Salmon, & Goode, 2019; Watson, Salmon, Lacey, & Kerr, 2018).

Research has examined factors contributing to identity crime. For example, an individual’s routine internet use for banking and communication increases their risk of victimisation (Reyns, 2013), while privacy protection behaviours decrease risk (Holt & Turner, 2012; Lai, Li, & Hsieh, 2012). At a systemic level, mandatory data breach disclosure laws reduce the rate of identity crime (Romanosky, Telang, & Acquisti, 2011) and Australia recently adopted laws consistent with this evidence (Australian Government Office of the Australian Information Commissioner, 2018). Research has also examined how individuals conduct identity theft attacks, for example, using social media (Bilge, Strufe, Balzarotti, & Kirda, 2009; He, Chen, Su, & Sun, 2014) and email phishing scams (Vijaya Geeta, 2011). Social engineering, rather than technical hacking, is the predominant means data are breached and people vary in their susceptibility based on their trust in others and deference to supposed authority figures (Workman, 2007).

Having secured stolen information, criminals may exploit it personally or sell it to others who have greater expertise in doing so (Holt & Lampke, 2010). A research literature is growing about the processes criminals undergo to trade in stolen identity data online (Holt & Lampke, 2010; Holt, Smirnova, & Chua, 2016; Hutchings & Holt, 2015; Lacey & Salmon, 2015; Lacey, Salmon, & Glancy, 2015; Lane, Lacey, Stanton, Matthews, & Salmon, 2018; Lane, Salmon, Cherney, Lacey, & Stanton, 2019; Salmon et al., 2019). The darknet, in particular, has emerged as an avenue through which identity crime can be facilitated (Lane et al., 2018, 2019). The darknet is accessed using TOR, the Onion Router, which anonymises internet use. Via the darknet, users can access marketplaces that permit peer-to-peer trading of illicit goods, primarily identity information and controlled substances (Lane et al., 2018). These marketplaces self-regulate and support regular transaction partnerships built on trust (Lane et al., 2018, 2019). The darknet has removed traditional barriers to entry to participate in crime, providing access to globally connected markets for illicit goods and services which require no previous criminal networks. This has disrupted established criminal channels and opened these markets to new sources of supply and demand. Along with anonymity, cryptocurrency use, and increasing user capabilities, the darknet thus emboldens criminal behaviour and allows motivated offenders greater access to targets, such as identity information. Whilst law enforcement operations have targeted processes on these new marketplaces, the markets involve great complexity (Lane et al., 2018) and there remains a need for novel interventions to address this societal issue.

Individuals receive many recommendations concerning how to protect themselves from becoming victims of identity crime, such as securing physical mailboxes and being cautious of sharing personal and financial information (Australian Federal Police, 2019). Although following such advice promotes protection, safety—from something such as identity crime—could be better conceptualised as an emergent property of the overall system (Leveson, 2017). It is not the actions of any one individual or entity that promotes safety, but the actions of many subsystems in concert. According to Leveson (2017), safety requires that constraints on the system be enforced. In the context of identity crime, for example, there should be assurances that payment of funds is never actioned without personal approval by a customer. However, with sufficient identity documentation, an individual has the power to convince banks, credit lenders, and government to grant them access to another individual’s bank accounts, credit rating, and otherwise good standing.

## *1.1 Systems-Based Approaches to Address Identity Crime*

Improving the understanding of why accidents happen and how to prevent them is a persistent ambition for safety researchers. In pursuit of this, Leveson (2004) developed STAMP (Systems Theoretic Accident Model and Processes), an accident analysis and risk prediction approach based on systems theory, that theorises accidents occur due to a failure of control mechanisms in the system. STAMP is based on the observation that component failures in isolation are rarely the cause of incidents. Rather, unanticipated incidents and events occur when dysfunctional components interact, or when external disturbances exceed the capabilities of the control structure (Leveson, 2004, 2011a, 2011b), for example, the introduction of novel criminal methods. A state of system equilibrium is sought via control and feedback mechanisms that link actors and factors across all levels of the system. Decisions and instructions are passed down the system to influence the behaviour and decisions of those in operational roles and, ideally, information is returned through the structure to inform decisionmakers about the system’s status. Whereas other systems analysis methods, such as the Event Analysis of Systemic Teamwork and Work Domain Analysis, focus on activities and objects within the system, STAMP considers the structure of the broader system and the entities within it, including agencies, organisations, professionals, and individuals. By considering the controls and decisions that these entities enact, STAMP can identify potential intervention points in which to influence the problem, in this case identity crime on darknet marketplaces, across all levels of the system.

STAMP has been applied to road safety (Salmon, Read, & Stevens, 2016), rail safety (Li, Tang, Chatzimichailidou, Jun, & Waterson, 2019; Read, Naweed, & Salmon, 2019), outdoor led education (Salmon, Cornelissen, & Trotter, 2012), sports injury prevention (Hulme, Salmon, Nielsen, Read, & Finch, 2017, 2018), the oil and gas industry (Altabbakh, AlKazimi, Murray, & Grantham, 2014), aviation safety (Allison, Revell, Sears, & Stanton, 2017; Schmid, Vollrath, & Stanton, 2018), maritime transportation safety (Kim, Nazir, & Øvergård, 2016), and healthcare (Canham, Jun, Waterson, & Khalid, 2018). These studies differ in their level of granularity, with some applications focusing heavily on process models (e.g., Altabbakh et al., 2014; Kim et al., 2017) and others emphasising controls and decision-makers at higher system levels (e.g., Hulme et al., 2017, 2018; Salmon et al., 2012, 2016). By considering the system as the unit of analysis with recognition of higher-level entities, the models can have compelling implications in understanding the critical role these entities have in influencing relevant outcomes (Hollnagel, 2016; Rasmussen, 1997).

Victims of identity crime commonly report feelings of personal stupidity or embarrassment as emotional impacts (Watson et al., 2019). However, as with incidents in other complex domains, placing blame on lone individuals is both unhelpful and inaccurate (Holden, 2009; Read, Salmon, & Lenné, 2013). There are many agents within a system, human and technical, whose actions influence eventual thefts. The goal of investigating this area is not to identify entities other than victims to blame (apart from the perpetrator/s), but rather to determine the range of influences leading to the incident despite well-meaning efforts of protective agents and systems (Leveson, 2011a). In line with the philosophy underpinning STAMP, incidents of identity crime on darknet marketplaces may be considered to result from inadequate control of constraints in the system. Behaviour is partially controlled by organisational processes and culture (Leveson, 2011a, 2017). It is also controlled through the design of the system. Thus, this perspective draws focus away from victims of identity crime towards potential intervention strategies and approaches that encompass the whole system.

In considering a completed control structure, two methods associated with STAMP can be used, the Causal Analysis based on STAMP (CAST) and Systems-Theoretic Process Analysis (STPA; Leveson, 2011b). CAST is used to support accident causation analysis, whereas STPA is used to identify risks and predict hazardous system states (Ishimatsu et al., 2014; Leveson, 2011b). STPA, in particular, is thus applicable to assessing general system risks. It provides a comprehensive analysis of potential risks, although without probability-based estimates, which are arguably uninformative in complex systems due to the many system outcomes resulting from interactions between multiple system conditions (Bjerga, Aven, & Zio, 2016). STPA has been applied in several domains, such as military training (Stanton, Harvey, & Allison, 2019), spacecraft design (Ishimatsu et al., 2014), aircraft safety (Allison et al., 2017), and information technology (Sulaman, Beer, Felderer, & Höst, 2019). Whereas applications in these domains use STPA to analyse risks within control structures that emphasise the process end of the system, applying the method to a high-level control structure draws focus to systemwide decision making, which may arguably have great utility in addressing a societal issue.

## *1.2 The Present Research*

This study sought to address limitations associated with existing research that focuses on individuals and their behaviour in relation to identity crime. Instead, using a systems approach, the study considered the influence of systemic structures and factors that influence the decisions, actions, and behaviours at the operational end of the system, which includes the darknet environment and actors involved in identity trading scenarios. STAMP and STPA have traditionally been applied to highly technical environments in which prevention of accidents is the main objective, such as in road and aircraft safety (Allison et al., 2017; Salmon et al., 2016). The application of STAMP to identity crime on darknet marketplaces extends its application to a social and insidious behaviour, driven by intentions rather than accidents. The aims of this study were therefore to (1) understand the entities and control and feedback mechanisms that influence identity crime prevention and trading on darknet marketplaces and to (2) comprehensively identify the implications of control failures across levels of the system. The analysis was scoped to the Australian system to maintain the feasibility of the analysis. The study was reviewed and approved by the Human Research Ethics Committee of the University of the Sunshine Coast, with considerations given to the use of publicly available information as well as the safety of the research team.

# 2. Material and Methods

## *2.1 Development of the Identity Crime Control Structure*

Although STAMP addresses both system development and operation (Leveson, 2004, 2011a), this study was scoped to system operation given that the system surrounding identity crime is well established. The control structure is a representation of this overall system, independent of any particular event or occurrence (Leveson, 2004). Initially, the first author constructed a draft control structure surrounding the activity of identity crime on darknet marketplaces. This process involved (1) adapting the generic STAMP control structure, (2) identifying the actors, groups, and organisations with decision-making capacities present at each level of the structure, and (3) identifying the control and feedback mechanisms that operate between each level of the identity crime control structure. The development of the initial control structure was informed by various sources. Information was derived from stakeholder websites (e.g., the Australian Law Reform Commission, Australian Criminal Intelligence Commission, and Australian Federal Police), inquiry reports (Australian Government, 2017, 2018a, 2018b; Shergold, Seidel, Gannon, & Lim, 2017), published literature on processes on darknet marketplaces (Lane et al., 2018, 2019; Salmon et al., 2019), and screenshots of darknet marketplace processes. The screenshots included all those processes able to be completed without depositing funds on the market. The operator used a personal computer with a separate virtual machine to access the darknet. No personal details were entered into the markets or within the virtual machine. International entities were also considered as per previous research (Parnell, Stanton, & Plant, 2017). A data dictionary was created to describe each entity and define their key roles (see supplemental materials). Control and feedback mechanisms were subsequently created by considering the relevant behaviours of each entity included in the control structure and their relationships with entities at other system levels.

With a complete draft of the identity crime control structure, four analysts additional to the first author subsequently met to consider the model until consensus was reached. Four analysts held a PhD qualification, with one in psychology, two in criminology, and one in ergonomics, and two had previous careers in federal law enforcement and criminal intelligence agencies. The relevant experience of authors is provided in Table 1. The presence of each entity in the control structure was considered systematically in reference to the entity’s role in ultimately influencing identity crime on darknet marketplaces.

## *2.2 STPA Data Analysis*

Following creation of the identity crime control structure, the STPA involved applying a taxonomy to identify unsafe control actions:

1. Action required but not provided
2. Unsafe action provided
3. Incorrect timing/order
4. Stopped too soon/ applied too long

The first author applied the taxonomy to each control measure identified in the control structure. All analysts were provided with the control structure and a word document which included a table of the STPA risks for each of the four control failure categories. Analysts reviewed all of the risks and provided feedback where the risk descriptions required modification or where they had identified additional risks. As this study aimed to identify the effects of control implications of control failures rather than remedy them, the further step in STPA of analysing the cause of unsafe control actions using feedback loops was not pursued.

# 3. Results

## *3.1 Control Structure*

Excerpts from the identity crime control structure are presented in Figures 1, 2, and 3, documenting each decision-maker in the system and the controls and feedback they may enact. There were 94 entities, 86 control mechanisms, and 61 feedback mechanisms identified in the control structure. Table 2 presents the division of these characteristics across system levels. The process of constructing the control structure provides a framework for understanding the entities involved in the system. The following sections provide a description of the entities and their behaviour at each system level.

**3.1.1 International context**

The Australian system exists within a broader international framework. As shown in the control structure across the three figures, as well as influencing Australia's government agencies (Level 2), international taskforces (International Context) can initiate direct impacts within the darknet (Level 5) through controls such as covert operations and direct regulation of darknet environment. Based on this, international taskforces have been responsible for several high-profile seizures of darknet marketplaces, such as Alpha Bay and Hansa Market as part of Operation Bayonet in 2017 (Europol, 2017). Further to this, international crime syndicates are included in the structure because business-to-business transactions have been identified as a driver of darknet marketplace activity previously (Aldridge & Décary-Hétu, 2016) and transactions are known to span continents (Broséus, Rhumorbarbe, Morelato, Saehli, & Rossy, 2017). A control mechanism of strategic direction of criminal activity is thus linked from the International Context to the darknet operating environment (Level 5). Broadly, the International Organization for Standardization (ISO) promotes worldwide proprietary, industrial, and commercial standards and creates specifications, guidelines, and requirements to shape systems and processes. These directions have a pervasive influence on technologies and processes worldwide and contribute control through international guidelines and frameworks that filter through the system.

**3.1.2 Parliament and legislators**

The parliament and legislators (Level 1) are responsible for passing legislation, representing citizens, scrutinising government action, and coordinating policy decisions. Specifically, the Australian Law Reform Commission reviews laws, whereas the Council of Australian Governments served to coordinate between the nation's Federal and State governments. In Australia, political parties allow diverse ideologies to be represented. Along with the Federal Parliamentary Committees and Prime Minister and Cabinet, these entities enact control through various government agencies (Level 2), by setting strategy, policy, and plans; allocating funding; communicating political objectives; and setting targets. Lobbyists, media, and public opinion received from those in operational delivery and management (Level 3) or local management and supervision (Level 4) may feed into informing decision-making across any of the entities. However, feedback is mostly received by the various subsidiary departments and agencies (Level 2) in the form of reports, proposals, and draft documents. Parliament is accountable to the public and provides information through media channels.

**3.1.3 Government agencies**

Government agencies and public services feature most commonly at Level 2, although tertiary institutions and independent organisations, such as the TOR project, are also present. These entities hold diverse purposes. For example, the Cyber Resilience Taskforce in Australia (Level 2) hosts companies and industry associations to develop approaches to cybersecurity, a "guidelines" control mechanism affecting operational bodies (Level 3). Government departments hold vast portfolios. Of importance to identity crime, the Department of Home Affairs includes a portfolio of agencies, all represented at Level 2; the Australian Criminal Intelligence Commission, Australian Federal Police, Australian Border Force, and the Australian Transaction Reports and Analysis Centre (AUSTRAC). This portfolio arrangement is intended to provide more coordinated intelligence and investigation activities against threats. Many agencies share priorities and jurisdiction in addressing criminal activity, including crime on darknet marketplaces, which lends itself to a multi-agency task force approach to addressing these threats.

Many of the control mechanisms between the government agencies (Level 2) and operational delivery and management (Level 3) apply generally across the entities. Similar to the parliament and legislators, entities at this level enact control on subsidiaries through strategies, policy, and plans. The guidance provided is more specific and agencies vary in their priorities and funding allocations. For example, AUSTRAC provides guidance to banks and businesses broadly on how to comply with financial regulations. The Australian Criminal Intelligence Committee coordinates information sharing amongst law enforcement agencies as well as identifying priorities and strategic directions through national reports. The agencies tend to direct national agendas and public education and enact legal penalties across system levels. Entities largely receive performance reports and statistics from the operational subsidiaries (Level 3).

**3.1.4 Operational delivery and management**

Operational delivery and management includes private organisations and service providers, operational law enforcement, and social forces, such as the media. Notably, darknet marketplaces and organised crime syndicates were placed at this level. Diverse control mechanisms are thus present. For example, organised crime syndicates (Level 3) have a role in controlling tradecraft, operational security, and product and service availability within the marketplaces (Level 5). Essential services, such phone and Internet plans, are represented by control mechanisms from Telephone service providers, hosting companies, and VPN providers (Level 3) to both organisation staff (Level 4) and end users such as market buys, sellers, and vulnerable individuals (Level 5). Further, agencies, such as the Australian Passport Office and banks, issue many of the identity documents that hold value on darknet marketplaces, influencing the use of these credentials by organisation staff (Level 4) as well as their value and availability as products on darknet markets (Level 5). Law enforcement and intelligence operational groups (Level 3) direct the behaviour of analysts, agents, and intelligence officers (Level 4) and the outcomes of these individuals may be fed back via progress updates, team meetings, and similar means.

**3.1.5 Local management and supervision**

Local management and supervision include operatives, agents, and officers in addition to darknet administrators and moderators. Market administrators (Level 4) have control mechanisms of marketplace management and announcements, orchestration, guidance, disruption resolution, and enabling access to markets (Level 5). Marketplace success relies on the effectiveness and upkeep of market transactions and adequate user trust in the system, such as through addressing user disputes (Lane et al., 2019). Administrators may hire moderators (Level 4) to assist in negotiating these disputes, managing forums, and regulating other user-created content, such as advertisements and profiles.

Several control mechanisms from local management (Level 4) to the operating environment (Level 5) relate to the behaviour of law enforcement and intelligence operatives, such as monitoring, orchestration, and investigation. In this ecosystem, counsellors and education providers (Level 4) also assist and convey guidance and measures for individuals (Level 5) to protect their identity data. The marketplaces (Level 5) feed information back regarding sales and products, as well as other observable behaviours and components.

**3.1.6 Operating process and environment**

The operating environment itself, darknet marketplaces (Level 5), features dynamic interplay between buyers, sellers, covert operatives, and Machiavellian users, seeking to extort others or bolster their own reputation through various means. The marketplaces self-regulate and product reviews and community engagement on forums act as control mechanisms from the operating environment to the process of identity trading. Vulnerable individuals were included as an entity at this level. They may control some elements of darknet trading through their own protective measures and may detect consequences of darknet sales such as unrecognised bank or credit card charges. Such observable behaviour is identified as a feedback mechanism from the operating process to the operating environment as well as to higher levels, including local management and supervision (Level 4) and operational delivery and management (Level 3).

## *3.2 Systems-Theoretic Process Analysis*

The STPA was applied to the 86 control mechanisms in the control structure. An excerpt from the analysis is provided in Table 3 and the full analysis in the supplemental materials. Across the four taxonomy modes, an example is given for each based on the implications of the mode eventuating. In most cases, all four taxonomy modes were applicable. Overall, 82 control mechanisms had consequences when the action was not provided, 82 had consequences when an unsafe action was provided, 76 had consequences when timing or order was incorrect, and 70 had consequences when the control was stopped too soon or applied too long. For example, as shown in Table 3, the STPA identified risk states including that (1) strategy, policy, and action plans from the parliament and legislators are not provided, resulting in lack of strategic direction; (2) unhelpful controls are provided; (3) the timing is suboptimal, resulting in outdated approaches; and (4) when the existing controls are not provided for an effective duration. With these risks established for each level of the control structure, working with subject matter experts drew focus to potential interactions of risks across levels, which are explored in the Discussion section.

# 4. Discussion

This study sought to understand the control structure in place in the prevention and occurrence of identity crime on darknet marketplaces in Australia and identify the implications of control failures in the system. The study has two key contributions. First, the identity crime control structure supported the identification of the entities that influence identity crime on darknet marketplaces. Specifically, using Leveson’s control structure we were able to identify the actors and organisations who share the responsibility for identity crime management in Australia as well as the control and feedback mechanisms that are used to achieve this. This extends the scope of STAMP applications beyond accident prevention to crime prevention. Previous applications of the STAMP control structure method have focused on safety management (e.g. Allison et al., 2017; Kim et al., 2016; Read et al., 2019; Salmon et al., 2016). This analysis has demonstrated the utility of the control structure method for crime prevention, opening up many other potential applications. Second, the STPA identified the consequences of potential control failures across the system, providing information that can be used to strengthen identify crime prevention activities. Trading on darknet marketplaces involves complex networks of behaviour (Lane et al., 2018, 2019). However, the full arrangement of actors in the system has not been previously documented. This study expands the lens on the issue to include distal parts of the system, such as government agencies and international standards. Conceptualising identity crime in the context of this broad and complex system—that cannot be reduced to a single actor, action, or legislative change—is a significant step in understanding this societal issue.

***4.1 Systems-Theoretic Accident Model and Process Control Structure***

The identity crime control structure highlights the actors whose decisions affect the target problem. With the construction of the control structure complete, STAMP permits analysis of the whole system according to the systems-thinking principles upon which it was designed (Underwood & Waterson, 2014). For example, the nature of the control structure and its entities may be explored in more depth. In considering the identity crime control structure, the sheer number of entities highlights the potential for duplication of effort. Many government agencies are involved in the oversight of developing counter measures. However, the process of researching the entities identified that they do not specify clear delineation of roles or operations. It should be acknowledged that joint task forces exist, which may assist in coordinating technology and enforcement resources and overcoming jurisdictional issues, allowing subpoenas, search and extradition warrants, and access to witnesses. The major international operations, such as Operation Bayonet (Europol, 2017), are testament to the potential of these approaches and the level of coordination achievable. Those outside these task forces, however, operate independently and may be unable to benefit from information and other assets being shared. There is also potential for specific agencies to have competing priorities. Agencies, in addition to political parties, may wish to uphold targets that complement their public image and attract funding which could compromise operational work not aligned with these goals. In these examples, the control structure provides a framework to guide the generation of insights.

Unique to the crime prevention context, consideration of the identity crime control structure may also be taken from the perspective of nefarious entities. The construction of the control structure identified that darknet marketplaces operate as self-regulating subsystems within the broader context of government and organisational activity. It further represents how senior actors within these systems, including administrators and moderators, have power to influence trading, including the items permitted to be advertised, the users allowed to continue sales, and—to an extent—the level of trust in the marketplaces. Whilst some users sell peer-to-peer via i2P, an alternative to the TOR network used to access darknet sites, and encrypted messaging applications such as WhatsApp, the demand for their services may be influenced by these greater market forces. Beyond the marketplace, the control structure also represents that government agencies influence the presence of the opposing law enforcement actors in the markets as well as the value of goods traded. The value of stolen and fraudulent identity documents is also increased due to their use to comply with "know your customer" requirements in the creation of financial accounts (Watson et al., 2019). These considerations allude to layers of vulnerabilities and faciliatory factors within the control structure that ultimately influence whether successful identity trading occurs. The control structure in this context enables concurrent analysis of the forces that aim to maintain safety and those that intend to disrupt it.

***4.2 Systems-Theoretic Process Analysis***

The STPA, as an extension of the control structure, provided a systematic approach to exhaustively consider the effects of control failures, identifying 310 potential risk states in preventing and protecting against identity crime. The use of STPA with a high-level control structure is a novel extension of the method. Of note, the four error modes were found to be applicable in almost all depicted controls. This finding may relate to the general nature of these control mechanisms, which allows them wide scope to capture many risks. Each of the resulting risk states may occur in isolation or together, producing great fluctuations in the system’s safety. Whilst the insights outlined may be realised independently from completing the STPA, the systematic process supports the analyst in identifying a comprehensive selection of risks. With the framework of risks established, analysts may use the STPA to interrogate particular risks further.

To demonstrate this potential, the STPA was discussed with subject matter experts who identified that ‘strategic direction’ at higher levels of the system (Levels 1 to 3) may dramatically affect operational behaviour (Levels 4 and 5). Insufficient strategic direction, or direction that arrives too late, prevents the agile responses that are required in a rapidly evolving environment such as the darknet. A failure of higher-level actors to accommodate these needs would result in wasted time and resources as well as an inability to respond effectively to emerging challenges. New markets and targets appear on the darknet, interventions from law enforcement worldwide occur, and products vary in supply and demand.

An additional example from the STPA relates to the system’s constraints. The power to pursue cases of criminal activity are dependent on the resources allocated, which is identified in the STAMP as a control mechanism spanning from Levels 1 to 3. These allocations are also often contingent on performance indicators such as the number of arrests made (Holm, 2017), damage thresholds, likelihood of prosecution, and the return on investment, which correspond to feedback mechanisms throughout the control structure. Governments hold a priority to maintain their public branding and image, driven by constraints that they must address to remain elected. Thus, operations that do not have visible effects may not attract funding compared to those that have more salient rewards, such as large seizures of controlled substances. These considerations particularly affect attempts to influence darknet trading given that a single vendor may engage in a high volume of small-scale sales where any individual seizure is seen as insignificant. The feedback mechanisms identified in the control structure may therefore be insufficient in supporting effective interventions with contributions across the system. Law enforcement agencies often contend with limited resources (Rid & Buchanan, 2015) and it is a risk for them to pursue interventional strategies that do not have clear outcomes. Insufficient funding allocations, or funding allocations that are stopped too soon, are thus plausible risk states identified in the STPA that likely occur in practice. An implication of this system analysis is a recommendation for higher-level entities to value the investment of law enforcement resources in long-term oriented, disruption-based operations. By overlapping known issues in the domain against the STPA, insights such as these can be drawn regarding the parts of the system that have responsibility for action. Furthermore, with the risk identified, consideration can then be directed to potential practical implications.

### 4.3 Practical Implications

Taken as a whole, the identity crime control structure provides a roadmap to identify which entities are involved, the control mechanisms needed to be enacted or modified, and the feedback mechanisms required to support adequate communication between operational activity and managerial decision making. Thus, in working with law enforcement, shared understanding of the system is supported, and system analysis and redesign considerations can take place. Specifically, with an outline of the control and feedback mechanisms, the control structure provides the opportunity to consider what mechanisms may be missing or in need of reinforcement. For example, existing control mechanisms involving the communication of strategy, policy, and procedures from Levels 1 or 2 may need to be modified in accordance with the operational requirements within Levels 3 to 5 and a changing landscape of crime management brought about by criminal innovations. Additional control mechanisms may be needed to be considered that enable greater agility in responding to problems. In turn, feedback mechanisms that address the consequences of any changes in operations may then be instated.

As a further example regarding feedback mechanisms, although reporting is often acknowledged within the control structure, these mechanisms may benefit from being bolstered. In an incident in Australia in 2017, a journalist reported the availability of Australian government issued healthcare cards on the darknet market, Alphabay, which the relevant Government department claimed to have no knowledge about (Farrell, 2017). The incident instigated a formal government review and investigation (Australian Government 2017, 2018a, 2018b). Using the control structure framework, the incident may be interpreted as being the absence of feedback mechanisms that connect law enforcement observations of goods on the darknet to notification of relevant government departments that are implicated. With further interrogation of the control structure as a framework, further identification of control and feedback mechanisms could have significant implications for identity theft management across the system as a whole.

The identity crime control structure also provides the opportunity to consider the system with regard to general principles of systems thinking. In our subsequent work with operational law enforcement, the control structure was able to shift focus towards the organisational control mechanisms present that act as barriers to effective operational decision-making. By being able to describe a complex organisational structure, problem solving was considered at the national and company levels rather than mostly the responsibility of operational staff and supervision. There are insights specifically into the ways in which management contribute to risk management in a dynamic environment.

Insights were further identified in relation to the domain itself. In contrast to other safety-oriented domains, the system is comprised of both safety-promoting and safety-disrupting entities. Indeed, the sites that populate the darknet are created to evade regulatory powers. Although regulation guided the initial development of the Internet and computing technology, individuals can manipulate these systems to suit their goals. With these uncertainties and criminal users’ active pursuit of system disruption, the system surrounding the darknet likely struggles to maintain dynamic equilibrium, in which continual control inputs aim to maintain operations within ‘safe’ boundaries (Dekker & Pruchnicki, 2014; Hale, Guldenmund, & Gossens, 2006). Innovations by nefarious entities on darknet marketplaces outpace the capacity of agencies to implement counter measures and this may lead to unexpected and frequent deficiencies in the protective structure.

Taking a broad perspective, cybersecurity is recognised as one of the global problems that humanity faces in the 21st century (Thatcher, Waterson, Todd, & Moray, 2018). The reporting, investigation, and analysis of cybersecurity incidents remains scarce in the academic literature while also being of increasing relevance to government and business security internationally (Paté-Cornell, Kuypers, Smith, & Keller, 2018; Scala, Reilly, Goethals, & Cukier, 2019). As an additional practical implication, the identity crime control structure presented here could be used in conjunction with the CAST method to support the investigation and analysis of cybersecurity incidents. Specifically, incident investigation is supported by allowing identification of where weaknesses may exist. Incident analysis may take place through the classification of control and feedback failures.

Future research may consider how insights from STAMP can be translated into the practical implications discussed. The research-practice gap is well-documented and researchers should consider how to implement findings (Goode, Salmon, Lenné, & Finch, 2018; Read, Salmon, Lenné, & Stanton, 2015; Shorrock & Williams, 2016). Underwood, Waterson, and Braithwaite (2016) argued that STAMP would need to be simplified to bridge this gap. With simplification, STAMP may be integrated into darknet investigations and intelligence-led policing training to draw awareness to control and feedback mechanisms that support or inhibit their work and other system considerations. Alternatively, the use of systems methods, such as STAMP, also presents an opportunity for human factors and ergonomics academics and professionals and law enforcement institutions to work cooperatively, drawing on systems thinking expertise from the academics and professionals, and operational expertise from law enforcement stakeholders, to develop insights. Those with human factors and ergonomics expertise have a potential role in guiding system analysis and redesign.

## *4.4 Limitations*

Although we argue that STAMP provides a useful framework for generating system insights, limitations should be noted in its application. Foremost, like many systems-ergonomics methods, STAMP and STPA rely heavily on the analysts’ insights (Stanton et al., 2013). Understanding a domain and the interrelationships between entities appropriately is challenging when considering the complexity inherent in a single entity, such as a government department. It is difficult to know what all the activities of a given entity include. Further to this, all modelling relies on assumptions and simplifications, preventing the control structure from representing the system completely. Although the control structure was constructed and validated with subject matter experts, it remains a complex phenomenon to approximate. Notably, the analysis was also limited to the Australian system. However, while there are some unique agencies within this system, many entities have an equivalent internationally that enacts similar control and feedback mechanisms. The STAMP analysis of darknet marketplaces is, therefore, applicable irrespective of national interest or enforcement jurisdiction. Darknet marketplaces transcend national boundaries and their customers are global in nature but their structure remains constant regardless of which market is under analysis. Following this application, those internationally may use the present control structure and analysis as a template and replace country-specific entities and controls as appropriate.

## *4.5 Conclusions*

In the face of the global challenge of cybersecurity, this study indicates that human factors and ergonomics can provide frameworks for guiding system redesign and generating specific and practical insights. The identity crime control structure and STPA provide useful tools in cooperating with law enforcement and understanding system design, control and feedback mechanisms, and vulnerabilities. This study extends STAMP to consider intention-driven risks and indicates its potential to inform system change by addressing the control pathways from higher-level to operational entities in the system relating to the problem of identity crime. The study also extends STPA by considering risk identification across control mechanisms enacted by entities at all levels of the system. Researchers and practitioners are encouraged to consider further applications to gain system thinking insights within the broader realm of crime prevention.

Funding: This work was supported by the Australian Research Council, Queensland Police Service, IDCARE, Australian Postal Corporation, Department of Home Affairs, Australian Criminal Intelligence Commission, and Australian Transaction Reports and Analysis Centre [LP160100277]. Paul Salmon's contribution to this article was funded by the Australian Research Council [FT140100681].

# References

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, *35*, 7-15. doi: 10.1016/j.drugpo.2016.04.020

Allison, C. K., Revell, K. M., Sears, R., & Stanton, N. A. (2017). Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Safety Science*, *98*, 159-166. doi: 10.1016/j.ssci.2017.06.011

Allison, S. F. H., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, *33*, 19-29. doi: 10.1016/j.jcrimjus.2004.10.007

Altabbakh, H., AlKazimi, M. A., Murray, S., & Grantham, K. (2014). STAMP – Holistic system safety approach or just another risk model? *Journal of Loss Prevention in the Process Industries*, *32*, 109-119. doi: 10.1016/j.jlp.2014.07.010

Australian Federal Police. (2019). Identity crime. Retrieved from <https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime>

Australian Government Office of the Australian Information Commissioner. (2018). Notifiable data breaches scheme. Retrieved from <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>

Australian Government. (2017). Circumstances in which Australians’ personal Medicare information has been compromised and made available for sale illegally on the ‘dark web’. Available: <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/medicareinformation>

Australian Government. (2018a). Australian Government response to the independent review of health providers’ access to Medicare card numbers. Available: <https://www.humanservices.gov.au/organisations/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers>

Australian Government. (2018b). Australian Government response to the Senate Finance and Public Administration References Committee report: Circumstances in which Australians’ personal Medicare information has been compromised and made available for sale illegally on the ‘dark web’. Available: <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/medicareinformation>

Bilge, L., Strufe, T., Balzarotti, & Kirda, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. *Proceedings of the 18th International World Wide Web Conference*, 551-560. doi: 10.1145/1526709.1526784

Bjerga, T., Aven, T., & Zio, E. (2016). Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliability Engineering and System Safety*, *156*, 203-209. doi: 10.1016/j.ress.2016.08.004

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International*, *277*, 88-102. doi: 10.1016/j.forsciint.2017.05.021

Canham, A., Jun, G. T., Waterson, P., & Khalid, S. (2018). Integrating systemic accident analysis into patient safety incident investigation practices. *Applied Ergonomics*, *72*, 1-9. doi: 10.1016/j.apergo.2018.04.012

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, *38*, 1045-1052. doi: 10.1016/j.jcrimjus.2010.07.007

Dekker, S., & Pruchnicki, S. (2014). Drifting into failure: Theorising the dynamics of disaster incubation. *Theoretical Issues in Ergonomics Science*, *15*, 534-544. doi: 10.1080/1463922X.2013.856495

Europol. (2017). Massive blow to criminal dark web activities after globally coordinated operation. Available: <https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>

Goode, N., Salmon, P. M., Lenné, M. G., & Finch, C. F. (2018). *Translating systems thinking into practice: A guide to developing incident reporting systems* (1st ed.). Boca Raton, FL: CRC Press.

Farrell, P. (2017). The Medicare machine: Patient details of 'any Australian' for sale on darknet. The Guardian Australia. Available: https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet

Hale, A., Guldenmund, F., & Goossens, L. (2006). Auditing resilience in risk control and safety management systems. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 289-314). Aldershot, England: Ashgate.

He, B., Chen, C., Su, Y., & Sun, H. (2014). A defence scheme against identity theft attack based on multiple social networks. *Expert Systems with Applications*, *41*, 2345-2352. doi: 10.1016/j.eswa.2013.09.032

Holden, R. J. (2009). People or systems? To blame is human. The fix is to engineer. *Professional Safety*, *54*(12), 34-41. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3115647/>

Hollnagel, E. (2016). *Barriers and accident prevention*. London: Routledge.

Holm, E. (2017). The darknet: A passageway to identity theft. *International Journal of Information Security and Cybercrime*, *6*, 41-50. doi: 10.19107/IJISC.2017.01.04

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*, 33-50. doi: 10.1080/14786011003634415

Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, *33*, 308-323. doi: 10.1080/01639625.2011.584050

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, *37*, 353-367. doi: 10.1080/01639625.2015.1026766

Hulme, A., Salmon, P. M., Nielsen, R. O., Read, G. J. M., & Finch, C. F. (2017). Closing Pandora’s Box: Adapting a systems ergonomics methodology for better understanding the ecological complexity underpinning the development and prevention of running-related injury. *Theoretical Issues in Ergonomics Science*, *18*, 338-359. doi: 10.1080/1463922X.2016.1274455

Hulme, A., Salmon, P. M., Nielsen, R. O., Read, G. J. M., & Finch, C. F. (2018). From control to causation: Validating a ‘complex systems model’ of running-related injury development and prevention. *Applied Ergonomics*, *65*, 345-354. doi: 10.1016/j.apergo.2017.07.005

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*, 596-614. doi: 10.1093/bjc/azu106

Ishimatsu, T., Leveson, N. G., Thomas, J. P., Fleming, C. H., Katahira, M., Miyamoto, Y.,…, Hoshino, N. (2014). Hazard analysis of complex spacecraft using systems-theoretic process analysis. *Journal of Spacecraft and Rockets*, *51*, 509-522. doi: 10.2514/1.A32449

Jorna, P., & Smith, R. G. (2019). Identity crime and misuse in Australia 2017 (Statistical Reports no. 10). Canberra: Australian Institute of Criminology. Retrieved from <https://aic.gov.au/publications/sr/sr10>

Kim, T., Nazir, S., & Øvergård, K. I. (2016). A STAMP-based causal analysis of the Korean Sewol ferry accident. *Safety Science*, *83*, 93-101. doi: 10.1016/j.ssci.2015.11.014

Lacey, D., & Salmon, P. M. (2015). It’s dark in there: Using systems analysis to investigate trust and engagement in dark web forums. In D. Harris (Ed.), E*ngineering psychology and cognitive ergonomics* (pp. 117-128). doi: 10.1007/978-3-319-20373-7\_12

Lacey, D., Salmon, P. M., & Glancy, P. (2015). Taking the bait: A systems analysis of phishing attacks. *Procedia Manufacturing*, *3*, 1109-1116. doi: 10.1016/j.promfg.2015.07.185

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*, 353-363. doi: 10.1016/j.dss.2011.09.002

Lane, B. R., Lacey, D., Stanton, N. A., Matthews, A., & Salmon, P. M. (2018). The dark side of the net: Event Analysis of Systemic Teamwork (EAST) applied to illicit trading on a darknet market. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *62*, 282-286. doi: 10.1177/1541931218621065

Lane, B. R., Salmon, P. M., Cherney, A., Lacey, D., & Stanton, N. A. (2019). Using the Event Analysis of Systemic Teamwork (EAST) broken-links approach to understand vulnerabilities to disruption in a darknet market. *Ergonomics*, *62*, 1134-1149. doi: 10.1080/00140139.2019.1621392

Leveson, N. G. (2004). A new accident model for engineering safer systems. *Safety Science*, *42*, 237-270. doi: 10.1016/S0925-7535(03)00047-X

Leveson, N. G. (2011a). Applying systems thinking to analyze and learn from events. *Safety Science*, *49*, 55-64. doi: 10.1016/j.ssci.2009.12.021

Leveson, N. G. (2011b). Engineering a safer world: Systems thinking applied to safety. Cambridge, Massachuesetts: MIT Press.

Leveson, N. G. (2017). Rasmussen’s legacy: A paradigm change in engineering for safety. *Applied Ergonomics*, *59*, 581-591. doi: 10.1016/j.apergo.2016.01.015

Li, C., Tang, T., Chatzimichailidou, M. M., Jun, C. T., & Waterson, P. (2019). A hybrid human and organisational analysis method for railway accidents based on STAMP-HFACS and human information processing. *Applied Ergonomics*, *79*, 122-142. doi: 10.1016/j.apergo.2018.12.011

Parnell, K., Stanton, N. A., & Plant, K. L. (2017). What's the law got to do with it? Legislation regarding in-vehicle technology use and its impact on driver distraction. *Accident Analysis and Prevention*, *100*, 1-14. doi: 10.1016/j.aap.2016.12.015

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*, 226-241. doi: 10.1111/risa.12844

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*, 193-213. doi: 10.1016/S0925-7535(97)00052-0

Read, G. J. M., Naweed, A., & Salmon, P. M. (2019). Complexity on the rails: A systems-based approach to understanding safety management in rail transport. *Reliability Engineering and System Safety*, *188*, 352-365. doi: 10.1016/j.ress.2019.03.038

Read, G. J. M., Salmon, P. M., & Lenné, M. G. (2013). Sounding the warning bells: The need for a systems approach to understanding behaviour at rail level crossings. *Applied Ergonomics*, *44*, 764-774. doi: 10.1016/j.apergo.2013.01.007

Read, G. J. M., Salmon, P. M., Lenné, M. G., & Stanton, N. A. (2015). Designing sociotechnical systems with cognitive work analysis: Putting theory back into practice. *Ergonomics*, *58*, 822-851. doi: 10.1080/00140139.2014.980335

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*, 216-238. doi: 10.1177/0022427811425539

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*, 4-37. doi: 10.1080/01402390.2014.977382

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*, 256-286. doi: 10.1002/pam.2056

Salmon, P. M., Cornelissen, M., & Trotter, M. J. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*, *50*, 1158-1170. doi: 10.1016/j.ssci.2011.11.009

Salmon, P. M., Lane, B. R., Desmond, D., Cherney, A., Kulatilleke, G., Matthews, A., Lacey, D., & Stanton, N. (2019). Breaking bad systems with human factors and ergonomics: Using Work Domain Analysis to identify strategies to disrupt trading in dark net marketplaces. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*, 458-462. doi: 10.1177/1071181319631315

Salmon, P. M., Read, G. J. M., & Stevens, N. J. (2016). Who is in control of road safety? A STAMP control structure analysis of the road transport system in Queensland, Australia. *Accident Analysis and Prevention*, *96*, 140-151. doi: 10.1016/j.aap.2016.05.025

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*, 2119-2126. doi: 10.1111/risa.13309

Schmid, D., Vollrath, M., & Stanton, N. A. (2018). The System Theoretic Accident Modelling and Process (STAMP) of medical pilot knock-out events: Pilot incapacitation and homicide-suicide. *Safety Science*, *111*, 58-71. doi: 10.1016/j.ssci.2018.07.015

Shergold, P., Seidel, B., Gannon, M., & Lim, K.-S. (2017). Final report: Independent review of health providers’ access to Medicare card numbers. Available: <https://www.humanservices.gov.au/organisations/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers>

Shorrock, S. T., & Williams, C. (2016). Human factors and ergonomics methods in practice: Three fundamental constraints. *Theoretical Issues in Ergonomics Science*, *17*, 1-15. doi: 10.1080/1463922X.2016.1155240

Stanton, N. A., Harvey, C., & Allison, C. K. (2019). Systems Theoretic Accident Model and Processes (STAMP) applied to a Royal Navy Hawk jet missile simulation exercise. *Safety Science*, *113*, 461-471. doi: 10.1016/j.ssci.2018.12.020

Stanton, N. A., Salmon, P. M., Rafferty, L. A., Walker, G. H., Baber, C., & Jenkins, D. P. (2013). *Human factors methods: A practical guide for engineering and design* (2nd ed.). Surrey, England: Ashgate.

Sulaman, S. M., Beer, A., Felderer, M., & Höst, M. (2019). Comparison of the FMEA and STPA safety analysis methods: A case study. *Software Quality Journal*, *27*, 349-387. doi: 10.1007/s11219-017-9396-0

Thatcher, A., Waterson, P., Todd, A., & Moray, N. (2018). State of science: Ergonomics and global issues. *Ergonomics*, *61*, 197-213. doi: 10.1080/00140139.2017.1398845

Underwood, P., & Waterson, P. (2014). Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. *Accident Analysis and Prevention*, *68*, 75-94. doi: 10.1016/j.aap.2013.07.027

Underwood, P., Waterson, P., & Braithwaite, G. (2016). ‘Accident investigation in the wild’ – A small-scale, field-based evaluation of the STAMP method for accident analysis. *Safety Science*, *82*, 129-143. doi: 10.1016/j.ssci.2015.08.014

Vijaya Geeta, D. (2011). Online identity theft – an Indian perspective. *Journal of Financial Crime*, *18*, 235-246. doi:10.1108/13590791111147451

Watson, J. M., Lacey, D., Kerr, D., Salmon, P. M., & Goode, N. (2019). Understanding the effects of compromise and misuse of personal details on older people. *Australasian Journal of Information Systems*, *23*, 1-29. doi: 10.3127/ajis.v23i0.1721

Watson, J. M., Salmon, P. M., Lacey, D., & Kerr, D. (2018). Continuance in online participation following the compromise of older adults’ identity information: A literature review. *Theoretical Issues in Ergonomics Science*, *19*, 637-657. doi: 10.1080/1463922X.2018.1432714

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*, 315-331. doi: 10.1080/10658980701788165

Table 1

*Analyst Expertise and Publications on Systems Thinking, Criminology, and the Darknet*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Participant | Qualification level | Experience in criminology (years) | Experience in systems thinking (years) | Experience in darknet (years) | Peer-reviewed papers published on darknet or criminology | Peer-reviewed papers published on systems thinking | Total citationsa | h-indexa |
| 1 | PhD (psychology) | 3 | 3 | 3 | 3 | 3 | 68 | 4 |
| 2 | PhD (human factors) | 4 | 14 | 4 | 4 | >150 | 5320 | 41 |
| 3 | MA (Russian studies) | 26 | 2 | 10 | 3 | 1 | 0 | 0 |
| 4 | PhD (criminology) | 16 | 3 | 3 | 16 | 1 | 864 | 17 |
| 5 | Post Graduate Diploma (Intelligence) | 24 | 0 | 7 | 0 | 0 | 0 | 0 |
| 6 | PhD (systems) | 0 | 4 | 0 | 0 | 11 | 170 | 8 |
| 7 | PhD (human factors) | 0 | 29 | 2 | 2 | >150 | 10,206 | 52 |

Table 2

*The Number of Entities, Control Mechanisms, and Feedback Mechanisms Identified in the Existing Australian Identity Crime Control Structure*

|  |  |  |  |
| --- | --- | --- | --- |
|  | Entities | Control mechanisms | Feedback mechanisms |
| International Context | 5 | 6 | - |
| Parliament and Legislators | 7 | 7 | - |
| Government Agencies | 24 | 20 | 9 |
| Operational Delivery and Management | 32 | 18 | 19 |
| Local Management and Supervision | 14 | 17 | 13 |
| Operating Process and Environment | 12 | 13 | 20 |

Table 3

*An Excerpt of the Systems-Theoretic Process Analysis (STPA) of the Control Mechanisms in the Australian Identity Crime Control Structure*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control mechanism | Action required but not provided | Unsafe action provided | Incorrect timing/order | Stopped too soon/ applied too long |
| *Parliament & Legislators* to *Government Agencies* | | | | |
| Strategy, policy & actions plans | Agencies do not have strategic direction. Non-unified approach to problem. | Agencies focus on unhelpful strategies. | Agencies are unable to respond effectively and efficiently to problems in the darknet. | Insufficient direction. |
| Laws, rules & regulations | Legal framework not in place to support prevention. Boundaries of appropriate agency behaviour not clear. | Laws interfere with agencies' abilities to control problems. | Effectiveness and efficiency compromised. | Out of date laws remain in effect. |
| Funding/resource allocation | Insufficient funding available to combat the problem. | Funding allocated to agencies that do not contribute to addressing the problem. | Funding arrives too late to be effective. | Projects and operations have funding cut and are unable to be completed. |
| *Government Agencies* to *Operational Delivery & Management* | | | | |
| Legal penalties | Legal penalties not applied. | Legal penalties applied incorrectly or inefficiently. | Legal penalties applied to issues that are no longer relevant. | Too little disincentive for darknet users. |
| Research priorities | Research priorities not communicated. | Incorrect research priorities communicated. | Priorities change by the time they are communicated. | Priorities change before research delivers outcomes. |
| Research funding allocation | Research not funded. | Research outside of priority area funded. Advances in knowledge not adequate to address problem. | Funding arrives too late to be effective. | Funding is removed before research outcomes are delivered. |
| *Local Management & Supervision* to *Operating Process & Environment* | | | | |
| Monitoring | Darknet environment not monitored. No awareness of market activity. | Monitoring focuses on aspects of darknet that do not provide full account of activity. | Monitoring occurs during other operations that confound observations. | Monitoring stopped before insights are developed. |
| Assistance | Assistance not received in darknet operations. | Ineffectual assistance received. | Assistance not provided in timely manner. | Assistance not provided long enough or becomes micromanagement. |
| Orchestration | Approach not communicated. | Incorrect approach communicated. | Approach communicated at inappropriate time. | Approach ceased before outcomes or continues too long without outcomes. |

A screenshot of text

Description automatically generated

*Figure 1*. The international entities, Australian parliament and legislators, and Australian government agencies, industry associations, user groups, and other bodies that seek to control identity crime occurring on darknet marketplaces.

A close up of text on a white background

Description automatically generated

*Figure 2*. The entities and control and feedback mechanisms related to operational delivery and management and local management and supervision that address identity crime occurring on darknet marketplaces.

A screenshot of a cell phone

Description automatically generated

*Figure 3*. The operating environment surrounding identity crime and trading occurring on darknet marketplaces.