It's Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums

David Lacey(✉) and Paul M. Salmon

Centre for Human Factors and Sociotechnical Systems,
University of the Sunshine Coast, Sippy Downs, Australia
dlacey@usc.edu.au

Abstract. The dark web is a layer of the Internet that exists to preserve the anonymity of its users. Features of the dark web include websites, discussion forums, and marketplaces that trade in legitimate and illicit products and services. Common examples that have gained public notoriety include Silk Road, Agora and Taobao5, generating hundreds of thousands of users worldwide. One of the major features of the dark web is obscuring the originating Internet Protocol (IP) address of its users. Perhaps this may explain why little research exists on participant trust and engagement within this environment. This research paper contributes to this gap in two ways. First it explores the application of the Event Analysis of Systemic Teamwork (EAST) methodology to the dark web context, and specifically, the tasks and interactions associated with enrolling as a first-time participant within an illicit marketplace. The second contribution, is a compelling view on the nature of trust establishment within a dark web system of relevance to participants, hosts, and law enforcement stakeholders alike. The research is novel in its approach and application of sociotechnical systems methodologies within a highly under-researched but popular environment. The implications for future research and practice in this area are discussed.

1 Introduction

The Internet comprises multiple layers of data repositories, and with it, multiple forms of accessibility. Most Internet users only ever engage in what is known as the *surface-layer web* and *deep web*. The surface layer is accessible via common search engines, such as Google and Yahoo. A secondary and much richer layer of the Internet is referred to as the *deep web*. The deep web is accessible via the public Internet, but is typically not obtainable through popular search engines. Search engines crawl the Internet looking for search bots that index data, mostly using robots.txt files as guides that tell them what data to index under the Robot Exclusion Standard (Koster 2014). Such web crawlers cannot index deep web content, and thus leaves this material unattainable to most common forms of search engines. This is not to say that the content cannot ever be retrieved. Accessing the deep web is a common occurrence for users that direct their searching through the data repository in question. For example, users that seek to find the residential address of a person may not achieve this result

D. Harris (Ed.): EPCE 2015, LNAI 9174, pp. 117–128, 2015.
DOI: 10.1007/978-3-319-20373-7_12

from a common search engine. However, should they enter the same search criteria within a specific residential address database they may well get a different result – one that extracts the answer from the deep web, not the surface-layer web.

The third layer of the Internet, the focus of this research, is the *dark web*. The dark web whilst still accessible publicly has several distinct features when compared with the surface-layer and deep web. Content within the dark web requires manual searching. Users typically access via dark web mechanisms that create anonymizing pathways to access the dark web content, such as The Onion Router (Tor). The anonymization pathways are typically available via open source software options. The sender of information will find an entry point and choose random routing pathways through which to obfuscate their point of origin. The traffic along this pathway is encrypted and the point of leaving the routing pathways reveals that specific IP address, which is not the originating participant's actual IP address (Bradbury 2014). Dark web sites, forums, and marketplaces are popular environments for many individuals, including those in countries that have Internet content restrictions, face the risk of persecution for their religious or ideological beliefs, or seek to communicate anonymously content relating to terrorist plots, child pornography, and of specific interest to this paper, the buying and selling of stolen personal information and credentials (O'Brien 2014; and Chen et al. 2008).

Despite the reported growth of dark web content and popularity, little research exists that explores the operations of this complex system and the related trust and engagement dynamics between its users (Bradbury 2014). Much of the usage of the dark web involves interactions between users and technologies. This feature suggests that systems analysis methods from the discipline of human factors are suited to understanding dark web operations, primarily since they examine interactions and emergent behaviors. The following section explores the nature of existing research on the dark web and examines the utility of using a systems analysis method, the Event Analysis of Systemic Teamwork (Stanton et al. 2013), for examining dark web operations. An overview of the applicability of EAST as a method to explore the task environment in question is provided, followed by its methodical testing from the content and observations made from a dark web marketplace case study. The case study is supported by interviews with Subject Matter Experts (SMEs) within law enforcement that specialize in cyber-crime investigations and expert cyber-security counselors within a national identity theft support service. The paper concludes with a section on the results and implications of the research and opportunities identified to extend the use of human factors methods within the cybercrime environment.

2 Dark Web and Trust Literature

Research on the dark web has been limited and sporadic at best. This may be a factor of the only recent growing notoriety of the dark web through forums such as Silk Road, established in 2011. There is little denying its exponential popularity. Since the mastermind of Silk Road, one of the dark web's most successful marketplaces, was arrested on 2 October 2013, the marketplaces, participants, volume of trade, and diversity of products and services on offer via the dark web continues to grow. O'Neill (2014) and

other popular online commentators reveal that since the arrest of Ross Ulbricht, aka the 'Dread Pirate Roberts', by the Federal Bureau of Investigation (FBI), black markets have not only grown in size — "they're flourishing". O'Neill (2014) claims that there are now at least 16 major black markets that have risen in Silk Road's wake currently offering over 60,000 products — a cumulative total nearly three times the amount offered at the time of Ulbricht's arrest in late 2013.

Supporting the growth of the dark web, and presumably the trust gained by participants to engage, are open source software anonymizing tools, such as Tor. It's arguable that Tor, like other dark web anonymizing tools, acts as a third party trust-builder for participants (or users) of forums, websites and marketplaces. In fact it is a mandatory feature of a number of dark web forums that participants use Tor and agree to transact only through the use of anonymous virtual currencies, such as Bitcoin (Bradbury 2014).

One of the earliest studies on the antecedent of the dark web, the *darknet*, investigated the relevance of content protection and distribution architectures given the inevitability of its expansion (Biddle et al. 2002). This research paved the way for future efforts in exploring how enforcement agencies and regulators could detect and respond to the darknet, or as its referred to now, dark web content. (Chen et al.'s 2008) work presents a multi-method approach for collecting web content through the use of *spidering* or *crawler* techniques that harvest web-page content relevant to a specific seed URL. Their data collection methodology was tested as a means to examine its validity in the dark web, specifically relating to *Jihad* content suspected of being terrorist affiliated (Chen et al. 2008). Whilst of value in revealing the location of dark web content, (Chen et al.'s 2008) research fell short of understanding the specific tasks involved in hosting and participating in such forums that could prove useful in detecting future methods of participant concealment. Highlighting these challenges, and fueling the calls for some form of dark web regulation was O'Brien's (2014) paper that calls for alternative regulatory methods be developed to counter the criminal aspects of its content and participation. Whilst O'Brien's (2014) work highlights the growing challenge for law enforcement and national security agencies in responding to advancements in anonymization, such as the merging of Tor with cloud-based peer-to-peer (P2P) file sharing techniques, it too falls short in providing any in-depth analysis of the task, social and knowledge networks in operation. The absence of a socio-technical systems approach to understanding the dark web has meant a limited ability to decompose tasks and interactions, evaluate networks, and understand its interdependencies and emergent behaviours. To put it simply, the dark web research to date has largely identified the challenges posed by the environment, rather than its specifications, and ultimately, intervention opportunities.

The multiple network perspectives at play within the dark web offer a unique slant on the volume of research published in relation to online trust and engagement. Unlike the major focus on surface-layer and deep web marketplace trust and engagement being on participant or online user trust creation, the dark web emphasis originates largely from the opposite direction. In other words, eCommerce in the dark web is not solely about engendering trust from the perspective of the user having to be convinced about the legitimacy of the market they wish to interact with, rather the administrator or manager of the dark web and the existing participants must be convinced of the

legitimacy of the user. This is not to say that trust creation and engagement is not important for prospective users, it clearly is. However, the process of deciding to participate and enrolling or applying to join such dark web forums appears to place a critical reliance upon the prospective user to demonstrate their legitimacy. As will become apparent with the case study chosen, trust building activities are a mandatory requirement for prospective users to complete prior to gaining acceptance and membership of the dark web marketplace in focus.

The concept of trust within the human factors domain have focused largely on the trust to be gained by the user resulting from specific website content, attributes, ease of use, and related consumer centric acceptance models (Corritore et al. 2003). Trust is an enabler of online engagement. To engage online, certain levels of trust in what is being offered or accessed is required. The host of dark web marketplaces offer participants an anonymized service to connect buyers and sellers. The users of such marketplaces must trust that such environments will maintain their anonymity and will also follow through with the service communicated, such as provision of information on stolen credit cards following the payment for such commodities – as would be the case in surface layer and deep web marketplaces. Ironically the uniqueness of the trust environment for dark web participants and hosts appears to distil to the singular issue of preserving anonymity. If this were true, then the highest risk presented to the dark web marketplace host and existing participants resides at the point at which a new participant or user seeks to engage in such forums for the first time. By the very nature of these environments, new users are unknown, untested, and untrustworthy. Such participants or users have no established track record of behavior that would engender trust. The formation of trust, and the ultimate acceptance of the new user within the community, is often constructed via prospective users demonstrating their legitimacy through action. Mayer et al. (1995) based their observations on trust as relating to ability, integrity and benevolence. Within the dark web context, ability can relate to the extent to which a new user can contribute to the needs of the dark web community, such as provide new sources of compromised credit card information (Lampaduza.so; 2015). Integrity as a bases for trust in the dark web can encapsulate the overall integrity of the marketplace in maintaining anonymity of its users and hosts, which also connects with Mayer's et al. (1995) benevolence observation – anonymity as a binding mutual interest for participants.

Trust is dynamic. It can build, diminish, and be removed at any point. Within a dark web marketplace environment, the initial point at which a new user is accepted within such a community offers critical insights into how the underlying collaborative networks form, communicate, socialize, share knowledge, and ultimately perform. Online participant trust and engagement has dominated information systems research for over twenty years. The vast majority of this research considers what environmental and system factors influence the decision of participants to engage online, typically within eCommerce contexts (Pavlou and Gefen 2004). How the underlying collaborative networks within a dark web marketplace originate through the attainment of trust is not understood, and provides an excellent opportunity to examine the relevance of adopting EAST in gaining a view from multiple network perspectives (Salmon et al. 2011). The following section examines the applicability of EAST in understanding the formation of trust within a specific dark web marketplace.

3 EAST and the Selected Dark Web Forum

Many characteristics surrounding human behavior within the dark web remain ambiguous and largely unexplored. For example, how users assess and perceive risk whilst operating within the dark web remains unclear. Moreover, the ways in which trust is developed between users have not been explored. In particular, the interactions and information underpinning trust have not been examined. The aim of this proof of concept study was to use EAST in order to understand how individual participants in such forums perceive risk, and ultimately develop trustworthiness to a point where engagement of new users within such forums is accepted by hosts and existing participants.

EAST provides an integrated suite of methods for analyzing performance and behavior in human-technical systems. Underpinning the framework is the notion that system performance can be meaningfully described via a 'network of networks' approach in which three network-based representations are used to describe and analyze behavior: task networks, social networks, and information networks. Task networks are used to describe the goals and subsequent tasks being performed within a system (i.e. which agents, both human and non-human, do what). Social networks are used to analyze the organization of the system and the communications taking place between agents (i.e. who/what interacts and communicates with who/what). Information networks show how information and knowledge is distributed across different agents within the system (i.e. who/what knows what at different points in time). It is these authors' opinion that this tripartite perspective on behavior will provide a rich explanation of dark web operations.

With the conceptual method in place, the research team enlisted the assistance of a national identity theft support center and a State law enforcement agency. These research partners supported the researchers in their access of the target dark web marketplace that buys and sells stolen personal information and credentials, such as compromised credit card information. Tor was used on an unattributable computer to gain access to the target marketplace, known as *The Republic of Lampeduza* (ROL). ROL at the time of writing this paper was an active "carding forum" that specializes in the buying and selling of credit card "dumps". Carding forums act as a virtual marketplace that specialize in the trading in large volumes of compromised credit card details for further criminal use. Such forums are a good source of information about task, social and situation awareness or knowledge networks. At the time of accessing ROL, the marketplace had over 4,000 trusted members and over 71,000 total posts, most of which appeared to offer specific products or services, such as assistance with undertaking data harvesting (or hacking), through to the provisioning of various credit card "dumps" – or significant quantities of compromised credit card information.

Influencing the selection of ROL as an appropriate research site was the information provided by the marketplace host on the "rules" or "enactment" that concerned the initial user application process. The ROL marketplace at the time was chosen given the contemporary nature of its operations and the information available on the site that enabled the ability to test the EAST method (see Fig. 1).

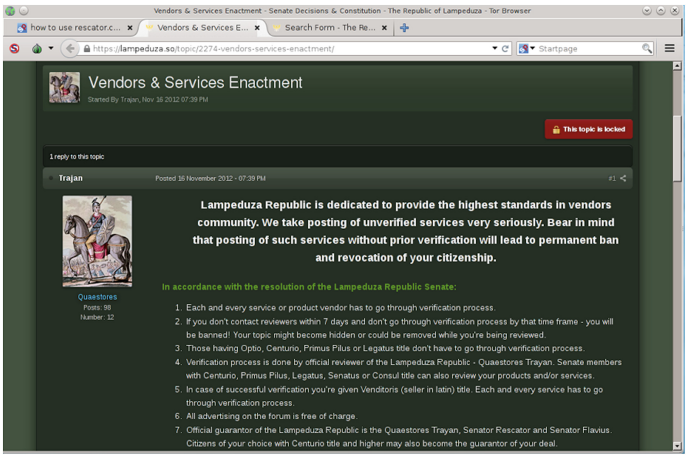

Fig. 1. Extract from The Republic of Lampeduza carder forum "Vendors & Services Enactment"

4 Application and Testing of EAST

As with most human factors methods, the initial point of the research undertaken was to define the analysis aim, the overall reason for applying EAST in this context (Stanton et al. 2013). As discussed, limited research has been published on the dark web. What exists at the time of undertaking this research appears limited to describing methods of collecting information from dark web sites and describing the regulatory challenges in keeping abreast of the evolving anonymizing technologies (O'Brien 2014; Chen et al. 2008). The primary aim of the analysis is to understand and represent the requirements for establishing trust within a dark web carder marketplace. To achieve this aim, the research team required access to a dark web marketplace, an understanding of the enrolment process, the recording of information needed to comply with the rules of enrolment, and participant discussions about the process of enrolling in such forums.

The first step was followed by the undertaking of a Hierarchical Task Analysis (HTA). The underlying principle of this step was to break down the enrolment process into individual sub goals of the task itself, thereby representing the system goals and plans. In constructing the HTA for the ROL enrolment process, the researchers systematically observed and recorded each step of the process involved in registering and, ultimately, enrolling as a registered and trusted user of the marketplace. The HTA revealed a unique orientation of trust enabling activities that is the onus of trust building being placed mostly on the new applicant user, and not the host or existing participants within the site itself. The HTA is presented in Table 1.

Within the HTA, *Task 3 – Compliance with Minimum Reviewer Requirements* was then split into a number of specific sub-tasks. The ROL marketplace defines eleven participant types (excluding the ROL reviewer and administrator). Each participant assumes a specific role within the system. There is no one generic member type. Each participant role demonstrates initial and on-going trust through action. Like surface

Table 1. Hierarchical task analysis – task definition

ROL User Initial Enrolment
0. Provide Human-Computer Validation (Plan 0. Do 1 then 2 then 3 then EXIT)
1. [All Users] Complete Human Interface Validation (Plan 1. Do 1.1, then 1.2, then EXIT)
1.1 Enter 'Captcha' Phrase
1.2 Enter Randomized Alphanumeric Code
2. [All Users] Membership Status (Plan 2. Do 2.1 if Current Member, all else 2.2, then 2.3, then 2.4 then EXIT
2.1 [Existing User] Enter Member Email and Password
2.2 [New User] Enter Tor Email Address
2.3 [New User] Confirm Tor Email Address
2.4 [New User] Enter New Password & Confirm New Password
3. [New Users] Compliance with Minimum Reviewer Requirements (Plan 3. Do 3.1, then 3.2 then EXIT
3.1 Transfer financial amount to ROL transaction payment system (role specific)
3.2 Respond to specific reviewer task requirement according to nominated role

layer web marketplaces, ROL also presents scorecards on the marketplace's rating of each user. Rating measurements in ROL are specific to the participant role, and are geared towards encouraging or dissuading participant interaction. The primary participant roles within ROL are described in the following table with the minimum entry requirements to establish trust (Table 2).

A distinguishing feature of the trust building task analysis for ROL is the prospective orientation of how new users engage. A new user applicant is allocated an anonymous reviewer from ROL. The reviewer determines the precise nature of the trust building requirements, for example, the type of credit card dump to provide.

Table 2. Specific ROL roles and minimum trust building requirements

User role name	Role description	Trust requirement
Dump seller	Provider of large files containing information for verification and sale	25,000 USD (incl VAT) pa and 500 valid dumps as defined by the reviewer
Card seller	Provides credit and debit card information for verification and sale	5,000 USD (incl VAT) pa and 500 valid cards as defined by the reviewer for examination
Information services seller	Provides specialized information services, including personal information files, credit reports, and related information	Three demonstrations of the extraction of specific information types for review
Virtual private server hosting	Provides anonymized server for ROL marketplace participants	Provision of a server to ROL for the entire period they are a participant
Spam services vendor	Generates email spams to directed and non-directed target groups	3,000 USD (incl VAT) pa and a test spam of 100,000 emails as defined by the reviewer
DDos services vendor	Distributed denial of service attack vendor to enable the flooding of the target source with external communications	Target a defined site for a certain period of time at the request of the reviewer
eBay & PayPal vendor	Provides legitimate accounts on eBay and PayPal for laundering and fraudulent services usage	Vendor must provide 20 accounts at the specific request of the reviewer
Bank account vendor	Provides legitimate bank accounts for laundering and fraudulent usage	Vendor must provide three accounts with all login information
Sellers of cards for withdrawal	Provides pre-paid money cards, such as travel cards	Provide two examples of each type of card offered and pay 5,000 USD pa
Software developer sellers	Provides development services that enable data harvesting and/or protection	Vendors must provide the ROL reviewer with a fully functional sample of their products (with full support)
Sellers of technological products	Providers of solutions to enable marketplace participants to fulfill their specific role	Vendor must submit samples of each type of product to the ROL reviewer for testing

Instructions can be quite explicit, such as specific card issuer (for example, Visa, Mastercard, AMEX etc.), the issuing financial institution (i.e. the specific bank issuing the credit/debit card), and the card limit (for example, Platinum or Gold cards).

The remaining focus of testing the application of EAST to more completely understand the enrolment process for new users of dark web marketplaces involved developing a social and information network for the tasks experienced by new users, and by way of example, card selling vendors. These types of prospective vendors are

required by the ROL host to provide 5,000 USD (incl. VAT) for one year and 500 valid cards as defined by the reviewer for examination. The social network diagram is presented at Fig. 2 for the enrolment of card selling vendors in relation to meeting the payment trust building requirement.

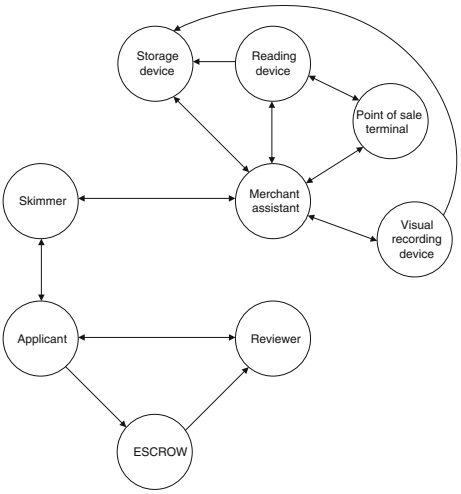

Fig. 2. Social network showing human and non-human agents involved in responding to trust building requirements for card selling vendor new applicants (users)

The social network incorporates both human (e.g. applicant, reviewer) and non-human actors (e.g. reading device, Escrow). As shown in Fig. 2, the mere payment of the 5,000 USD requires at least two other agents within the established bilateral relationship – the "skimmer" and the "merchant assistant". The payment system of choice for ROL is an Escrow system. Like popular marketplaces found in the surface layer and deep web, the Escrow system for ROL provides a level of assurance between two transacting parties that a payment has been made. Once notification that the payment has been made to this service, communication is made to the seller to release the product or service in question to the buyer. A clear distinction is made between the normal operation of Escrow, and the trust building payment process for ROL. The payee or prospective vendor/user has no way of validating that money has been received by the Escrow account, nor that membership will be granted. This perhaps challenges the use of the term Escrow for those involved in the initial application payment.

The second aspect of the trust building activity for card selling vendor applicants involves the acquisition of 500 cards as specified by the reviewer. This is a much more complex network where other agents outside of the bilateral relationship are introduced. The depth and breadth of external agent participation is a factor of how independent and capable the applicant is in their acquisition of card information. It is no good going into ROL as a card vendor applicant with 500 cards already to share with

the receiver. The receiver dictates the type of card, the issuing bank, and the credit limit–thus requiring the applicant vendor to respond to this new requirement. A number of information systems and criminology research papers shed light on the networks required to acquire credit card data fraudulently. The most common method of acquiring credit card data is credit card skimming (Barker et al. 2008). Credit card skimming typically occurs at a merchant point of sale (POS). The skimming device that reads each card that is used during the POS transaction may either be a circuit board located within the re-configured POS terminal or a hand-held wireless unit (Quah and Sriganesh 2008). The agents within the card skimming network may include corrupted employees and technicians capable of extracting the data from the skimming data storage file (ACFE 2007). Such a social network is representative of a "Y" configuration with the point of centrality shifting to the applicant vendor from the reviewer, when compared with the payment trust building task. Both networks, most likely for security purposes, are low density in its distribution.

The final component of the EAST analysis involved developing a high level information network which captures the information passed around during the card selling scenario (see Fig. 3). This provides a description of the different pieces of information used by different actors throughout the process. As shown in Fig. 4, the network is highly connected, with various interdependencies and relationships between pieces of information. The utilization of the observations from within ROL, coupled with invaluable SME guidance from law enforcement, enabled the research team to consider various interactions and information dependencies previously unseen.

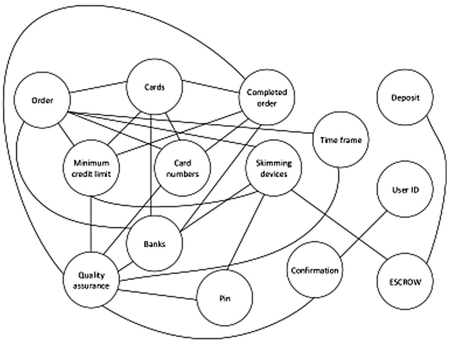

Fig. 3. ROL information network – card selling vendor new user trust building requirements.

The information network provides unique insights into the operation of a dark web marketplace. For prospective card selling vendors, the most connected and therefore critical piece of information is the *Quality Assurance* node. Underpinning the success of the trust building activities is the ability for the reviewer to validate the legitimacy of the 500 cards acquired for the purposes of enrolling. Cards must be active, have sufficient credit limits, and issued by the very bank and card type as specified by the reviewer in order for the trust to be built. The high connectedness of this node suggests that interventions designed to disrupt trust building should be aimed at discrediting the

quality of sale items. Access to a skimming device as a technology component is equally critical. Both these nodes within the network itself provide law enforcement and related agencies opportunities to detect potential dark web marketplace enrolment activity. In other words, the application of EAST as a method for preventing accidents (Salmon et al. 2011) can more readily be applied to a cybercrime environment as a method for detecting future compromise sites, or at the very least indicators of such compromises.

5 Conclusions

This proof of concept study was undertaken to test the utility of applying EAST to understand dark web operation. A strong onus within the dark web environment is on the searcher to know what they are looking for and to demonstrate their participatory credentials in order to access content. The orientation of trust in the dark web context is not as one may assume exists with the surface-layer web. Surface-layer web has occupied a substantial body of research, particularly the online transaction environment. Online trust and engagement across information system, human factors and sociotechnical systems research is not new. However, the orientation of trust has often been focused on the trust to be gained by those seeking to engage, put simply, the prospective applicant. The EAST method has assisted this research in examining a different and unique trust perspective – that of prospective applicant having to demonstrate to the e dark web marketplace provider (in this case, the reviewer) that they are to be trusted. A key feature of EAST is the ability to analyze systems from multiple actors perspectives, showing how different actors behave, interaction and think.

The EAST method assisted the research team to systematically explore the dark web marketplace enrolment process; however, some noteworthy challenges were faced during the analysis. First and foremost was the very nature of the dark web and the variability in potential responses and methods used in meeting the trust building requirements. The ROL marketplace had pre-defined categories of vendors. The trust building task for each vendor differed, as could the actual method in meeting the task requirements.

Despite the challenges, there are some obvious benefits for using the EAST method in exploring and better understanding the dark web. Firstly, EAST is a comprehensive method that provides researchers of the dark web an opportunity to view a system from multiple perspectives (Salmon et al. 2011). The dark web should not purely be viewed as an environment that enables criminal activity, rather an environment where technology and human interaction facilitate the flow of information, goods and services anonymously. Secondly, the limitations of the task analyzed in this paper should not dissuade researchers from applying EAST to a broader dark web market system. The task under analysis for this research paper was a specific area of interest in exploring the enrolling trust dynamic. It also proved to be its major limitation in adopting the EAST method. A much broader view of participant interactions within the dark web, subject of course to an appropriate level of data collection, would likely result in a much more complete application of EAST, and with it, a much greater realization of the benefits in doing so.

Notably, the EAST analysis presented did not incorporate the full analysis approaches utilized in other EAST assessments (e.g. Stanton et al. 2013). Future work will involve using network analysis metrics to identify the key actors and information involved in dark web operations, and also the integration of task, social and integration networks will enable the relationships between tasks, interactions, and information to be unearthed. These rich explanatory analyses will support the development of targeted interventions designed to limit illicit dark web operations. Unfortunately most of what we hear about the dark web relates to its criminalization. The real benefits in exploring the dark web from a human factors perspective remain some way off from being realized. This paper is a first attempt at introducing the human domain to an increasingly popular context for participants, hosts and law enforcement agencies alike.

References

ACFE: The 2007 Fraud Examiners Manual. Association of Certified Fraud Examiners, Austin (2007)

Barker, K.J., D'Amato, J., Sheridon, P.: Credit card fraud: awareness and prevention. J. Financ. Crime **15**(4), 398–410 (2008)

Bradbury, D.: Unveiling the dark web. Netw. Secur. **2014**(4), 14–17 (2014)

Chen, Hsinchun, Chung, Wingyan, Qin, Jialun, Reid, Edna, Sageman, Marc, Weimann, Gabriel: Uncovering the dark web: a case study of jihad on the web. JASIST **59**(8), 1347–1359 (2008)

Corritore, C., Kracher, B., Wiedenbeck, S.: Online trust: concepts, evolving themes, a model. Int. J. Hum Comput Stud. **58**, 737–758 (2003)

Koster, M.: A standard for robot exclusion. Robotstxt.org (2014). http://www.robotstxt.org/orig.html. Accessed 28 February 2015

Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Acad. Manag. Rev. **20**, 709–734 (1995)

O'Neill, P.H.: The unstoppable rise of the Deep Web. The Kernel, 28 September 2014. http://kernelmag.dailydot.com/issue-sections/headline-story/10397/deep-web-size-infographic/. Accessed 28 February 2015

Pavlou, P.A., Gefen, D.: Building effective marketplaces with institution-based trust. Inf. Syst. Res. **15**(1), 37–59 (2004)

Quah, J.T.S., Sriganesh, M.: Real-time credit card fraud detection using computational intelligence. Expert Syst. Appl. **35**(4), 1721–1732 (2008)

Salmon, P., Stanton, N., Lenne, M., Jenkins, D., Rafferty, L., Walker, G.: Human Factors Methods and Accident Analysis: Practical Guidance and Case Study Applications. Ashgate, England (2011)

Stanton, N.A., Salmon, P.M., Rafferty, L., Walker, G.H., Jenkins, D.P.: Human Factors Methods: A Practical Guide For Engineering And Design, 2nd edn. Ashgate, Aldershot, UK (2013)