**Using the Event Analysis of Systemic Teamwork (EAST) broken-links approach to understand vulnerabilities to disruption in a darknet market**

B. R. Lanea\*, P. M. Salmona, N. A. Stantona,b, A. Cherneyc, D. Laceyd

aCentre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Sippy Downs, Australia; bTransportation Research Group, Civil, Maritime and Environmental Engineering and Science Unit, Faculty of Engineering and the Environment, Boldrewood innovation Campus, University of Southampton, Southampton, UK; cSchool of Social Science, University of Queensland, Brisbane, Australia;  dUniversity of the Sunshine Coast, Sippy Downs, Australia

\*Ben Lane, Centre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Locked Bag 4, Maroochydore DC, 4558 QLD, Australia. E-mail: blane@usc.edu.au

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 under the Linkage Grant, ‘Optimising illicit dark net marketplace interventions’ [number LP160100277].

<https://doi.org/10.1080/00140139.2019.1621392>

**Using the Event Analysis of Systemic Teamwork (EAST) broken-links approach to understand vulnerabilities to disruption in a darknet market**

Darknet markets provide an anonymous, online platform for users to trade illicit drugs, fraudulent identity data, and other commodities. Although law enforcement agencies have been successful in seizing many markets, the Darknet is an agile and dynamic environment and market activities often persist and emerge in a new form. Given this constantly changing environment, new ways of disrupting darknet markets are required. This study used Event Analysis of Systemic Teamwork (EAST) to analyse market activity and understand vulnerabilities to disruption. This involved using the EAST broken-links approach to assess the effects of compromising the transmission of information between tasks and between agents. The analysis identified critical vulnerabilities in the system, which included information involved in registering, depositing funds, communicating listing details to buyers, and communicating dispute resolution messages. This study is a proof-of-concept that EAST can provide insight into vulnerabilities within darknet markets that can be exploited by law enforcement.

Keywords: broken links; cryptomarket; Darknet; Event Analysis of Systemic Teamwork; sociotechnical systems

Practitioner Summary: This study provides a conceptualisation of the processes, people, structures, and information involved in the buying and selling of goods on a darknet market. Law enforcement agencies may use broken-links analyses to systematically consider the effects of their interventions.

# Introduction

The Darknet is an alternate layer of the Internet, accessible using anonymising software, such as The Onion Router (TOR), which disguises user activity. One of the revolutions brought about by the Darknet has been in allowing users to transact anonymously when used in conjunction with cryptocurrencies. Markets on the Darknet consequently provide a venue for buying and selling illicit goods, including drugs, weapons, and fraudulent personal identity documents and information. Transactions span continents (Broséus et al. 2017) and market administrators have been known to earn millions of dollars in illicit profits (US Department of Justice 2017).

Since the conception of darknet markets, law enforcement agencies have been involved in various disruption efforts. Silk Road, the first major market, was shut down in 2013 and new markets and vendor stores subsequently emerged. Operation Onymous sought closure of these markets, successfully resulting in the closure of 410 hidden services and arrest of 17 vendors and administrators (Europol 2014). Operation Bayonet resulted in the closure of AlphaBay, the largest market yet, and users were lured to Hansa Market, which was under the control of Dutch law enforcement. Many users’ details were captured as a result (Europol 2017). However, researchers have questioned the effectiveness of market closures in causing long-term disruption (Buxton and Bingham 2015; Décary-Hétu and Giommoni 2017; Soska and Christin 2015; Van Buskirk et al. 2014). Although vendor activity decreased following Operation Onymous, after a month the activity recovered and buyer consumption continued an upward trend (Décary-Hétu and Giommoni 2017).

Market disruptions may also have unintended emergent effects. An analysis of the seizure of the original Silk Road suggested that, having decreased trust in the existing system, it likely initiated development of escrow technologies, which provide buyers with a level of protection against scams by having a third party hold payment until the buyer and seller confirm the goods have been delivered (Horton-Eddison and Di Cristofaro 2017). Subsequent operations were followed by security improvements, including message encryption and two-factor authentication (Buxton and Bingham 2015; Décary-Hétu and Giommoni 2017). In addition to such innovations, it has been argued that Operation Onymous contributed to reduced focus on intermarket competition and hacking, leading to greater focus of individual markets on improving their own security (Moeller, Munksgaard, and Demant 2017). The dynamic and agile nature of the Darknet engenders a need also for interventions to be dynamic, agile and constantly evolving. Given the evidence suggests that existing disruption efforts have done little to stop market operations long-term and may spur technological innovation, new strategies are needed that result in lasting and effective disruption while minimising the potential for users to pursue innovation.

Ergonomics methods have been primarily used to identify ways to optimise systems and enhance human wellbeing (International Ergonomics Association 2000). Salmon, Carden, and Stevens (2018), however, discuss the potential for using systems ergonomics methods to identify ways in which to compromise (and thus potentially disrupt) systems that are designed for illicit ends. Methods such as Cognitive Work Analysis (CWA; Vicente 1999) and Event Analysis of Systemic Teamwork (EAST; Stanton et al. 2013) provide the capability to describe entire systems, their component parts, and more importantly the relationships and interactions between these parts. Whilst the detailed and rich outputs are typically used to support the optimisation of systems, it is precisely these features that provide an opportunity to also inform the disruption of systems.

Salmon et al. (2018) demonstrated this by using Work Domain Analysis, the first phase of CWA, to identify ways to disrupt terrorist cells. This form of analysis represents a new endeavour for ergonomics that potentially may be pursued in other areas to inform the development of interventions which aim to disrupt systems that are used for illicit purposes (e.g., the Darknet, child sexual abuse). As a new direction for ergonomics, further applications are required in different contexts and using other systems ergonomics methods.

The present study achieves this by using the EAST broken-links method (Stanton and Harvey 2017) to model a darknet market, Dream Market, and identify ways in which vulnerabilities could potentially be exploited to prevent illicit trading of identities. The primary purpose was to develop recommendations for law enforcement agencies designed to assist in the prevention of trading in darknet markets. The secondary purpose was to confirm the potential utility of using systems ergonomics to disrupt systems which support illicit activities. The study represents the first application of systems ergonomics methods within darknet environments, and builds on recent work in which such methods have been used in a disruptive capacity.

## Event Analysis of Systemic Teamwork

EAST (Stanton et al. 2013) provides a framework for describing complex systems and the activities and interactions that occur within them. Recent applications of EAST have involved developing task, social, and information networks (Banks and Stanton 2017; Banks et al. 2018; Stanton and Harvey 2017; Stanton and Roberts 2017) and combining them into a composite network to show the relationships between tasks, agents, and information (Stanton 2014). Network analysis metrics are also typically applied to describe the system and determine key tasks, agents, and information. Protecting the anonymity of the communication of information is central to the operation of the Darknet and therefore EAST was considered appropriate for this domain.

Studies have applied EAST across multiple domains, including submarine control (Stanton 2014), road and rail transport (Banks and Stanton 2017; Banks et al. 2018; Salmon et al. 2014, In Press), search and rescue (Plant and Stanton 2016), air traffic control (Walker et al. 2010), various military domains (Stanton and Harvey 2017; Stanton, Rafferty, and Blane 2012; Walker et al. 2009), and identity theft (Lacey and Salmon 2015; Lane et al. In Press). Studies typically focus on analysing networks to identify modifications designed to support effective functioning and safety management. To date the framework has not yet been applied to comprehensively identify ways in which to exploit vulnerabilities and thus promote disruption of the system and activities.

Stanton and Harvey (2017) recently introduced the broken-links analysis component to enable EAST to be used for risk assessment purposes. The broken-links approach models the effects of communication breakdowns within the task, social and information networks and is used to identify key vulnerabilities within the system under analysis. Stanton and Harvey used the approach to develop mitigation strategies. However, the identification of vulnerabilities, via broken links, potentially provides useful information for disruption in the context of the Darknet. That is, by applying the EAST broken-links approach it may be possible to identify critical vulnerabilities that could be actively exploited by law enforcement agencies. As such, an EAST broken-links analysis could provide a systematic consideration of the potential intervention targets and outcomes in the Darknet system.

## EAST Dream Market broken-links study

The aim of the study was to first describe the key tasks, social agents, and information involved in the buying and selling of goods on a darknet market, and second to use the EAST broken-links method to identify critical vulnerabilities and potential disruption interventions. The scope of the analysis was the overall process of buying or selling goods on Dream Market, beginning with account creation and continuing to the finalisation of a transaction for both buyers and vendors. Whilst the aims of the analysis centre around identifying vulnerabilities in darknet markets, the analysis also acted as a proof-of-concept study to determine whether or not EAST could be usefully applied as a tool to disrupt, as well as optimise, a unique sociotechnical system such as the darknet. Verification of this method opens up various additional areas in which EAST could be applied to develop strategies for disrupting systems designed to achieve illicit ends.

Method

## Research context

This study was based on the largest and oldest active darknet market at the time of writing, Dream Market. Dream Market was established in November 2013. Although run by administrators, all product and service listings are provided by independent users, who sign up for vendor status. When other users purchase products, funds typically are held in an escrow service, which requires two users out of the vendor, market staff, and buyer to confirm the product has been delivered before the funds are released to the vendor. Users avoid detection by using a virtual private network in conjunction with TOR software and payment in cryptocurrency. On 19 January 2018, Dream Market featured approximately 97 thousand listings, predominantly drugs and fraudulent identity data. The market expressly forbids the sale of assassination services, weapons, poisons, child pornography, and violent live action audio and visual recordings or images.

## Data collection

Working in conjunction with a third-party organisation, which works with law enforcement to monitor darknet markets, screenshots of Dream Market and forums for our source data were collected (e.g., see Figure 1). About 40 screenshots were used in total. The boundary of the analysis was restricted to the activities undertaken by buyers and sellers and the information that could be gained from publicly available sources without direct interaction with other human agents (e.g., by messaging vendors, buyers, or market staff). Therefore, limited detail was available on private interactions between users, such as in dispute negotiations and elements of the buying and selling processes, such as receipt of products and additional communications between buyers and vendors.

[Figure 1 near here]

To allow secure access to the Darknet, the operator used a configured personal computer with appropriate software to permit anonymous browsing. The computer was not used for any purpose other than darknet monitoring and was connected to a separate internet network. No personal details of operators were entered into the market or the designated computer.

## Data analysis

Initially, a Hierarchical Task Analysis (HTA; Stanton, 2006) of buying and selling illicit goods was constructed in Microsoft Notepad. HTA provides a detailed description of the activity under investigation and is typically used as the input for EAST analyses (Stanton et al. 2013). Following this, EAST task, social, and information networks were constructed in Microsoft Visio. To identify nodes, one analyst initially assessed each screenshot and coded items relevant to each of the networks. For example, in forming the HTA and task network, screenshots of the forums, vendor profiles, and product listings were coded as relating to the goal of assessing vendor reputation given the availability of relevant information in these locations. A second analyst with expertise in darknet markets validated the coding and an additional three other analysts worked through about 20% of the coding in a later workshop as a further validation.

The social agents involved in these tasks were then identified, in this case the forum, the user types contributing on the forum, the vendor’s profile, and the product listing. Agents were defined as physical entities that hold and transfer information, both human and nonhuman.

To form the information network, concepts associated with the buying and selling of goods and services were identified. The general type of information rather than the specific text was coded, for example, the text on a product listing, ‘Yahoo hacked mails packs 500/1000+ pcs’ was coded as ‘product title’. Each piece of information was a noun-like word or phrase, after Griffin et al. (2015). After establishing these components, one analyst systematically assessed them to ensure they represented a piece of information rather than a social entity, process, or abstract idea.

Links between tasks were determined by systematically considering the potential progression from each node to every other node. For example, when a user browses the listings, they may then navigate to a different product category, use the search function again, or assess a particular listing. At that point, they would not create an account again or directly assess a vendor’s reputation.

Links between social agents were created based on the communication flows identified in the HTA as necessary for completion of each task. For example, to complete registration and browse listings, a user must interact with the registration form, navigation panel or search form, and the product listings themselves. Whereas the user both inputs and receives information from the navigation panel, search form, and registration form (two-way links), the user is only a passive recipient of information from the product listing (a one-way directional link).

Links in the information networks were formed when additional information was required for comprehension and when additional information influenced, or was influenced by, other information. For example, product reviews are only informative when connected with a product title and username, but are also influenced by the product’s price, description, and actual qualities once received. Therefore, product reviews link with all the mentioned nodes.

Following development of each network, network analyses were conducted and composite networks were created for each phase. To conduct the network analyses, connections between nodes were converted to a matrix format and the data were inputted to the Agna (version 2.1) and SocNetV (version 2.4) network analysis software. Several analyses were conducted on those applied in previous EAST studies (Banks and Stanton 2017; Salmon et al., In Press; Stanton 2014; Stanton and Harvey 2017). These metrics included those describing the overall system: density, diameter, cohesion, and the number of edges and nodes (see Table 1). The metrics also included those describing individual nodes: sociometric status, degree centrality, betweenness centrality, eigenvector centrality, emission, and reception. Key nodes were identified when their metric value exceeded the mean and one standard deviation (Stanton and Harvey 2017). For the information networks, a hierarchical clustering analysis was also conducted using distances as the input matrix, Euclidean distance as the distance metric, and average-linkage as the clustering method. The resulting clusters were organised based on levels that were thematically meaningful.

[Table 1 near here]

The composite networks were constructed by systematically considering whether tasks and social agents across the phases required each piece of information. For example, it was identified that creating an account (task) required a password, PIN, registration status, username, and captcha (information). The analysis was presented in task-information and agent-information matrices, which were used for the broken-links analysis. The broken-links analysis involved breaking each of the relationships in the composite networks and considering the impact on task performance when information was not transmitted between two tasks or two agents. Four analysts initially conducted the analysis for an initial phase of tasks and actors in a one-day workshop and one analyst subsequently completed the remainder. All analysts had a PhD, with two in ergonomics, one in psychology, and one in criminology and information systems. All analysts had prior experience in applying EAST and two had significant expertise. A further two subject matter experts, who worked in Australian criminal intelligence organisations, reviewed the analysis and provided feedback. All analysts reviewed the final analysis and disagreements were resolved through further discussion.

Results

## Task, social, and information networks

Based on the HTA, three key phases of trading were identified, comprising the activities required to:

1. create an account, search listings, and assess the marketplace;
2. deposit cryptocurrency, register as a vendor, list a product, and build reputation; and
3. buy and sell a product.

The task networks are presented in Figure 2 and the associated network analysis is presented Table 2. Please note that the layout of each network diagram was chosen to maximise clarity and does not reflect the level of association between nodes. There were 8 tasks in Phase 1, 8 in Phase 2, and 11 in Phase 3. Phase 1 can be completed in a linear fashion, although there are several tasks that may feedback into earlier tasks. Phase 2 begins in a linear fashion, but then shifts into a dynamic process of listing products and then developing reputation. Phase 3 similarly begins linear, but then becomes dynamic as users seek validation that their order is being processed and moving into order disputes as and when required.

[Table 2 and Figure 2 near here]

The social networks represent the interactions of human and nonhuman agents (see Figure 3). There were 12 agents in Phase 1, 13 in Phase 2, and 13 in Phase 3. In all phases, users interacted with a combination of static webpages and communication media, such as forums. The provision of information by webpages was especially common in Phase 2, whereas Phase 3 featured communication mediums more heavily. The network analysis is presented in Table 3.

[Table 3 and Figure 3 near here]

Information networks for the phases are presented Figure 4. There were 29 information pieces in Phase 1, 35 in Phase 2, and 26 in Phase 3. In each phase, information typically clustered according to involvement in common tasks, although some information was required in the context of multiple tasks. For example, the username is required in the continuity between browsing listings, assessing listings, and assessing vendor reputation. The network analysis is presented in Table 4 and the hierarchical clusters are presented in Table 5. In Phase 1, there were thematic clusters regarding user accounts, product listing details, reputational information, and website features. In Phase 2, the thematic clusters included monetary transactions, account status, user settings and reputation (username featured across these latter two), and product listing details. Forbidden products and services was identified as a separate piece of information. Phase 3 included reputational information, order processing details, product listing details, and encryption.

[Tables 4 and 5 and Figure 4 near here]

## Broken-links analysis

Following Stanton and Harvey (2017), the broken-links analysis reveals the immediate effects of disrupting each piece of information in transitions between tasks and communications between agents. The basis of the broken-links analysis was the task-information and agent-information matrices, presented in Tables 6 and 7, respectively. Each broken link represents a communication failure, which can be used to predict possible outcomes in the system (Stanton and Harvey 2017). Given the large number of broken links identified, each one was assessed as to whether it would have a low, medium, or high impact on the Dream Market system. The criteria used for this judgement included:

1. Low impact. Defined as a broken link that would be unlikely to have more than minimal effects on market activities in that market activities could continue without the information. For example, when a buyer communicates on the forum, failure to communicate their avatar contributes to missing identity information, but otherwise does not affect market activity.
2. Medium impact. Defined as a broken link that had the potential to affect market activities and sales in that necessary information was incomplete but market activities could continue. For example, in communication from a vendor’s profile to a buyer, missing profile text may dissuade the buyer from making a purchase from that vendor.
3. High impact. Defined as a broken link that was highly likely to prevent a sale or disrupt effective market functioning. For example, in a buyer’s communication with a tumbling service, failure to transmit the Dream Market destination cryptocurrency address would mean the buyer cannot deposit funds and cannot engage in purchases.

These thresholds were chosen to facilitate accurate classification of the broken links while also accommodating categories likely to be useful for end users. Overall, there were 802 possible broken links identified and rated, with 388 (48%) being classified as low impact, 312 (39%) classified as medium impact, and 102 (13%) classified as high impact.

[Tables 6 and 7 near here]

To illustrate the broken-links analysis, an example can be described based on the relationship between the vendor and the product listing. These agents share information on packaging, product qualities, price, escrow option, product image, product description, title, and shipping details. Given the directional link between the two, the vendor must supply this information to the product listing to support the goals of the system. Table 8 demonstrates the outcomes that occur if this information is not transmitted. The vendor is a key agent by sociometric status across all phases and the product listing features in several key tasks. Table 8 also features communications between the forum and the buyer, the consequences of the broken links, and an intervention necessary to cause the broken link. Although the relationship is reciprocal, information flow from the forum to buyers is particularly important in the system’s operation. Information communicated includes usernames, product reviews, product descriptions, product titles, vendor reviews, and product adverts. Both the buyer and forum are key agents by sociometric status and centrality in Phases 1 and 3 and the buyer by sociometric status in Phase 2.

From a task-oriented perspective, the network was analysed to consider what would occur if information did not transmit from one task to another. Table 9 considers the reciprocal relationship between negotiating a solution and creating a formal dispute. Negotiating a solution is a key task by sociometric status in Phase 3. To progress from negotiating a solution to creating a formal dispute, information transmitted includes order status, order details, username, solution, and dispute message. Through considering the outcomes, it is evident that progressing to a formal dispute relies on much of the information created in initial negotiations to be processed effectively. After the formal dispute is initiated, information about the order as well as the vendor’s reputation are necessary to conduct further negotiations. Although this information is created in previous tasks, such as creating a listing and ordering a product, the information must still be available at these later stages for the system to function. Failure of information transmission from the negotiation of the solution to other tasks, such as discussion on forums or sending messages, has the potential for significant aftereffects given that multiple users rely on such information in making decisions on the marketplace. For example, buyers decide whether to purchase from a particular vendor and whether to trust the system generally, and moderators use the information to inform future dispute resolution involving these users.

[Tables 8 and 9 near here]

Discussion

This study used EAST in a first-of-its-kind analysis to describe and analyse the tasks, agents, and information involved when buying and selling on Dream Market, a darknet market, and analysed the effects of preventing information transmission during the required tasks and interactions. Previous darknet market research has investigated factors related to product characteristics and dynamics (Broséus et al. 2017; Décary-Hétu and Giommoni 2017) and the characteristics of users (Barratt, Ferris, and Winstock 2016). However, limited research has explored the processes underlying illicit trading on the Darknet (Hutchings and Holt 2015; Lacey and Salmon 2015; Lane et al. 2018). This study helps address this knowledge gap. The study also affirms the potential that systems ergonomics methods can be used to identify vulnerabilities that may be exploited to disrupt the functioning of a particular system (darknet marketplace) which expands the literature which has typically focused on improving systems in areas such as transport (Banks and Stanton 2017; Banks et al. 2018; Salmon et al. 2014, In Press), defence (Stanton and Harvey 2017; Stanton, Rafferty, and Blane 2012; Walker et al. 2009), and search and rescue (Plant and Stanton 2016). This further confirms the utility of systems ergonomics for disrupting, as opposed to optimising, complex systems (Salmon et al., 2018).

The broken-links analysis has implications for the development of interventions for disrupting darknet markets as well as other nefarious activities. The analysis provides a systematic consideration of consequences of information transmission failures throughout the system and the classification of low, medium, and high impact breaks provides a suite of potential targets. In particular, the broken links classified as high impact show that there are numerous potential interventions that could halt market activity. The network metrics provide further empirical support for interventions and the likely extent of systemic effects of particular breaks. The question now raised is how these specific transmission failures can be facilitated by law enforcement. Notably, nearly all the identified broken links require interventions that prevent information from displaying on the marketplace website. This may be achieved by either introducing bugs into the website itself or taking control of user accounts and removing key information from profiles, forums, and listings. Whilst each of the strategies might have been identified by other means, the systematic approach offered by EAST means that the system may be considered in a more comprehensive and holistic manner.

It is important to note that the extent of interventions currently occurring in darknet markets is unknown from an academic perspective. Researchers have documented some strategies, such as Sybil attacks in which an actor creates multiple user identities and uses these identities to provide positive feedback to each other (Hutchings and Holt 2017). The identities then use their reputation to entice sales from real buyers and simply fail to deliver, which is intended to create a general sense of distrust on the market in vendors with supposedly good standing. Although law enforcement agencies internationally are likely to be engaged in numerous darknet operations, structured guidance is useful in determining which approaches are likely to have the greatest impact. For example, across all phases of the analysis, the metrics suggest that changes to usernames would result in significant disruption to the system. The username connects with all reputation-based indicators and allows users to make quick decisions regarding a vendor's trustworthiness. Indeed, consistent with the results of the clustering analysis, research has identified that usernames, product titles, and other listing qualities work in conjunction to form a vendor’s brand (Afilpoaie and Shortis 2015). If the marketplace no longer links product reviews or descriptions with a vendor username, vendors would lose the advantages conferred by their branding. Furthermore, in considering broken links associated with username, much of the other information involved loses meaning without the context of an individual user account.

Price and funds are also key components in the darknet system and the broken-links analysis showed that interventions involving these components are likely to cause significant disruption. If users are unable to deposit or access funds, their activity on the market is halted. Disruptions can already be observed with some users of Dream Market posting on Reddit that Bitcoin had disappeared from their wallet. It is suspected that this occurs due to users becoming victims of phishing scams and law enforcement agents may arrange similar scams to enact such disruptions. Additional natural disruptions have occurred due to the fluctuating nature of cryptocurrency. Although a price in AUD may remain the same, the value of the payment currency can demonstrate considerable fluctuation. In 2017, Bitcoin rose in value from US$1000 to over US$19000, before varying between US$13000 and US$17000 in January 2018 (Coindesk 2018). Buyers experience dramatic changes in their spending power as a result.

There are numerous other potential interventions identified through the broken-links analysis. In the task of developing a profile, if the information is not created, engagement on forums and profile development will be stilted. In interacting on forums, failure to communicate usernames and avatars creates difficulties in signalling identity. This problem is shared in product listings broadcasting information to users. There may be the added complication of not being able to link reputation information to user identities. Complications arise if various market components do not provide relevant information to users, but also if market components do not provide information for other market operations. For example, the order page must communicate with the escrow system to initiate transfer of funds. Likewise, the user’s wallet on Dream Market must communicate with both the order page and escrow for the system to recognise whether sufficient funds are available and how much the new balance should be. Furthermore, if the tumbling service does not transmit to Dream Market’s wallet system, the status of deposits would be unknown, the funds would not transfer, and they may even be sent to a different address.

As a first-of-its-kind study testing the efficacy of the interventions identified was not possible. Further ongoing work as part of the wider program of research will refine, test, and evaluate the interventions identified. Further research by others focusing on how law enforcement can produce the greatest effects on market activity is also recommended.

When contemplating the potential effects following any of the disruptions identified, it is likely that the marketplace system would adapt. For example, administrators develop and implement solutions to bypass issues, and users migrate to other markets and develop other means of communication and transaction. Sustained disruption of different targets or concurrent disruption of multiple targets may be avenues to consider in making change in this dynamic environment. Using multiple interventions target different vulnerabilities simultaneously may also hinder marketplaces ability to respond and adapt. Further research should therefore explore the likely emergent effects of the disruptions, including marketplace adaptations. This could involve using EAST to model new tasks, agents, interactions, and information that might emerge in response to the disruptions. Alternatively, Read et al. (2017) used Work Domain Analysis (WDA), the first phase of CWA, to identify positive and negative emergence following the introduction of new railway level crossing treatments. This involved inserting objects (e.g., in-vehicle displays) into the bottom level of the WDA and identifying emergent effects throughout the abstraction hierarchy (e.g., driver distraction). A similar approach could be used in conjunction with EAST.

## Limitations and future directions

The analysis revealed information on the steps required for an individual to begin using a market and to buy and sell product. However, information on the intricacies of building reputation, delivery and retrieval of products, and dispute resolution remains limited. This is a limitation of the use of market screenshots in informing the analysis. Potentially, in assessing the impact of disruption strategies and in building understanding, an observational or action research approach could be used. For example, researchers could engage in vending on a darknet market, although this would require law enforcement agency endorsement. Another future direction is to consider the perspectives of administrators and moderators in the system. There have been numerous examples of cases where administrators have withheld information, such as plans to commit an exit scam whereby they steal large amounts of cryptocurrency from market users. The consideration of such information has implications for understanding users trust in the system and the motivations for engaging in certain behaviours.

In considering the methodology itself, the broken-links approach was designed with cooperation in mind and was considered applicable to any sociotechnical system for which an EAST model had been developed (Stanton and Harvey 2017). Given the novelty of applying the approach to disrupt a system, it is likely that the method could be refined. For example, instead of only considering the failure to transmit information between tasks or agents, the approach could consider the effects of manipulations or alterations of information. Communication of false information may have greater impacts than lack of communication due to resulting uncertainty and frustration. Indeed, Stanton and Harvey (2017) suggested that the method could be extended by adding nodes and links as well as breaking multiple links simultaneously. In contrast, in keeping with the original design of EAST, research may also consider the communication and cooperation requirements of law enforcements agents engaging in the system. These activities are not modelled in the current version of the EAST networks. Various agencies seek to maintain security of classified information to help maximise effectiveness of their interventions. However, this approach can be problematic, as it creates difficulty for deconfliction. Agencies may not be aware of the interventions, strategies, and other endeavours undertaken by allied forces.

## Conclusion

The key outcomes of this study are an analysis of the components in the darknet market system and thorough consideration of the likely effects of low, medium, and high impact broken links in the system. The study indicates that there are numerous key components in the system that law enforcement interventions may target to achieve disruption. These findings may have implications for the design of future intervention efforts. The findings also provided a proof-of-concept that the EAST broken-links approach can be used to model intentional disruption of a system. Future research should seek to extend the method and undertake simulated attacks on networks to see if the anticipated disruption actually occurs.

References

Afilipoaie, A., and P. Shortis. 2015. "The Growing Industry of Darknet Marketing." Global Drug Policy Observatory Situation Analysis. http://www.swansea.ac.uk/media/GDPO%20SA%20Marketing.pdf

Banks, V. A., and N. A. Stanton. 2017. “Analysis of Driver Roles: Modelling the Changing Role of the Driver in Automated Driving Systems using EAST.” *Theoretical Issues in Ergonomics Science*. Advance online publication. doi: 10.1080/1463922X.2017.1305465

Banks, V. A., N. A. Stanton, G. Burnett, and S. Hermawati. 2018. “Distributed Cognition on the Road: Using EAST to Explore Future Road Transportation Systems.” *Applied Ergonomics* 68: 258-266. doi: 10.1016/j.apergo.2017.11.013

Barratt, M. J., J. A. Ferris, and A. R. Winstock. 2016. “Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence.” *International Journal of Drug Policy* 35: 24-31. doi: 10.1016/j.drugpo.2016.04.019

Bradbury, D. 2014. "Unveiling the Dark Web." *Network Security* 2014(4): 14-17. doi: 10.1016/S1353-4858(14)70042-X

Broséus, J., D. Rhumorbarbe, M. Morelato, L. Staehli, and Q. Rossy. 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

Buxton, J., and T. Bingham. 2015. "The Rise and Challenge of Dark Net Drug Markets." Global Drug Policy Observatory Policy Brief 7. https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf

Coindesk. 2018. “Bitcoin (USD) Price.” https://www.coindesk.com/price/

Décary-Hétu, D., and L. Giommoni. 2017. "Do Police Crackdowns disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous." *Crime Law and Social Change* 67: 55-75. doi: 10.1007/s10611-016-9644-4

Europol. 2014. “Global action against dark markets on TOR network.” https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network

Europol. 2017. “Massive blow to criminal dark web activities after globally coordinated operation.” https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

Griffin, T. G. C., M. S. Young, and N. A. Stanton. 2015. *Human Factors Models for Aviation Accident Analysis and Prevention*. Surrey, England: Ashgate.

Horton-Eddison, M., and M. Di Cristofaro. 2017. "Hard Interventions and Innovations in Crypto-Drug Markets: The Escrow Example." Global Drug Policy Observatory Policy Brief 11. http://www.swansea.ac.uk/media/Escrow\_PB11\_GDPO\_AUGUST2017.pdf

Houghton, R. J., C. Baber, R. McCaster, N. A. Stanton, P. Salmon, R. Stewart, and G. Walker. 2006. “Command and Control in Emergency Services Operations: A Social Network Analysis.” *Ergonomics* 49(12-13): 1204-1225. doi: 1080/00140130600619528

Hutchings, A., and T. J. Holt. 2015. “A Crime Script Analysis of the Online Stolen Data Market.” *British Journal of Criminology* 55: 596-614. doi: 10.1093/bjc/azu106

Hutchings, A., and T. J. Holt. 2017. “The Online Stolen Data Market: Disruption and Intervention Approaches.” *Global Crime* 18(1): 11-30. doi: 10.1080/17440572.2016.1197123

International Ergonomics Society. 2000. “What is Ergonomics?” https://www.iea.cc/whats/index.html

Kalamaras, D. 2015. “The SocNetV Manual: Social Network Visualizer (SocNetV).” http://socnetv.org

Lacey, D., and P. Salmon. 2015. “It’s Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums.” In *Engineering Psychology and Cognitive Ergonomics*, edited by D. Harris, 117-128. doi: 10.1007/978-3-319-20373-7\_12

Lane, B. R., D. Lacey, N. A. Stanton, A. Matthews, and P. M. Salmon. 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

Moeller, K., R. Munksgaard, and J. Demant. 2017. “Flow my FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs.” *American Behavioral Scientist* 61(11): 1427-1450. doi: 10.1177/0002764217734269

Plant, K. L., and N. A. Stanton. 2016. “Distributed Cognition in Search and Rescue: Loosely Coupled Tasks and Tightly Coupled Roles.” *Ergonomics* 59(10): 1353-1376. doi: 10.1080/00140139.2016.1143531

Salmon, P. M., T. Carden, and N. J. Stevens. 2018. “Breaking Bad Systems: Using Work Domain Analysis to Identify Strategies for Disrupting Terrorist Cells.” *Proceedings of Ergonomics and Human Factors 2018*.

Salmon, P. M., G. J. M. Read, G. H. Walker, N. Goode, E. Grant, C. Dallat, T. Carden, A. Naweed, and N. A. Stanton. In Press. “STAMP goes EAST: Integrating Systems Ergonomics Methods for the Analysis of Railway Level Crossing Safety Management.” *Safety Science.* doi: 10.1016/j.ssci.2018.02.014

Salmon, P. M., M. G. Lenne, G. H. Walker, N. A. Stanton, and A. Filtness. 2014. “Using the Event Analysis of Systemic Teamwork (EAST) to explore Conflicts between Different Road User Groups when making Right Hand Turns at Urban Intersections.” *Ergonomics* 57(11): 1628-1642. doi: 10.1080/00140139.2014.945491

Soska, K., and N. Christin. 2015. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." *Proceedings of the 24th USENIX Security Symposium* 24: 33-48. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska.pdf

Stanton, N. A. 2014. “Representing Distributed Cognition in Complex Systems: How a Submarine Returns to Periscope Depth.” *Ergonomics* 57(3): 403-418. doi: 10.1080/00140139.2013.772244

Stanton, N. A., and C. Harvey. 2017. “Beyond Human Error Taxonomies in Assessment of Risk in Sociotechnical Systems: A New Paradigm with the EAST ‘Broken-Links’ Approach.” *Ergonomics* 60(2): 221-233. doi: 10.1080/00140139.2016.1232841

Stanton, N. A., and A. P. J. Roberts. 2017. “Examining Social, Information, and Task Networks in Submarine Command and Control.” *IEEE Transactions on Human-Machine Systems* PP(99): 1-14. doi: 10.1109/THMS.2017.2720659

Stanton, N. A., L. A. Rafferty, and A. Blane. 2012. “Human Factors Analysis of Accidents in Systems of Systems.” *Journal of Battlefield Technology* 15(2): 23-30. http://www.argospress.com/articles/2012/human-factors-analysis-of-accidents-in-system-of-systems

Stanton, N. A., P. M. Salmon, L. A. Rafferty, G. H. Walker, C. Baber, and D. P. Jenkins. 2013. *Human Factors Methods: A Practical Guide for Engineering and Design (2nd Edition)*. Surrey, England: Ashgate.

US Department of Justice. 2017. “Acting Manhatten U.S. Attorney Announces Forfeiture of $48 Million from Sale of Silk Road Bitcoins.” https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins

Van Buskirk, J., A. Roxburgh, M. Farrell, and L. Burns. 2014. "The Closure of the Silk Road: What has this meant for Online Drug Trading." *Addiction* 109(4): 517-518. doi: 10.1111/add.12422

Vicente, K. J. 1999. *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*. Mahwah, New Jersey: Lawrence Erlbaum Associates/

Walker, G. H., H. Gibson, N. A. Stanton, C. Baber, P. Salmon, and D. Green. 2006. “Event Analysis of Systemic Teamwork (EAST): A Novel Integration of Ergonomics Methods to Analyse C4i Activity.” *Ergonomics* 49(12-13): 1345-1369. doi: 10.1080/00140130600612846

Walker, G. H., N. A. Stanton, C. Baber, L. Wells, H. Gibson, P. Salmon, and D. Jenkins. 2010. “From Ethnography to the EAST Method: A Tractable Approach for Representing Distributed Cognition in Air Traffic Control.” *Ergonomics* 53(2): 184-197. doi: 10.1080/00140130903171672

Walker, G. H., N. A. Stanton, R. Stewart, D. Jenkins, L. Wells, P. Salmon, and C. Baber. 2009. “Using an Integrated Methods Approach to Analyse the Emergent Properties of Military Command and Control.” *Applied Ergonomics* 40: 636-647. doi: 10.1016/j.apergo.2008.05.003

### Table 1. Social network analysis metrics.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Metric | Description | Formula |
| Network level | Density | The number of connections as a proportion of the total possible number of connections | $$Density=\frac{T}{N (N-1)}$$ |
|  | Reciprocity cohesion | The number of reciprocal connections relative to the total number of connections | $$Cohesion= \frac{C}{T}$$ |
|  | Diameter | The shortest distance to cross the network from the farthest nodes | $$Diameter=max \{d\left(u, v\right), ∀u, v\in V\}$$ |
| Node level | Sociometric status | The number of emissions and receptions of a node relative to number of nodes overall | $$Status= \frac{1}{g-1}\sum\_{j-1}^{g}(x\_{ji}+ x\_{ij})$$ |
|  | Degree centrality (DC) | Level of connectivity to other nodes | $$DC\_{i}= \sum\_{j}^{}a\_{ij}$$ |
|  | Betweenness centrality (BC) | The frequency that a node lies between pairs of other nodes | $$BC= \sum\_{j<k}^{}\frac{Gjk(Ni)}{Gjk}$$ |
|  | Eigenvector centrality (EC) | A measure of influence taking into account connections to high-scoring nodes | $$EC= \frac{1}{λ}\sum\_{u\in N(v)}^{}x\_{u}= \frac{1}{λ}\sum\_{u\in G}^{}a\_{v,u}x\_{u}$$ |
|  | Emission | The number of connections originating from the node |  |
|  | Reception | The number of connections terminating at the node |  |

*Note.* Formulas and definitions were obtained from Houghton et al. (2006) and Kalamaras (2015).

### Table 2. Task network metrics.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task network | Nodes | Edges | Density | Diameter | Cohesion | Sociometric status  | Degree centrality | Betweenness centrality | Greatest emitters | Greatest receivers |
| Phase 1 | 8 | 23 | .41 | 5 | .43 | Browse listings (1.14) | Assess listings (5), assess vendor reputation (5) | Browse listings (14.00) | Create account (4), browse listings (4), assess listing (5), assess vendor reputation (5) | Navigate to product (5), use search (5), browse listings (4), assess market status (4) |
| Phase 2 | 8 | 22 | .39 | 4 | .73 | List product (1.29), maintain security (1.14), develop profile (1.14) | Maintain security (4), list product (4), develop profile (4) | Maintain security (14.00), send cryptocurrency through tumbler (11.00) | Maintain security (4), list product (4), develop profile (4) | List product (5), develop profile (4), maintain security (4), engage on forums (4) |
| Phase 3 | 11 | 41 | .37 | 5 | .68 | Maintain security (1.40), send message (1.20), negotiate solution (1.20) | Maintain security (7), negotiate solution (7) | Add order details (25.00), maintain security (21.38) | Maintain security (7), negotiate solution (7), send Message (6) | Maintain security (7), send message (6) |

*Note*. Only key nodes are presented for sociometric status, centrality, emission, and reception.

### Table 3. Social network metrics.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Social network | Nodes | Edges | Density | Diameter | Cohesion | Sociometric status | Degree centrality | Betweenness centrality | Greatest emitters | Greatest receivers |
| Phase 1 | 12 | 33 | .25 | 4 | .73 | Buyer (1.0), forum (0.91), prospective vendor (0.91) | Forum (5), news panel (5) | Forum (60.28), buyer (36.00) | Forum (5), news panel (5), buyer (4), prospective vendor (4) | Buyer (7), prospective vendor (6), forum (5) |
| Phase 2 | 13 | 31 | .20 | 4 | .58 | Vendor (1.08), buyer (0.83) | Vendor (6), forum (4) | Vendor (57.50), forum (41.40) | Vendor (7), buyer (4), forum (4) | Vendor (7), buyer (7), forum (4) |
| Phase 3 | 13 | 41 | .26 | 5 | .78 | Buyer (1.00), vendor (0.92), forum (0.83), escrow (0.83) | Vendor (6), forum (5), escrow (5), buyer (4) | Buyer (46.25), vendor (34.25), forum (33.03) | Vendor (6), buyer (5), escrow (5), forum (5) | Buyer (7), forum (5), vendor (5), escrow (5) |

*Note*. Only key nodes are presented for sociometric status, centrality, emission, and reception.

### Table 4. Information network metrics.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Information network | Nodes | Edges | Density | Diameter | Sociometric status | Degree centrality | Betweenness centrality | Eigenvector centrality |
| Phase 1 | 29 | 158 | .19 | 5 | Username (1.00), title (0.86), price (0.71), categories (0.79), search phrase (0.79), product qualities (0.64) | Username (14), title (12), categories (11), search phrase (11), price (10), product qualities (9) | Username (162.01), title (51.34) | Title (0.36), price (0.32), categories (0.32), search phrase (0.32), username (0.32), product physical qualities (0.28), average rating (0.27) |
| Phase 2 | 35 | 142 | .12 | 5 | Username (1.06), title (0.59), external market reputation (0.47), deposit (0.47), product adverts (0.47) | Username (18), title (10), deposit (8), external market reputation (8), product adverts (8) | Username (293.89), deposit (124.58) | Username (0.51), title (0.32), product adverts (0.28), external market reputation (0.28) |
| Phase 3 | 26 | 168 | .26 | 4 | Order status (1.04), username (0.96), order details (0.96), title (0.80) | Order status (13), username (12), order details (12), title (11) | Order status (54.97), title (45.57), product qualities (31.28), username (29.45), order details (29.00) | Order details (0.33), order status (0.33), username (0.32), dispute message (0.29), dispute conference (0.29) |

*Note*. Only key nodes are presented for sociometric status and centrality.

### Table 5. Hierarchical clustering analysis across the information networks.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information network | Cluster 1 | Cluster 2 | Cluster 3 | Cluster 4 | Cluster 5 |
| Phase 1 | Password, login status, registration status, username, terms and conditions, vendor join date, vendor last active | Escrow option, product image, shipping details, product description, page number, product qualities, price, number of listings, date of listing  | Categories, search phrase, title, vendor reviews, product reviews, deal count, external market reputation, average rating | Withdraw PIN, captcha, market status, JavaScript | - |
| Phase 2 | Commission, confirmation status, tumbler address, pending balance, deposit, valid period, transaction time, bond, encrypted code | Balance, Dream address, vendor status, verified vendor status, external market reputation, username | Terms and conditions, shop URL, finalise early rule, autofinalise option, preferred currency, avatar, deal count, PGP, forum posts, product reviews, average rating, username | Shipping details, product physical qualities, product image, price, product description, title, escrow option, product adverts | Forbidden products and services |
| Phase 3 | Price, username, average rating, deal count, vendor reviews, title | Shipping details, address, order details, order status, tracking number, product qualities, buyer feedback, dispute message, dispute conference, wallet balance, funds in escrow, solution, auto-finalisation status, date,  | Escrow option, product image, product description, packaging, external market reputation | encryption | - |

### Table 6. Task-information composite networks.

|  |  |  |
| --- | --- | --- |
| Phase | Task | Information |
| 1 | Maintain security | Password, PIN, username, escrow option, captcha, JavaScript |
|  | Create account | Password, PIN, registration status, username, captcha |
|  | Navigate to product category | Login status, category |
|  | Search | Search phrase |
|  | Browse listings | Username, page number, image, escrow option, shipping details, title, price, deal count, average rating, number of listings |
|  | Assess market | Market status |
|  | Assess listings | Username, image, product quality, product reviews, escrow option, shipping details, product description, title, price, deal count, external reputation, average rating, number of listings |
|  | Assess vendor reputation | Username, profile, vendor reviews, product reviews, deal count, external reputation, average rating |
| 2 | Maintain security | Username, forum posts, product reviews, shipping details, product description, profile, title |
|  | Identify cryptocurrency address | Balance, valid period, Dream Market address, username |
|  | Tumble cryptocurrency | Commission, tumbler address, confirmation status, pending balance, price, balance, deposit, transaction time, valid period, Dream Market address, bond |
|  | Register as vendor | Balance, bond, vendor status, username |
|  | List product | Shipping details, forbidden products, product qualities, product image, price, product description, title, username, escrow option |
|  | Develop profile | Shop URL, vendor status, profile, verified vendor status, username, external reputation, finalise early rule, autofinalise option, avatar, PGP, deal count, product reviews, preferred currency, average rating |
|  | Engage on forums | Username, avatar, forum posts, product reviews |
|  | Link external reputation | External reputation, PGP, deal count, encrypted code, average rating |
| 3 | Maintain security | Packaging, solution, dispute conference, escrow option, username, product reviews, product image, product description, title, dispute message, buyer feedback, encryption |
|  | Navigate to product page | Username, title, search phrase, categories |
|  | Add order details | Wallet balance, price, order details, username, title, shipping details, address |
|  | Accept order and arrange delivery | Funds in escrow, order status, order details, title, shipping details, address |
|  | Send message | Order status, order details, username, dispute message |
|  | Negotiate solution | Solution, order status, order details, username, dispute message.  |
|  | Discuss on forums | Username, buyer feedback, vendor reviews, product reviews |
|  | Retrieve product | Packaging, product qualities |
|  | Finalise order | Autofinalisation status, order status, order details, username, title, buyer feedback, date |
|  | Create formal dispute | Tracking number, solution, dispute conference, price, escrow option, username |
|  | Process refund | Funds in escrow, wallet balance, dispute conference, price, escrow option, username |

### Table 7. Agent-information composite networks

|  |  |  |
| --- | --- | --- |
| Phase | Agent | Information |
| 1 | Registration form | Password, PIN, username |
|  | Buyer | Password, PIN, registration status, login status, username, profile, category, page number, image, search phrase, vendor reviews, product reviews, escrow option, shipping details, product description, title, price, deal count, external reputation, average rating, captcha, JavaScript, market status, number of listings, date of listing, vendor join date, date of last sale |
|  | Prospective vendor | Password, PIN, registration status, username, profile, captcha, JavaScript, market status |
|  | Product listing | Username, image, product reviews, escrow option, shipping details, product description, title price, deal count, external reputation, average rating |
|  | Search form | Username, search phrase, title |
|  | Navigation panel | Category, number of listings |
|  | Vendor profile | Username, profile, image, vendor reviews, product description, deal count, external reputation, average rating, vendor join date, date of last sale |
|  | Established vendor | Password, PIN, registration status, login status, username, profile, image, product quality, vendor reviews, product reviews, escrow option, shipping details, product description, title, price, deal count, external reputation, average rating, captcha, JavaScript, market status, number of listings, date of listing, vendor join date, date of last sale |
|  | Forum | Product quality, vendor reviews, product reviews, product description, title, price, external reputation, market status |
|  | Other users | Product quality, vendor reviews, product reviews, product description, title, price, external reputation, JavaScript, market status |
|  | Administrator | Registration status, image, vendor reviews, product reviews, shipping details, product description, title, price, external reputation, JavaScript, market status, date of listing, vendor join date, date of last sale |
| 2 | Bank account | Balance, deposit |
|  | Tumbling service | Commission, tumbler address, confirmation status, deposit, transaction time, valid period, Dream Market address |
|  | Cryptocurrency page | Pending balance, balance, deposit, transaction time, valid period, Dream Market address,  |
|  | Forum | Username, avatar, forum posts, product reviews |
|  | Other users | Username, avatar, forum posts |
|  | Buyer | Commission, tumbler address, confirmation status, shipping details, product image, pending balance, price, product description, balance, deposit, transaction time, valid period, Dream Market address, profile, title, username, external reputation, escrow option, autofinalise option, avatar, PGP, deal count, forum posts, product reviews, preferred currency, average rating |
|  | Vendor | Commission, tumbler address, confirmation status, shipping details, forbidden products, product qualities, product image, shop URL, pending balance, price, product description, balance, bond, deposit, transaction time, vendor status, valid period, Dream Market address, profile, title, verified vendor status, username, external reputation, escrow option, finalise early rule, autofinalise option, avatar, PGP, deal count, forum posts, product reviews, encrypted code, preferred currency, average rating |
|  | Vendor registration page | Bond, vendor status |
|  | Dream Market wallet | Balance, deposit, transaction time, Dream Market address |
|  | Product listing | Shipping details, product image, price, product description, title, username, external reputation, escrow option, deal count, product reviews, preferred currency, average rating |
|  | Encrypted message | Encrypted code |
|  | Administrator | Username, avatar, PGP, forum posts |
|  | Profile | Shop URL, vendor status, profile, verified vendor status, username, external reputation, finalise early rule, autofinalise option, avatar, PGP, deal count, forum posts, product reviews, preferred currency, average rating |
| 3 | Dream market wallet | Wallet balance, username |
|  | Product listing | Price, escrow option, username, product reviews, product image, product description, title, average rating, shipping details, external reputation, deal count |
|  | Order page | Wallet balance, price, order status, order details, escrow option, username, title, shipping details, address |
|  | Product | Product qualities  |
|  | Postal service | Packaging, address |
|  | Buyer | Autofinalisation option, funds in escrow, tracking number, packaging, solution, product qualities, wallet balance, dispute conference, price, order status, order details, escrow option, username product reviews, product image, product description, title, average rating, dispute message, shipping details, external reputation, deal count, address, buyer feedback, date, encryption, search phrase, vendor reviews, product adverts, categories |
|  | Vendor | Autofinalisation option, funds in escrow, tracking number, packaging, solution, product qualities, wallet balance, dispute conference, price, order status, order details, escrow option, username product reviews, product image, product description, title, average rating, dispute message, shipping details, external reputation, deal count, address, buyer feedback, date, encryption, vendor reviews, product adverts |
|  | Messaging service | Solution, dispute conference, username, dispute message |
|  | Other users | Username, product reviews, buyer feedback, date, vendor reviews, product adverts |
|  | Forum | Username, product reviews, product description, title, vendor reviews, product adverts |
|  | Escrow | Funds in escrow,  |
|  | Administrator | Funds in escrow,  |
|  | Moderator | Funds in escrow, tracking number, solution, dispute conference, price, order status, order details, escrow option, username, product reviews, product image, product description, title, average rating, dispute message, shipping details, external reputation, deal count, buyer feedback, vendor reviews, product adverts |

### Table 8. Extract from broken-links analysis for EAST social network.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| From (agent) | To (agent) | Information not communicated | Outcome | Intervention strategy | Impact |
| Vendor | Product listing | *Packaging* | Product listing does not describe packaging | Prevent vendor from describing packaging on listing | L |
| Vendor | Product listing | *Product qualities* | Product listing does not accurately describe product qualities | Prevent vendor from describing product qualities on listing | H |
| Vendor | Product listing | *Price* | Product listing does not display price | Prevent vendor from entering price on product listing | H |
| Vendor | Product listing | *Escrow option* | Product listing does not display escrow option | Prevent vendor from selecting whether escrow is available | M |
| Vendor | Product listing | *Product image* | Product listing does not display image | Prevent vendor from uploading product image | L |
| Vendor | Product listing | *Product description* | Product listing does not have description | Prevent vendor from typing product description | H |
| Vendor | Product listing | *Title* | Product listing does not have title | Prevent vendor from entering title for listing | H |
| Vendor | Product listing | *Shipping details* | Product listing does not have shipping details | Prevent vendor from selecting shipping details for listing | H |
| Forum | Buyer | *Username* | User account associated with forums posts not communicated | Prevent username from appearing with user forum posts | L |
| Forum | Buyer | *Product reviews* | Product reviews not communicated | Prevent product reviews from displaying on forum | L |
| Forum | Buyer | *Product description* | Product description not communicated | Prevent product descriptions from displaying on forum | L |
| Forum | Buyer | *Title* | Title not communicated | Prevent product titles from displaying on forum | L |
| Forum | Buyer | *Vendor reviews* | Vendor reviews not communicated | Prevent vendor reviews from displaying on forum | L |
| Forum | Buyer | *Product adverts* | Product adverts not communicated | Prevent product adverts from displaying on forum | L |

*Note*. L = low impact, M = medium impact, H = high impact.

### Table 9. Extract from broken-links analysis for EAST task network.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| From (task) | To (task) | Information not communicated | Outcome | Intervention strategy | Impact |
| Negotiate solution | Create formal dispute | *Order status* | Order status does not inform whether a formal dispute is necessary | Prevent order status from being communicated | L |
| Negotiate solution | Create formal dispute | *Order details* | Order details are not communicated | Prevent order details from being communicated | H |
| Negotiate solution | Create formal dispute | *Username* | Unclear which users are involved | Prevent username from displaying in messaging service | M |
| Negotiate solution | Create formal dispute | *Solution* | Solution unknown; unclear how to proceed | Prevent messages from displaying in messaging service | H |
| Negotiate solution | Create formal dispute | *Dispute message* | Message is not communicated | Prevent messages from displaying in messaging service | H |
| Create formal dispute | Negotiate solution | *Tracking number* | No verification that order was shipped | Prevent users from accessing tracking information | M |
| Create formal dispute | Negotiate solution | *Solution* | No solution communicated | Prevent messages from displaying in messaging service | H |
| Create formal dispute | Negotiate solution | *Dispute message* | Previous messages about dispute not communicated | Prevent messages from displaying in messaging service | M |
| Create formal dispute | Negotiate solution | *Dispute conference* | New messages about dispute not communicated | Prevent messages from displaying in messaging service | H |
| Create formal dispute | Negotiate solution | *Order status* | Status of order not communicated | Prevent order status from being communicated | M |
| Create formal dispute | Negotiate solution | *Order details* | Details of order not communicated | Prevent order details from being communicated | M |
| Create formal dispute | Negotiate solution | *Escrow option* | Whether order involved escrow not communicated | Prevent escrow option from being displayed | M |
| Create formal dispute | Negotiate solution | *Username* | Users involved in dispute and moderation unclear | Prevent username from being displayed with messages | M |
| Create formal dispute | Negotiate solution | *Product reviews* | Reviews of product not communicated | Prevent access to product reviews | M |
| Create formal dispute | Negotiate solution | *Product description* | Cannot check whether product description matches user expectations | Prevent access to product description  | M |
| Create formal dispute | Negotiate solution | *Title* | Unclear which product dispute involves | Prevent title from being displayed | M |
| Create formal dispute | Negotiate solution | *Average rating* | Existing feedback on product cannot inform resolution | Prevent average rating from being displayed | M |
| Create formal dispute | Negotiate solution | *External reputation* | Vendors’ external reputation cannot inform dispute resolution | Prevent external reputation from linking to Dream Market | M |
| Create formal dispute | Negotiate solution | *Deal count* | Existing feedback on product cannot inform resolution | Prevent deal count from being displayed | M |
| Create formal dispute | Negotiate solution | *Vendor reviews* | Vendors’ reputation cannot inform resolution | Prevent access to vendor reviews | M |

*Note*. L = low impact, M = medium impact, H = high impact.

# Figure Captions

Figure 1. Screenshot of Dream Market vendor feedback.

Figure 2. Task networks for each phase, with key nodes by sociometric status bolded, by centrality shaded, and both sociometric status and centrality bolded and shaded.

Figure 3. Social networks for each phase, with key nodes by sociometric status bolded, by centrality shaded, and both sociometric status and centrality bolded and shaded.

Figure 4. Information networks for each phase, with key nodes by sociometric status bolded and both sociometric status and centrality bolded and shaded.