Winter 12-13-2018

An investigation on the generative mechanisms of Dark Net markets

Paolo Spagnoletti
LUISS University

Federica Ceci
G. d'Annunzio University

Bendik Bygstad
University of Oslo

An investigation on the generative mechanisms of Dark Net markets

Paolo Spagnoletti[1]
Department of Business and Management, LUISS University,
Roma, Italy

Federica Ceci
Department of Economics and Management, G. d'Annunzio University,
Pescara, Italy

Bendik Bygstad
Department of Informatics, University of Oslo,
Oslo, Norway

ABSTRACT

In this paper we investigate the Dark Net which is the part of Internet accessible only via special browsers such as Tor. The Dark Net is the home of black-markets for illegal goods and services such as drugs, weapons and fake identities. In this study we investigate the Dark Net as a digital infrastructure over time to address the following research question: what are the forces underlying Dark Net markets? Our empirical approach is based on a set of techniques for accessing Dark Net marketplaces (DNM) and collecting various types of information on sites, transactions and users. We draw also on secondary sources such as reports of police interventions and interviews. Our analysis follows the tradition of critical realism to shed light on the generative mechanisms enabling Dark Net markets to operate and survive.

[1] Corresponding author. pspagnoletti@luiss.it +39 0685225795

Keywords: Dark Net marketplace, black-market, generative mechanism, critical realism, cyber threat intelligence

INTRODUCTION

The illegal black markets that exist in the Dark Net can be considered the evil Mr. Hydes of the Internet, the ugly market of illegal drugs, guns, child porn and stolen documents. It is the place where the innovative power of technology is used for illegal and unethical purposes, and certainly is a place that most of us would not want to visit. It is a place that most of us prefer to ignore. In this paper, we argue that this disregard is unfortunate for two reasons. First, the Dark Net is a fact of the digital world, and increasing one. As Bartlett (2014) describes, the Dark Net is a strange mixture of crime and idealism, including both dissident sites, drug markets, terrorism and many things between, and should be researched as a global phenomenon.

Second, the criminal part of the Dark Net, fueled by cryptocurrencies such as Bitcoin, is a real and serious threat (Europol 2017), and we need knowledge about it in order to mitigate the risks generated by its users (Kethineni et al. 2017; Samtani et al. 2017). Recent studies show how the Dark Net is contributing to the rise of new forms of crime by providing platforms supporting criminal interactions (Spagnoletti et al. 2018). Dark Net Marketplaces (DNMs) are facilitating illicit trade in hacking services (e.g. renting a Botnet or a Thingbot), fake identity documents and stolen information (Odabas et al. 2017) useful to conduct online fraud through spear phishing and advanced persistent threats (Chaudhry 2017; Hurlburt 2017; Kraemer-Mbula et al. 2013; Samani 2016).

DNMs - described also as cryptomarkets or black-markets - are e-commerce platforms supporting interactions between the buyers and sellers of illegal goods. Therefore, DNMs combine Dark Net capabilities for anonymous surfing with traditional e-commerce functions. Moreover, to conceal payments and money laundering cryptocurrencies are often used in DNMs. Specialized law enforcement agencies (LEA) units survey and occasionally raid these web sites, an example being when the US Federal Bureau of Investigation (FBI) closed the Silk Road site in 2013 (Soska and Christin 2015). Despite growing international cooperation among private and public institutions, attribution is hard for LEAs given the anonymity of interactions. DNMs enable new forms of crime that take advantage of digital capabilities, anonymity and online collaboration and are difficult to fight by focusing only on observable events. The situation calls for an interdisciplinary and multi-level reconceptualization of Dark Net infrastructures. This effort should be accompanied by critical analysis and the exploratory power of social science to stimulate sense-making processes and make decision-making more effective.

We conceptualize Dark Nets as digital infrastructures where anonymity is a necessary condition for the active engagement of participants in online interactions. In digital infrastructures heterogeneous and autonomous human or organizational actors use information technology to allow adaptation to each other and their external environments (Hanseth and Lyytinen 2010; Henfridsson and Bygstad 2013). However, the anonymity of the technological and human components in Dark Nets can make this adaptation processes problematic and have a negative impact on infrastructure functioning. Our research questions are: how are digital

infrastructures generated under conditions of anonymity? What are the underlying mechanisms that explain the functioning of the Dark Net infrastructure?

In this study, we approach the Dark Net from both an empirical and a theoretical view. Empirically, we triangulate archival data from secondary sources with primary data obtained from interviews with LEA agents. We access the Dark Net using specially designed software that allows collection of substantial amounts of information on sites, anonymous actors, communications and transactions. Theoretically, we conduct an in-depth critical realist analysis which reveals the underlying forces shaping the evolution of the Dark Net infrastructure. We identify three generative mechanisms, i.e. Cybercrime scaling, Black platformization, Dark Net resilience.

These causal structures explain how cybercrime is fueled by illegal trading, hacking and collective recovery within regular market operations and breakdowns. Compared to other empirical contexts, breakdown events are more frequent in the Dark Net, and therefore are easier to observe. This allows a deeper understanding of the innovation dynamics occurring within digital infrastructures. Moreover, we shed light on the governance of global information infrastructures, identifying how interactions among multiple actors with different roles (hackers, criminal communities, LEAs agents, buyers and vendors) shape the functionalities and characteristics of the Dark Net infrastructure.

THEORETICAL LENS: DARK NET AS DIGITAL INFRASTRUCTURE

The term digital infrastructure[2] encompasses a socio-technical interconnected structure of systems, people and organizations. Examples include Internet, financial systems, Facebook and airline booking systems. The extant literature on digital infrastructures studies the phenomenon in several contexts such as Internet development (Hanseth and Lyytinen 2010), scientific infrastructures (Edwards et al. 2013), the evolution of mobile platforms (Eaton et al. 2015) and commercial developments.

Digital infrastructures can be considered as an organizational phenomenon; they include both technical solutions and also the organizations and people that leverage the services. They also include the development and knowledge communities that produce the solutions and the support functions. Many infrastructures include several million people, organized in digital ecosystems. The literature highlights some key attributes: (i) digital infrastructures are different from traditional information systems; they are heterogeneous, often with no dominant actor (Hanseth and Lyytinen 2010); (ii) the dynamics of digital infrastructures are different; they are not designed but evolve through innovation, adoption and scaling (Henfridsson and Bygstad 2013). Therefore, digital infrastructures are comprised of computing and network resources which allow multiple stakeholders to orchestrate their service and content needs by exploiting the externalities of digital platforms (Constantinides et al. 2018).

[2] Also called information infrastructures or cyberinfrastructures

In this paper we adopt a broad definition of Dark Net, intended as the portion of the Internet providing digital capabilities to clandestine groups that design, implement and maintain its functionality. There are few studies of the Dark Net that adopt this perspective but there is a line of organizational research on terrorist and drug organizations. For instance, Milward and Raab (2006) found that resilient dark networks manage to rebalance differentiation and integration mechanisms in their internal structure and adjust to the new requirements. Therefore, they are difficult to break. What is less well known is how the interplay among the digital and social elements produces the observed outcomes. It is reasonable to expect that some mechanisms operating in traditional and legal digital infrastructures will work also in the Dark Net. However, it is expected also that due to its particular technical and social structures, other and quite different mechanisms will exist. Our methodological approach is designed to reveal these.

METHOD: DATA COLLECTION AND DATA ANALYSIS

We take a critical realist case study approach (Bhaskar 1998; Mingers 2004; Wynn and Williams 2012) which requires comprehensive data collection, and in-depth data analysis, deploying retroduction to uncover causal mechanisms. We are looking not for regularities at the level of events but deeper level contingent (and generalizable) mechanisms operating on social and technical structures.

The empirical context of our study is the ecosystem of the DNMs. We collected data from multiple sources: the characteristics of anonymity and secrecy of the markets and users analyzed make use of data triangulation and mixed methods especially important since no single

source can provide a complete picture of the phenomenon (Ferguson 2017). We collected data referring to the period 2009 to 2018, covering 10 years. The aim of our data collection was to obtain a full understanding of events, products, actors, processes and technologies occurring in a specific class of fraudulent practice: illegal trade in credit card information.

Data were collected by a combination of crawling the Dark Net and analyzing open sources on the surface web. Table 1 presents an overview of our data collection strategies.

We conducted a critical realist analysis aimed at uncovering the deeper causal structure explaining the empirical observations (Bhaskar 1998; Sayer 1994). We used the technique called retroduction (Wynn and Williams 2012). We built on the method described in Bygstad and Munkvold (2011) (Table 2 presents the process). We started by identifying key events. We define events as clusters of observations. Some events such as the establishment of Dark Net sites (Silk Road, BMR, Agora) and police interventions were obtained from secondary sources, others emerged from the data. These included sites' offerings and the interactions among actors. Next we identified key components (assumed structural objects) of the case such as the Dark Net actors, the technologies and the users, and also the law enforcement actors.

To assess the material collected, we conducted a theoretical re-description of our research object conceptualizing it as a digital infrastructure. This allowed a deeper analysis in the next step of retroduction in which retroduction of candidate mechanisms is crucial. Following Hedström and Swedberg (1996), we looked for three types of mechanisms: how structure influences action (macro-to-micro), how action triggers action (micro-to-micro), and how action reproduces or changes structure (micro-to-macro).

Table 1. Overview of data collection strategies

Category	*Aim*	*Data source*	*Data collection method*	*Data collected*
Events	Evolution of the Dark Net	Open web: Way back machine, Deepdotweb.com, Darkwebnews.com	Identifying and counting activities per month	Evolution of 122 marketplaces in the deep web.
Products	Description of the illegal trade of financial documents and fake IDs	Six Tor marketplaces: AlphaBay, Dream Market, Hansa, Leo, Outlaw and Bloomfield	Crawling the web site and extracting information by the use of the Scrapy tool	A dataset of 36 GB: AlphaBay (9120 offers), Dream Market (18506 offers), Hansa (13068)
Actors	Vendors, Buyers, Administrators and LEAs	a) Deep web: Five Tor marketplaces: Alphabay, Dream, Hansa, Outlaw, Valhalla b) Police reports c) Interviews with LEA operators	Crawling the web site and extracting information by the use of the Scrapy tool Gathering of information on police operations	A dataset of PGP keys of vendors and buyers Process and operations by LEA
Processes	Understanding of security measures	a) Deep web: DNMs b) Open web: Deepdotweb.com and Darkwebnews.com	Identification of relevant technologies and security mechanism	Evolution of security functions implemented in DNM platforms

FINDINGS

In this short paper, we provide an overview of the evolution of DNMs in the past five years and discuss the mechanisms that explain the complex interactions among law enforcement, buyers and vendors of illegal goods and DNM platforms. We conduct an in depth analysis of the market for stolen data (e.g. credit card information) in which hackers - thieves sell information retrieved and services designed to acquire data and system-level access (Odabas et al. 2017). For space reasons, we provide only a short overview of the three mechanisms.

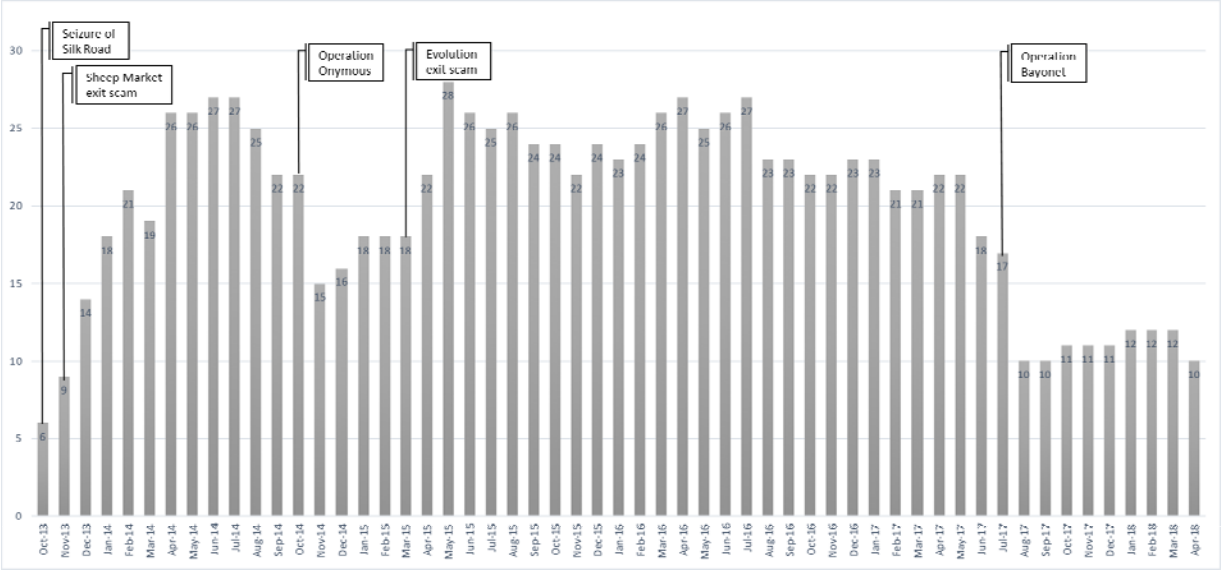

Figure 1. The establishment and termination of DNMs

Figure 1 provides a fine grained depiction of the evolution of the DNMs. Our analysis identifies development between October 2013 and April 2018 and the number of active sites, and indicates some key events. The first Dark Net site of which there was some public awareness, Silk Road, was closed down by the FBI in November 2013. At that point, there were 6 active sites; this number had increased to more than 25 by summer 2014. The Onymous operation in October 2014 resulted in some of these sites being closed down. In April 2015, the Evolution site was closed down by the site administrators who pocketed the funds. However, in the months following the number of active sites increased. After a period of relative stability involving more than 20 active sites, in July 2017 Operation Bayonet reduced this number to 5. At the time of writing (October 2018), the number of DNM sites actives is still low (8).

Through systematic retroduction we identified three high-level Dark Net mechanisms. Retroduction is a technique that looks for regularities not at the level of events but at the level of

causal mechanisms (Sayer 1994; Wynn and Williams 2012). These mechanisms operate on the structural elements and lead to observable events. Figure 2 provides a schematic illustration.

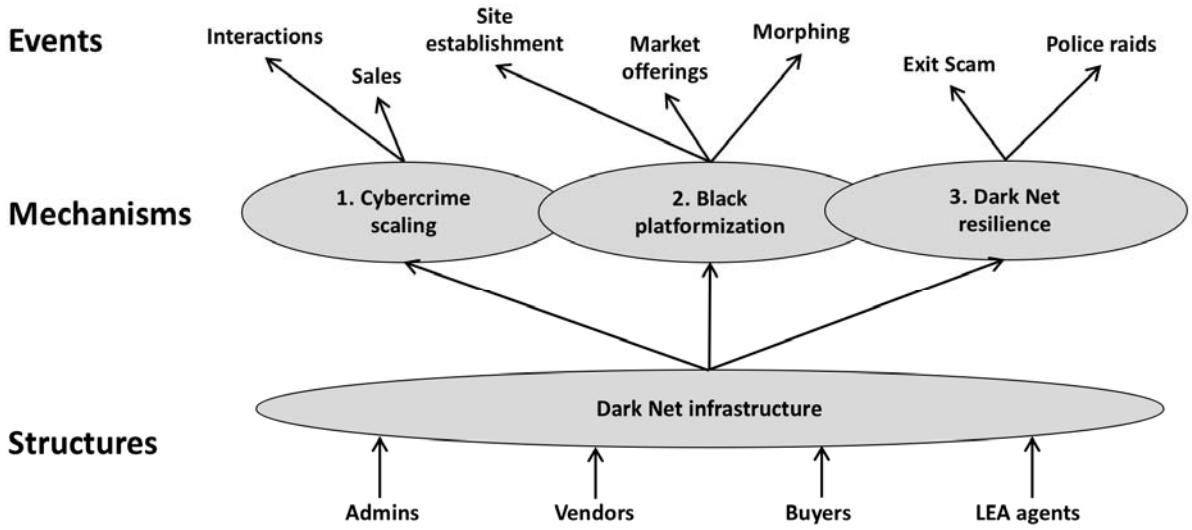

Figure 2. Events, mechanisms and structure

Mechanism 1: Cybercrime scaling

The structure of a DNM is quite similar to the structure of any other two-sided platform, and enables vendors and buyers to trade at low transaction costs (Parker and Van Alstyne 2005). Similar to traditional e-commerce platforms such as Amazon and eBay, DNM buyers can be victims of different forms of deception such as non-delivery of items, product inauthenticity, misrepresentation and shill bidding (Grazioli and Jarvenpaa 2000, 2003; Yar 2016). This risk is accentuated in DNMs given the lack of transparency and the impossibility to recur to trusted third parties in the case of disputes.

However, our evidence on the evolution of DNMs (Fig. 1) shows that despite police interventions and exit scams, black-markets are flourishing and supporting buyers and vendors to trade illegal goods successfully online. How can buyer, vendor and platform owner trust one another? The volume of transactions handled by DNMs shows that it is relatively easy for a buyer to browse the offerings, select an object, purchase it anonymously and rate the vendor. Therefore, vendors can build reputation by providing additional services and information to guarantee the quality of the purchase. Examples include the functions for checking the validity of stolen credit cards and the refunding policies issued by vendors. On the side of platform owners, advanced trust functions such as escrow and PGP (Pretty Good Privacy) multisignature are implemented in DNMs to prevent deception.

DNMs subsequent to Silk Road offer a larger variety of products and services such as credit card holograms, dumps, tools and guidelines for stealing and using stolen credit cards. These platforms activate network externalities by attracting new buyers and vendors and generating a cybercrime infrastructure. We describe this self-reinforcing mechanism as "cybercrime scaling". We define cybercrime scaling as a process where a *Cybercrime infrastructure enables vendors to build reputation, and successful purchases attract a critical mass of users to trade a greater variety of products and services.*

Mechanism 2: Black platformization

The second mechanism identified is called *black platformization*. We observed above that the Dark Net infrastructure is a powerful resource for establishing a market in both stolen data and hacking tools. For instance, hackers can develop and sell new versions of malware and

provide instructions to deceivers using secure communication channels. Sets of personal data are sold to deceivers who conduct personalized phishing campaigns to perform large scale fraud using cryptocurrencies to collect payments and enable money laundering.

Marketplace administrators constantly monitor the fast-evolving landscape of digital solutions and adapt their platforms by integrating functions to satisfy their users. Some black-markets specialize in serving a particular community, others serve different purposes. Therefore, DNMs can be conceptualized as digital platforms (Constantinides et al. 2018) enriched with new capabilities to follow the emerging needs of criminal communities. The Dark Net infrastructure consists of a combination of buyers, vendors and law enforcement agents adopting and innovating digital tools for anonymous interactions. The use of a virtual private network (VPN) to connect to the Tor network and install a new instance of a DNM (e.g. Silk Road 2) is an example of such interaction. We use the term platformization to emphasize the dynamic and volatile character of the innovation process taking place in the Dark Net infrastructure.

Black platformization is driven by the urgency to react to the new means adopted by LEAs in identifying online trade of illegal goods. Such crowd-based innovation exploits the potential of hacker communities whose cooperation is supported heavily by digital platforms (Samtani et al. 2017; Spagnoletti et al. 2015). For instance, payments methods for illegal goods changed from centralized services offered by actors in non-collaborating countries (e.g. Liberty Reserve in Costa Rica between 2006 and 2013) to decentralized systems based on blockchain technology (e.g. Bitcoin), to more recent tumbling tools for cryptocurrencies. These architectural changes were triggered by increased cooperation among LEAs (Hui et al. 2017) and

advancements in attribution methods and tools (i.e. "follow the money" practices). We define black platformization as a process where *the Dark Net infrastructure enables criminals to sell new digital products and DNM' administrators enhance the security and efficiency of transactions by implementing new features crowdsourced from hackers and online communities*.

Mechanism 3: Dark Net resilience

The specific characteristics of anonymous trade (i.e. anonymity, untraceability and illegality of the goods exchanged) lead to sudden and frequent interruptions to normal functioning. Such interruptions can be caused by sudden and unpredictable events such as an exit scam or a police operation. In the first case, the deceivers exploit the opportunity created by the presence in the escrow system of substantial amounts of money: the deceiver may simply transfer the crypto-currency to his or her own account, and close down the site leaving no traces of either vendors or buyers. In the case of police operations, LEAs seize sites and block the trade of illegal goods.

There are observable consequences of those events. For instance, the number of DNMs significantly reduces after documented police raids, while the Sheep Market and Evolution exit scams provoked reactions from the communities of users. In the Sheep Market case, users coordinated to collectively discover and disclose the identity of the deceiver. In the Evolution case, there was an increase in the number of active sites (see Fig. 1). After a period of "collective recovering" involving various different actions, we observe changes to both the process and technologies of the Dark Net. For instance, after an exit scam, vendors move to more trusted sites with enhanced security functionalities. Similarly, criminals react to the surveillance

activities of the police and experiment with new attack schemas based on the adoption of advanced tools such as peer-to-peer markets and payment systems, and encrypted point to point channels for communication (e.g. Tor on VPN).

We define *Dark Net resilience as a process where the Dark Net infrastructure enables successful and unpredictable actions by deceivers and LEAs to cause a breakdown in normal market operations that leads to a collective recovery among the user community determining the morphing of technological and fraudulent schemas*.

Table 2 presents a summary of the mechanisms and their link to the empirical data .

Table 2. Outcome of retroduction (adapted from Wynn and Williams (2012))

Mechanism	Definition	Key events	Data sources
Cybercrime scaling	Cybercrime infrastructure enables vendors to build their reputation and successful purchases attract a critical mass of users to trade a greater variety of products and services	Trusted credit card vendor Carder.su forum and card checking systems Liberty Reserve and Bitcoin Carding offerings in DNMs	Newspapers, court documents, police reports, blogs, Gwern Alphabay scraping
Black platformization	Dark Net infrastructure enables criminals to sell new digital products and DNMs' admins enhance the security and efficiency of transactions by implementing new features crowdsourced from hackers and online communities	Malware and ransomware Dataset of personal data Escrow and private messages Multisignature, Finalize Early and Forced PGP Vendor	Newspapers, police reports, blogs, websites, Gwern, IA
Dark Net resilience	Dark Net infrastructure enables successful and unpredictable actions of deceivers and LEAs to cause a breakdown in the normal market operation that leads to a collective recovery action by the user community determining the morphing of technological and fraudulent schema.	Sheep market and Evolution exit scams Peer to peer markets and payments LEAs cooperation to "Follow the money" Onymous and Bayonet operations	Newspapers, blogs, websites, IA, interviews with LEA, court documents, police reports

REFERENCES

Bartlett, J. 2014. *The Dark Net: Inside the Digital Underworld.*

Bhaskar, R. 1998. "General Introduction," in *Critical Realism: Essential Readings*, M. S. Archer, R. Bhaskar, A. Collier, T. Lawson, and A. Norrie (eds.), London: Routledge, Ix–Xxiv.

Bygstad, B., and Munkvold, B. E. 2011. "In Search of Mechanisms. Conducting a Critical Realist Data Analysis," in *Thirty Second International Conference on Information Systems, Shanghai*, pp. 1–15.

Chaudhry, P. E. 2017. "The Looming Shadow of Illicit Trade on the Internet," *Business Horizons* (60:1), Elsevier Ltd, pp. 77–89. (https://doi.org/10.1016/j.bushor.2016.09.002).

Constantinides, P., Henfridsson, O., and Parker, G. 2018. "Platforms and Infrastructures in the Digital Age," *Information Systems Research* (7047), pp. 1–20. (https://doi.org/10.1287/isre.2018.0794).

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., and Yoo, Y. 2015. "Distributed Tuning of Boundary Resources: The Case of Apple's IOS Service System," *MIS Quarterly* (39:1), pp. 217–243. (http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=100717566&site=ehost-live).

Edwards, P. N., Jackson, S. J., Chalmers, M. K., Bowker, G. C., Borgman, C. L., Ribes, D., Burton, M., and Calvert, S. 2013. *Knowledge Infrastructures : Intellectual Frameworks and Research Challenges*, (Ann Arbor:). (http://hdl.handle.net/2027.42/97552).

Europol. 2017. "Internet Organised Crime Threat Assessment (IOCTA) 2017." (https://www.europol.europa.eu/iocta/2017/index.html).

Ferguson, R. H. 2017. "Offline 'Stranger' and Online Lurker: Methods for an Ethnography of Illicit Transactions on the Darknet," *Qualitative Research* (17:6), SAGE Publications Ltd, pp. 683–698.

Grazioli, S., and Jarvenpaa, S. L. 2000. "Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers," *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans.* (30:4), pp. 395–410. (https://doi.org/10.1109/3468.852434).

Grazioli, S., and Jarvenpaa, S. L. 2003. "Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence," *International Journal of Electronic Commerce* (7:4), pp. 93–118. (https://doi.org/Article).

Hanseth, O., and Lyytinen, K. 2010. "Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet," *Journal of Information Technology* (25:1), Palgrave Macmillan, pp. 1–19.

Hedström, P., and Swedberg, R. 1996. "Social Mechanisms," *Acta Sociologica* (39:3), pp. 281–308.

Henfridsson, O., and Bygstad, B. 2013. "The Generative Mechanisms of Digital Infrastructure Evolution," *MIS Quarterly* (37:3), pp. 907–931.

Hui, K., Kim, S. H., and Wang, Q. 2017. "Cybercrime Deterrence and International Legislation: Evidence From Distributed Denial of Service Attacks," *MIS Quarterly* (41:2), pp. 497-A11.

(https://doi.org/10.14208/eer.2013.03.02.005).

Hurlburt, G. 2017. "Shining Light on the Dark Web," *Computer* (50:4), IEEE Computer Society, pp. 100–105. (https://doi.org/10.1109/MC.2017.110).

Kethineni, S., Cao, Y., and Dodge, C. 2017. "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes," *American Journal of Criminal Justice*, Springer New York LLC, pp. 1–17. (https://doi.org/10.1007/s12103-017-9394-6).

Kraemer-Mbula, E., Tang, P., and Rush, H. 2013. "The Cybercrime Ecosystem: Online Innovation in the Shadows?," *Technological Forecasting and Social Change* (80:3), pp. 541–555. (https://doi.org/10.1016/j.techfore.2012.07.002).

Milward, H. B., and Raab, J. 2006. "Dark Networks as Organizational Problems: Elements of a Theory," *International Public Management Journal* (9:3), Taylor & Francis, pp. 333–360.

Mingers, J. 2004. "Real-Izing Information Systems: Critical Realism as an Underpinning Philosophy for Information Systems," *Information and Organization* (14:2), pp. 87–103. (https://doi.org/10.1016/j.infoandorg.2003.06.001).

Odabas, M., Holt, T. J., and Breiger, R. L. 2017. "Governance in Online Stolen Data Markets," in *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy* (Vol. 87).

Parker, G. G., and Van Alstyne, M. W. 2005. "Two-Sided Network Effects: A Theory of Information Product Design," *Management Science* (51:10), pp. 1494–1504. (https://doi.org/10.1287/mnsc.1050.0400).

Samani, R. 2016. "Cybercrime: The Evolution of Traditional Crime," in *Beyond Convergence: World without Order*, H. Matfess and M. Miklaucic (eds.), Washington, D.C.: Center for Complex Operations Institute for National Strategic Studies National Defense University, pp. 275–296.

Samtani, S., Chinn, R., Chen, H., and Nunamaker, J. F. 2017. "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence," *Journal of Management Information Systems* (34:4), Routledge, pp. 1023–1053. (https://doi.org/10.1080/07421222.2017.1394049).

Sayer, A. 1994. *Method in Social Science. A Realist Approach*, Routledge.

Soska, K., and Christin, N. 2015. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem," *24th USENIX Security Symposium*, pp. 33–48.

Spagnoletti, P., Me, G., Ceci, F., and Andrea Prencipe. 2018. "Securing National E-ID Infrastructures: Tor Networks as a Source of Threats," in *Organizing for the Digital World. IT for Individuals, Communities and Societies.*, F. Cabitza, C. Batini, and M. Magni (eds.), LNISO - Springer, pp. 1–14.

Spagnoletti, P., Resca, A., and Lee, G. 2015. "A Design Theory for Digital Platforms Supporting Online Communities: A Multiple Case Study," *Journal of Information Technology* (30), pp. 364–380. (https://doi.org/10.1057/jit.2014.37).

Wynn, D., and Williams, C. K. 2012. "Principles for Conducting Critical Realist Case Study Research in Information Systems," *MIS Quarterly* (36:3), pp. 787–810.

Yar, M. 2016. *Cybercrime and Society*, (2nd ed.), London: Sage. (https://doi.org/10.1177/1741659006069691).