Mechanisms Fostering the Misuse of Information Systems for Corrupt Practices in the Nigerian Public Sector

Ibrahim Inuwa(✉), Chidi Ononiwu, Muhammadou M. O. Kah, and Ago K. M. Quaye

American University of Nigeria, (AUN), Yola, Nigeria
ibrahim.inuwa@aun.edu.ng

Abstract. The paper explores the misuse of information systems for corrupt practices in the Nigerian public sector as a phenomenon under study. Routine Activity theory, Model of Emergent IT Use, and Normalization theory were used as lenses. Danermark et al.'s six stage framework with a single case-study was adopted as the critical realist methodology. The anti-corruption and regulatory agency, the Economic and Financial Crimes Commission of Nigeria, is the case in focus. Semi-structured interviews, archival documents and press media were used as data sources. By analyzing the data, we identified motivated offender, suitable target, and the absence of a capable guardian as the entities/factors that characterized the phenomenon. Political clientelism patronage, socialization, embeddedness of corrupt routine into IT artifacts and rationalization were identified as causal mechanisms with culture as the enabling conditions. Dysfunctional structures of the Nigerian public sector were also identified as structures that breed the mechanisms. The study findings contribute to theory, practice, and the methodology of critical realism.

Keywords: Information systems · Misuse · Corrupt practices · Public sector

1 Motivation and Research Questions

The misuse of information systems (IS) for corrupt practices in the public sector is classified by IS scholars [e.g., 1, 2] as one of the "dark sides" of information technology (IT) usage. In this context IS covers e-government, business enterprise systems, computer mediated communications such as emails and mobile applications adopted by the public sector to deliver services to its citizenry. The revelation of Tarafdar, Gupta [2] coincides with the concerns of other IS scholars, who have observed that misuse of IS has enabled corrupt practices over the years [3–6]. Corrupt practices is defined as the form of financial crime that is skewed towards occupational fraud [7], involving the intentional misuse of organizational resources by employees. Financial crime described here could occur with or without IS in the public institutions. However, the focus of this paper is on corporate frauds that are facilitated with the use of implemented IS, which we conceptualize as misuse of IS for corrupt practices in public institutions.

Published by Springer Nature Switzerland AG 2019
P. Nielsen and H. C. Kimaro (Eds.): ICT4D 2019, IFIP AICT 552, pp. 122–134, 2019.
https://doi.org/10.1007/978-3-030-19115-3_11

IS has been touted for fostering development and contributing to citizens' right to freedom for better lives as well as fight corrupt practices in the public sector [8].

Despite the much anticipated expectations of IS to help curb corrupt practices, there is overwhelming anecdotal evidence that suggest that IS adoption has been misappropriated to enable corrupt practices in public institutions [3–5]. A typical example, is that of a Nigerian civil servant who was arraigned before an Abuja High Court by the Economic and Financial Crimes Commission (EFCC), "…for allegedly manipulating the Integrated Personnel and Payroll Information System [IPPIS] in collaboration with two of her sisters to enrich themselves. IPPIS is one of the functional systems [used by] the [Nigerian] Government [to pay] staff salaries" [9]. Such corrupt practices are seen as a "broad collection of 'negative' phenomena that are associated with the use of IT and that have the potential to infringe on the well-being of individuals, organizations and societies" [2, p. 161]. Following Heeks [5], we are of the notion that IS designed to function properly within an organization "have no innate property related to corruption except that of their imagery. They do not automatically provide a Panoptic model of control- this only comes if they are deliberately and systematically designed to do so" (p. 185). Therefore, the purpose of this paper is to explore and understand why misuse of IS for corrupt practices occur in the Nigerian public sector. Thus, we pose the following research questions: RQ1: What entities/factors characterize the misuse of IS for corrupt practices in the Nigerian public sector? and RQ2: What mechanisms are responsible for the misuse of IS for corrupt practices in the Nigerian public sector? The rest of this paper is organized as follows: Sect. 2 consists of the theoretical redescription of the context. Section 3 discusses the methodology. Section 4 presents the research findings and discussion. Section 5 presents the conclusion.

2 Theoretical Redescription of the Context/Research

To focus the research, we first consider RAT to understand and cluster what characterized the misuse of IS in our context as entities/factors. Given the multiple understandings of misuse of IS for corrupt practices, the entities help us to understand each perspective of corruption as a different frame of interpretation that triggers different program of actions. RAT proposed three terms/concepts - motivated offender, suitable target, and the absence of a capable guardian - stemming from the environment where the crime occurred. The theory argues that a crime is bound to take place at the convergence of the three concepts in time and space [10, 11]. The concepts represent *terministic clusters* that are used to group the dialectical negotiation of people's perceptions and experiences about the events. Such concepts have been adopted extensively in criminology research and when particularized to the context of misuse of IS for corrupt practices, RAT concepts can be used to cluster the entities associated with improper IS use. Motivated offender is a concept used to cluster occurrences of misuse of IS for corrupt practices that arise from IT employees conniving with their colleagues to compromise public sector IT infrastructures under their care. Suitable target is a concept that represent IS that are loosely coupled security-wise or an easily compromised IS by employees, while the absence of capable guardians could result in poor IT governance, legal and policing barriers in the adopting organization's routines of operation.

To understand the structures and mechanisms at the real domain, NT [12] and the MEITU [13] were adopted. NT focuses on the normalization of corruption in an organization through institutionalization, rationalization and socialization [12]. When particularized to our context, institutionalization is the process through which misuse of IS for corrupt practices are enacted by corrupt individuals as a matter of routine without regard for their reputation. Rationalization typifies a self-serving ideology develop to justify and perhaps even valorise misuse of IS for corrupt practices. Socialization is where new IT employees are induced to view misuse of IS for corrupt practices as permissible if not desirable. The concepts are mutually reinforcing and equally interdependent. Once established in an organization, the concepts create a situation where misuse of IS for corrupt practices can be practiced collectively by employees and may persist indefinitely [12]. On the other hand, MEITU provides a model for explaining the interplay of distinctive sets of causal powers of embedding organizational structures, culture, routines, institutional and environmental contexts into IT artifact by human agencies through socialization and reflexivity [13]. The two adopted theories can be helpful in understanding the misuse of IS for corrupt practices within the organizational setting, especially where corruption has been illegally and surreptitiously institutionalized with the help of implemented IT artifact. The overlap of the two theories occur in socialization, where corrupt individuals socialize to enact their corrupt routines into IT artifact through reflexivity.

Since all theories presuppose a set of philosophical assumptions about the nature of reality (ontology) [13, 14], we draw from critical realism (CR) to posit that the event/phenomenon understudy is stratified into three domains – the real, the actual and the empirical. The empirical domain is the experienced and observed layer, where the misuse of IS for corrupt practices is mediated through the lens of human experience and interpretation. The actual domain is where entities that constitute the phenomenon under study reside. Such entities may or may not be experienced/observed. The third is the real layer that consists of interactive causal forces which produce the phenomenon understudy at the empirical level. Thus, the primary goal of the research is "to explain the misuse of IS for corrupt practices through reference to the causal mechanisms and the effects they can have throughout the three layers of reality" [15, p. 183].

Apart from the nature of reality, all theories presuppose a set of philosophical assumptions about how reality can be known (epistemology) and theories thus, are the epistemological objects of science used in the social practice of research [13]. Thus, we engaged the concepts of RAT to cluster the entities into factors and posit such entities as what exist at the actual domain, while NT and MEITU theories are used to mediate into the real to identify the causal mechanisms that could cause misuse of IS for corrupt practices in the Nigerian public sector. Such mechanisms "exist only in virtue of the activities they govern and cannot be empirically identified independently of them" [16, p. 41]. It then follows that such mechanisms can be explained ultimately through the study of the phenomenon at the empirical level. However, the misuse of IS for corrupt practices exist in the social world that is dynamic and unpredictably open, there are social conditions inherent in causal mechanisms that could enable or constrain it from acting in certain ways [16]. In CR research, researchers engage in a retroductive reasoning process to identify such conditions for the actualization of causal mechanisms in the level of reality [16].

3 Methodology

To provide explanation of the process involved in conducting CR research, the present study follows the six stage methodological guidelines suggested by Danermark et al. [17, pp. 108–112]. When particularized to our context, the six stage includes: (1) description, which describes the misuse of IS for corrupt practices in the Nigerian public sector using everyday concepts and the interpretations of those involved; (2) analytical resolution which separates out various dimensions of misuse of IS for corrupt practices as factors that characterize the event; (3) abduction and theoretical redescription in which misuse of IS for corrupt practices are interpreted through theories that match the empirical situation discovered in stage one; (4) retroduction which identifies the structures and mechanisms and postulate them as what must exist for misuse of IS for corrupt practices to occur in the Nigerian public sector; (5) which can be included in stage four, compares various theories and abstractions to determine the relative explanatory power of the mechanisms and structures identified earlier, and; (6) concretization and contextualization, is the discussion stage of how the empirically identified mechanisms interact and manifest themselves in the concrete event under specific conditions in the same or different context.

3.1 Methods of Data Collection

The empirical data emanates from the EFCC as a case study research [18]. We adopted semi-structured interviews (i.e., face-to-face & focus group) as primary source of data, while archival documents, blogs, and press media were used as secondary data source [19]. EFCC is an agency of the Nigerian government that is saddled with the responsibility of combating financial and economic crimes, with headquarters in Abuja–Nigeria. The agency, the custodian of the evidence-based cases, also interrogates and prosecutes/investigates offenders of IS misuse for corrupt practices. Twenty-five EFCC cybercrime experts at the managerial level were used as proxies for the interview. They consist of 5 from forensic unit, 5 from legal and operations unit, 5 from IT unit, 10 from cybercrime unit. The choices were based on experience on the job, length of service at EFCC which we gleaned from long service awards received by staff and their technical expertise. Consent forms, guaranteeing confidentiality, voluntariness and ethical clearance as stipulated in the American university of Nigeria codes of ethics for research were given to each to complete. Getting access to interview the offenders directly proved to be difficult since most offenders are either in the prison or have fled the country for fear of prosecution. Besides, it is most likely that the offenders may not disclose information to researchers, rather, they can open up to EFCC operatives and the courts because evidences of their criminal acts have been established. Archival data such as court verdicts and interrogative documents on a case by case bases were also looked into. We collected more than one hundred court verdicts and other interrogative documents, out of which twenty-five were usable for corroborating the interview data. For the focus interview, assemblage of the group arises from informants from cybercrime, legal, research, forensic, and legal and operations units of EFCC and they are ten informants in number. The group brainstormed towards providing answers to our questions such as “what do you think could cause misuse of IS for corrupt practices to exist? What characterized such a misuse?” Among others. We audio-taped the discussion and also observed their body languages. Besides, second rounds of interviews were conducted between February 2018 and May 2018 respectively as a follow up to the focus interviews. The interviews lasted for about 50 min in each case. We moderated the interviews and audio taped (with their consent) it as well on a non-threatening environment to avoid distractions. We then pass-worded the folder that contained the file for safe keeping.

3.2 Methods of Data Analysis

At first, we transcribed the audio taped data into a word document of sixty-five pages, we triangulated the primary data sources to corroborate the secondary data for more insights. Data coding process was done in two stages: (1) data coding process of searching for entities that characterized the misuse of IS for corrupt practices as factors; and (2) data analysis through abduction and retroduction as shown in Fig. 1.

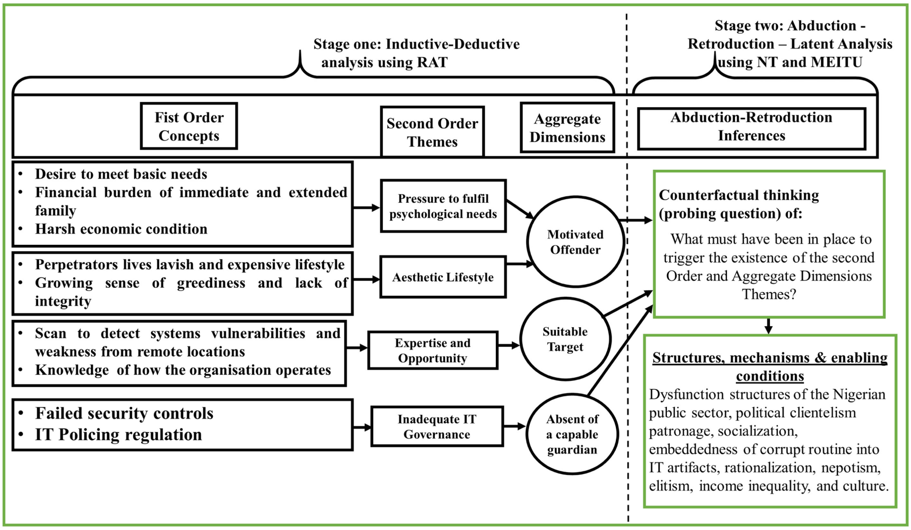
Stage one: Inductive-Deductive analysis using RAT
Stage two: Abduction - Retroduction – Latent Analysis using NT and MEITU
Fist Order Concepts
Second Order Themes
Aggregate Dimensions
Abduction-Retroduction Inferences
• Desire to meet basic needs
• Financial burden of immediate and extended family
• Harsh economic condition
Pressure to fulfil psychological needs
• Perpetrators lives lavish and expensive lifestyle
• Growing sense of greediness and lack of integrity
Aesthetic Lifestyle
Motivated Offender
• Scan to detect systems vulnerabilities and weakness from remote locations
• Knowledge of how the organisation operates
Expertise and Opportunity
Suitable Target
• Failed security controls
• IT Policing regulation
Inadequate IT Governance
Absent of a capable guardian
Counterfactual thinking (probing question) of:
What must have been in place to trigger the existence of the second Order and Aggregate Dimensions Themes?
Structures, mechanisms & enabling conditions
Dysfunction structures of the Nigerian public sector, political clientelism patronage, socialization, embeddedness of corrupt routine into IT artifacts, rationalization, nepotism, elitism, income inequality, and culture.

Fig. 1. Inductive-deductive semantic and abductive – retroductive latent data analysis [Adapted from 20, 21].

During stage one, the cycles of the coding process followed the inductive-deductive logic via a flexible theory “directed” coding process [20, 21]. The theory here is the RAT, where three concepts - motivated offender, suitable target, and the absence of a capable guardian- are used as terministic clusters of entities [22, 23] or themes [20, 21] that are grounded in the data. The terministic clusters represent theoretical grouping of the verbalization of the multiple interviewees as entities. Such entities express different dimensions surrounding the occurrence of the phenomenon understudy. It is more likely that there will be multiple perceptions and experiences about the occurrences of the phenomenon, and such will be expressed agonistically and consistently in the verbalization discourse. Indeed, we must exercise care to recognize and protect these terministic tensions as entities that reside at the actual domain within the social context that misuse of IS for corrupt practices occurred. Thus, the data coding process is guided by provisional codes that draw upon the RAT and the stratified ontological view of reality as endorsed by CR. Throughout the coding cycles, the most prominent codes are used as a foundation to identify the entities as factors that characterized the empirical situation.

After identifying the tendencies of the data, the second stage is the latent data analysis. This consists of abductive-retroductive reasoning to identify the misuse of IS for corrupt practices by engaging with the existing theories [12]. Abductive reasoning is the spotting of patterns and relationships in sets of data and matching them with theories or theoretical concepts, with a view to selecting theories or theoretical concepts with significant explanatory power or which offer better explanations [24, 25]. Thus, NT [12] and the MEITU [13] were applied not to mold the data to fit the preconceptions of the theories. Rather to identify the mechanisms operating in the empirical situation by choosing between a number of possible frames of theories to interpret particular empirical situation. The final stage of data analysis aims to ascertain the contextual condition for the causal mechanism to take effect and to result in what were seen from the empirical data. To identify the necessary contextual conditions, a retroductive reasoning process is applied by constantly moving from the empirical domain to the deeper levels of reality through counterfactual thinking and questioning (i.e., what must have been in place for the data to have been observed in the empirical domain) [26].

Again, NT and MEITU were applied to identify the specific context of the actualization of the causal mechanism as it relates to the social structures. Thus, analysis of the empirical data provides evidence of the observable outcome (i.e., misuse of IS for corrupt practices) that may enable plausible explanations of the generative mechanisms and enabling conditions that caused such an outcome to be hypothesized. Thus, empirical data analysis is not an end in itself but serves as a facilitation agent preparing the data needed to enable retroduction and abduction. It is an interim step and requires a combination of data from each of the three sources of empirical data described in Sect. 3.1. The raw material provided by analysis can then be interpreted using Danermark et al.’s framework to explain the entities and generative mechanisms giving rise to both visible outcome and causal inference as detailed next.

4 Research Findings

Stage 1 - Description of the context: In 1999, Nigerians adopted a constitution that empowered the public sector to exist and function. It encompassed over one hundred ministries, departments and agencies (MDAs) through which the government implements policies and delivers services to the citizenry. Such services spans health, security, education, utilities, and infrastructures among others. It is also categorized into Federal Civil Services, State Civil Services, Local Government Services, and the Public bureaucracy that includes the National and State Assemblies. Not long after inception, services to the citizenry have been characterized with intense corruption that have impeded good governance. Corrupt practices manifest in the form of bribery, misappropriation, embezzlement, and money laundering among others. To find solution to such corrupt practices the government of Olusegun Obasanjo in 1999 sought for the introduction of EFCC an anti-graft agency and the digitalization of the bureaucratic services across its MDAs via e-government initiatives. The EFCC Establishment Act of 2004 and the Money Laundering Act of 2004 legalized and governed its activities. Between 2004 and 2018 EFCC investigated/prosecuted several corrupt bureaucrats and politicians including state governors some of whom were convicted with jail terms while others are still facing trials in various courts as stated by one respondent, that "the cases are still ongoing in courts… there are many of them". Interviewee #8.

To strengthen the digitization agenda, the government in 2000–2001 enacted the National Telecommunications (NT) and the National Information Technology Policy (NITP) to regulate and manage the telecomm and IT industries. To enforce the digitization process into the fabric of the public sector, the National e-government Strategies (NeGSts) was created in 2004. Despite such attempts, it is rather unfortunate that the impact of EFCC and e-government initiatives seem not to have attained expected goals. In fact, our data suggests that the e-government systems domiciled in the MDAs were misused by bureaucrats and IT vendors for corrupt practices. Among such systems were the IPPIS and the Government Integrated Financial Management Information Systems (GIFMIS). The IPPIS platform plugged out over 46,000 "*ghost workers*" when it was initially implemented. However, such *ghost workers* found their way back into the system due to misuse by a group of syndicates (i.e., corrupt IT official(s)) as commented by one of our informant: "A director in the IPPIS and the IT vendors… are responsible for compromising the systems, they introduce *ghost workers* into the government payroll illegally". Interviewee #2. Another informant stated "…group of fraudsters recruited an IT staff in the office of the accountant general of the federation (AGF), now this guy connected the fraudsters to the network inside the AGF's office, scanned the network and exploit its vulnerabilities to transfer funds into various bank accounts". Interviewee #4.

Stage 2 - Analytical resolution: Misuse of IS for corrupt practices in the Nigerian public sector can be dissected into motivated offender based, suitable target based, and the absence of a capable guardian based dimensions. Such dimensions are entities that exist as individual instances of things under study [27], which we classify as factors that characterized the phenomenon. The dimensions are discussed as follows:

Motivated offender-based form of misuse of IS for corrupt practices: Misuse of IS for corrupt practices as a long term problem in the Nigerian public sector is framed by most informants as an invasive corruption perpetrated by motivated top employees at managerial levels in collaboration with external IT consultants within the public sector. Being vested with powers and the responsibility for approving changes in systems, they collude with the external IT consultants responsible for IT governance and control to compromise the system to meet their psychological needs. The following brief excerpts illustrate this terministic screen as stated by one informant "A Director in the IPPIS and the private entity [i.e., IT vendor] in charge of managing the IPPIS infrastructures… are responsible for compromising the systems, and this is common to all the IT platforms that you see in the public sector, they do this to make ends meet". Interviewee #2. Employees with pressure to fulfil the need of shelter, food and immediate need of families and acquaintances as stated by two respondents: "A syndicate confided in us that he perpetrated the act because his take home pay does not actually take him home. Besides, the pay he receives as salary does not meet the needs of the family". Interviewees #2 and #10. Other bureaucrats, who misuse IS for corrupt practice, exhibit lifestyles of pleasure, ownership of many exotic cars and expensive houses as exclaimed by two informants "… what do they use it for [i.e., the stolen funds]? Lavish and expensive life-style!" Interviewees #4 and #14.

Suitable target-based form of misuse of IS for corrupt practices: By clustering misuse of IS for corrupt practices as suitable target, informants give strong, severe and very negative connotations to e-government IT platforms and the dishonest IT officials and managers that man such IT platforms. Thus, such a dysfunctional public sector environment becomes a suitable target for breeding misuse of IS for corrupt practices. Our findings revealed that the syndicates of corporate and state fraud are IT experts who had been with the affected organizations for many years and have expertise on operations of the systems and the organization itself. This provides them the opportunity to capitalize on and coordinate to erroneously manipulate the IS at will. One informant attests that: "The syndicates are experts in IT, and as such they focus on vulnerabilities . . . then they . . . take advantage of the weaknesses of the system to penetrate … and transfer funds into different accounts for selfish gains. Such actions are usually done after working hours or on weekends". Interviewee #4. Suitable target refers to an opportunistic scenario where employees strive to use their IT skills to steal from national coffers.

Absence of a capable guardianship-based form of misuse of IS for corrupt practices: A third cluster of terms is absence of a capable guardianship. This type of misuse suggests that corruption is associated with deliberate relaxation of adequate control measures and IT polices to foster insider's cooperation to compromise the system. Such an environment breeds willing offenders to do the "needful" as commented by another informant: "…it is not the case that the IT is not functioning, but there is lack of trusted people, so vulnerabilities of the system are exploited. A situation where a director is also the chairman of the IT steering committee is the head of the corrupt syndicates, what do you do?" Interviewee #5. Absence of a capable guardianship is associated with distrust of the citizenry which becomes entangled in the culture of a given society.

Overall, the brief description and the elicitation of the three entities demonstrate the crucial elements for hypothesizing plausible generative mechanisms that produce the visible outcome, are explained further in stages 3–4 of the Danermark et al.'s [17, pp. 108–112] framework below.

Stage 3–4 - Abduction and Retroduction – identification of structures, mechanisms and conditions: We used theories of MEITU and NT to look in the data via abductive reasoning, while retroduction was used to identify the structures, mechanisms and the enabling conditions. With MEITU, we identified the dysfunctional structures of the Nigerian public sector as structures. Such structures manifest as: the quasi-democratic hijack of power by elites and their kleptocratic hijack of national sovereignty [28], a centralized economic decision-making and disbursement of funds, lawlessness in the administrative process, considerable lack of exemplary ethical leadership exhibited by politicians and senior public officials and deformed sociocultural norms that are skewed towards loyalty to friends, politicians, tribe and, superiors [28]. As commented by one informant: "Politicians highjack the institutions of government and make them to operate in their own way without observing the code of conducts guiding public service… institutions are centrally managed by corrupt politicians and bureaucrats who do not have conscience and morality…". Interviewee #16.

The dominant presence of dysfunctional structures gave rise to embeddedness of corrupt routines into IT artifacts as one of the mechanisms. Such a mechanism exists due to activities of motivated offenders who inscribe their corrupt intent into the IT artifacts through socialization. One informant commented: "pay officers, directors of ministries, and IT vendors entrusted for IT governance…. collude to help one another and rewrite the sources codes of the systems to pay ghost workers, employees in the ministries will not even report, they take their share of the proceeds, he [the director] takes his cuts, so it is a win-win situation for all of them". Interviewee #3. Thus, employees and IT vendors leverage socialization processes as a mechanism to normalize their corrupt tendencies. Cliques of syndicates with a common interest are formed to undermine IT governance and policies. An excerpt from an informant enlightens us thus: "…it is not that the IT controls are not functioning, it is the people that are compromising it, and they collude with one another. Where there is supposed to be a dual authentication, if the two people agree to help each other, the control is useless…" Interviewee #5. The long-term socialization process valorizes the misuse of IS as one informant attests: "… his bosses are busy making money on the basis of inserting ghost workers into the IPPIS…. he has to joyfully commit the act as well since there seem to be no consequences". Interviewee #5. Thus, rationalization becomes another mechanism in the context.

Cliques of syndicates with a common interest in the socialization process are actually stooges or proxies of politicians in the ruling political party. Such cliques are strategically positioned in IT infrastructures in critical ministries for the sole purpose of fraud. Proceeds from the fraud are given to the politicians who put them there on a sharing formula based on percentages. Thus, political clientelism patronage is one of the mechanisms operating in the context. Political clientelism patronage defined as "a more or less personalized relationship between actors… commanding unequal wealth, status or influence, based on conditional loyalties and involving mutually beneficial transactions" [29, p. 69] positions the politicians at a high level in the pyramid of loyalty, allegiance, and respect. Such a positioning breeds corrupt bureaucrats who collude with their cliques to embed corrupt routines into IT artifacts as stated by an informant: "one syndicate confided in us [the EFFC] that they are in government and wield power". Interviewee #17.

The identified structures and mechanisms are seen as tendencies and liabilities, i.e., susceptible to the powers of other mechanisms. They operate, in our case, by the help of enabling conditions. The key enabling condition, identified in our context, by drawing from MEITU is culture. Culture, defined as shared beliefs, values, attitudes, norms, customs and tradition established to strongly influence human behavior and reveals basic assumptions of how things are done by a particular group of people [30], is deeply shrouded in corruption in the Nigeria context. The following excerpts from informants summarize it: "Corruption is so pervasive in this country that it would be nearly correct to say that it is a way of life". Interview #11. "The reason why looting of public funds using IT is that Nigeria is morally bankrupt and IT has now become the facilitating agent. Despite our preference for anti-corruption set of rules, Nigerian governance culture is giving everybody the feeling of – "if you can't beat them, then you join them". Interviewee #18. "Our value system allows so much nepotism, impunity and lawlessness in the public sector and this is reflected in our national culture and the way we do things, even in using IT." Interviewee #20.

Stage 5 - Compares various theories and abstractions: Arguably, other potential mechanisms might be at work in our context. For instance, one might hypothesize that nepotism defined as a form of undue bureaucratic favoritism enjoyed by friends, members of the same tribes, and families of those in power or that elitism and income inequality (i.e., misallocation of national wealth in favor of elites to enrich a few at the expense of the nation as a whole) might explain the misuse of IS for corrupt practices in the Nigerian public sector. However, they were eliminated because of their plausibility of lack of a strong explanatory power in the empirical evidence [31, 32]. Several alternative and rival mechanisms were empirically collaborated to be at work [33], including nepotism, elitism and income inequality. However, mechanisms consistent with the whole data material, including feedback from key informants seem offered strong explanatory power and were therefore selected.

Stage 6 - concretization and contextualization – Discussion: Beyond the realm of experiences, there is a polysemy of misuse of IS for corrupt practices identified as motivated offenders, suitable targets, and absence of a capable guardians residing as entities/factors at the actual domain as shown in Fig. 2. This polysemous condition of misuse of IS has both material consequences leading to the normalization of corruption. The three different terministic screens that informants use to construct misuse of IS for corrupt practices suggest distinct programs of action as material consequences. For instance, motivated offender perspective regard wealthy Nigerians as corrupt, which might not necessary be the case. Thus, terrace and luxury houses or exotic cars are under the watch of EFCC with a view of interrogating owners. Suitable target perspective regards IT infrastructures in the public sector as an opportunistic artifact to steal, while absence of a capable guardians perceived IT employees as culprits and colluders with bureaucrats and politicians to defraud the Nigerian state. To give rise to such polysemous condition of misuse of IS are political clientelism patronage, socialization, embeddedness of corrupt routines into IT artifacts and rationalization mechanisms that interact to cause misuse of IS for corrupt practices. However, such interaction of the mechanisms would not have been fully possible without the enabling conditions of culture. The dysfunction structures of the Nigerian public sector were also identified as structures that breed such mechanisms as shown in Fig. 2 as the research model. Hence, our contribution.

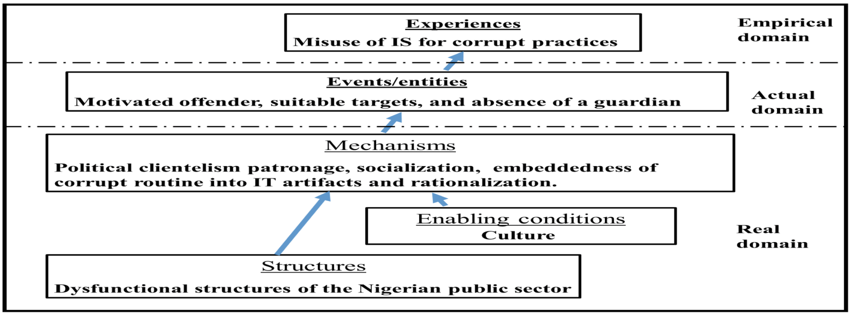
Experiences
Misuse of IS for corrupt practices
Empirical domain
Events/entities
Motivated offender, suitable targets, and absence of a guardian
Actual domain
Mechanisms
Political clientelism patronage, socialization, embeddedness of corrupt routine into IT artifacts and rationalization.
Enabling conditions
Culture
Real domain
Structures
Dysfunctional structures of the Nigerian public sector

Fig. 2. A realist model of IS misuse for corrupt practices in the Nigerian public sector.

5 Conclusion

In this paper, we leveraged the CR single case-study methodology to identify the generative mechanisms and enabling condition in concerted interactive form to cause misuse of IS for corrupt practices in the Nigerian public sector. Such misuse of IS was identified to have entities/factors (i.e., motivated offenders, suitable targets, and absence of a capable guardians) which represent the different interpretations and meanings given to it by the Nigerian audience. The identified mechanisms (i.e., political clientelism patronage, socialization, embeddedness of corrupt routine into IT artifacts, and rationalization) breed within the dysfunctional structures of the Nigerian public sector, with culture as the enabling condition. Thus, the paper contributes to both theory, practice and CR methodology. In theory, the research model in Fig. 2 is first of its kind in literature to explain the cause of misuse of IS for corrupt practices and the various interpretations and meanings in Nigeria. In practice, EFCC can use the research findings for intervention purposes. Lastly, by using CR methodology, we further added to the application of CR methodology literature. Presently, this paper identified a few generative mechanisms at work, thus, future study can identify more generative mechanisms and enabling conditions and their interplay until closure is attained.

References

1. D'Arcy, J., et al.: Reflecting on the "dark side" of information technology use. Commun. Assoc. Inf. Syst. **35**(5), 109–118 (2014)
2. Tarafdar, M., Gupta, A., Turel, O.: Editorial-special issue on 'dark side of information technology use': an introduction and a framework for research. Inf. Syst. J. **25**(3), 161–170 (2015)
3. Hutchings, A., Jorna, P.: Misuse of information and communications technology within the public sector. In: Tomison, D.A.M. (ed.) Trends and Issues in Crime and Criminal Justice, pp. 1–9. Institute of Criminology, Australia (2015)
4. Smith, R.G., Jorna, P.: Corrupt misuse of information and communication technologies. In: Handbook of Global Research and Practice in Corruption, pp. 255–281. Edward Elgar Publishing Limited, Cheltenham (2011)
5. Heeks, R.: Information technology and the management of corruption. Dev. Pract. **9**(1–2), 184–189 (1999)
6. Willison, R., Lowry, P.B.: Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives. ACM SIGMIS Database: Database Adv. Inf. Syst. **49**(1), 81–102 (2018)
7. Gottschalk, P.: Categories of financial crime. J. Financ. Crime **17**(4), 441–458 (2010)
8. Walsham, G., Robey, D., Sahay, S.: Foreword-special issue on information systems in developing countries. MIS Q. **31**(2), 317–326 (2007)
9. Punch-Newspaper: Ghost workers: EFCC arraigns family members for manipulating government's payroll. http://saharareporters.com/2017/06/07/ghost-workers-efcc-arraigns-family-members-manipulating-governments-payroll. Accessed 16 Jan 2018
10. Cohen, L.E., Felson, M.: Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. **44**, 588–608 (1979)
11. Felson, M., Clarke, R.V.: Opportunity makes the thief. Police research series, 98 (1998)
12. Ashforth, B.E., Anand, V.: The normalization of corruption in organizations. Res. Organ. Behav. **25**, 1–52 (2003)
13. Ononiwu, C.G., Brown, I.: Theorisation in critical realist IS research and its implications on structure and agency interplay: a morphogenetic approach. In: The Proceedings of the 21st ECIS 2013 Conference, Utrecht, Netherlands (2013)
14. Holland, D.: Integrating Knowledge Through Interdisciplinary Research: Problems of Theory and Practice. Routledge, London (2014)
15. Fletcher, A.J.: Applying critical realism in qualitative research: methodology meets method. Int. J. Soc. Res. Methodol. **20**(2), 1–14 (2016)
16. Bhaskar, R.: The Possibility of Naturalism: A Philosophical Critique of the Contemporary Human Sciences. Routledge, London (1998)
17. Danermark, B., et al.: Explaining Society: Critical Realism in the Social Sciences. Routledge, London (2002)
18. Easton, G.: Critical realism in case study research. Ind. Mark. Manag. **39**, 118–128 (2010)
19. Saunders, M., Lewis, P., Thornhill, A.: Research Methods for Business Students. Person Education Limited, Harlow (2009)
20. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qual. Res. Psychol. **3**(2), 77–101 (2006)
21. Gioia, D.A., Corley, K.G., Hamilton, A.L.: Seeking qualitative rigor in inductive research: notes on the Gioia methodology. Organ. Res. Methods **16**(1), 15–31 (2013)
22. Burke, K.: Terministic screens. In: Language as Symbolic Action: Essays on Life, Literature, and Method, pp. 44–57. University of California Press, Berkeley (1966)

23. Angel, A., Bates, B.: Terministic screens of corruption: a cluster analysis of Colombian radio conversations. J. Kenneth Burke **10** (2014)
24. Dixon, D.: Analysis tool or research methodology: is there an epistemology for patterns? In: Berry, D.M. (ed.) Understanding Digital Humanities, pp. 191–209. Palgrave Macmillan, London (2012). https://doi.org/10.1057/9780230371934_11
25. Eastwood, J.G., Jalaludin, B.B., Kemp, L.A.: Realist explanatory theory building method for social epidemiology: a protocol for a mixed method multilevel study of neighbourhood context and postnatal depression. SpringerPlus **3**, 12 (2014)
26. Meyer, S.B., Lunnay, B.: The application of abductive and retroductive inference for the design and analysis of theory-driven sociological research. Sociol. Res. Online **18**(1), 12 (2013)
27. Elder-Vass, D.: Re-examining Bhaskar's three ontological domains: the lessons from emergence. In: Contributions to Social Ontology, pp. 174–190. Routledge (2013)
28. Hope, K.R.: Corruption and development in Africa. In: Hope, K.R., Chikulo, B.C. (eds.) Corruption and Development in Africa, pp. 17–39. Palgrave Macmillan, London (2000). https://doi.org/10.1057/9780333982440_2
29. Lemarchand, R.: Political clientelism and ethnicity in tropical Africa: competing solidarities in nation-building. Am. Polit. Sci. Rev. **66**(1), 68–90 (1972)
30. Hofstede, G.: Dimensionalizing cultures: the Hofstede model in context. Online Read. Psychol. Cult. **2**(1) (2011)
31. Bygstad, B.: Generative mechanisms for innovation in information infrastructures. Inf. Organ. **20**(3–4), 156–168 (2010)
32. Sayer, A.: Method in Social Science: A Realist Approach, 2nd edn. Routledge, New York (1992)
33. Wynn Jr., D.E., Williams, C.K.: Principle for conducting critical realist case study research in information systems. MIS Q. **36**(3), 787–810 (2012)