HUMAN / TECHNOLOGY CO-ADAPTATION IN THE CONTEXT OF CYBERSECURITY

Research paper

Chemsi, Rachid, UNSW, Sydney, Australia, rachid.chemsi@dsfaustralia.com

Abstract

Understanding human-technology co-adaptation processes is becoming of utmost importance. Co-adaptation required among various actors is critical for their survival especially in turbulent environments such as the cyberspace. Indeed, cyberspace is marked by imminent cyber threats forcing IT stakeholders to act promptly, re-enforcing cybersecurity with complex and increasingly intrusive technologies with significant social impact. Based on a field study where a governmental organization (GO) acquired cybersecurity systems; and leveraging a constructive grounded theory extended with and abductive research, this study showcases that cybersecurity being as strong as its weakest actor, a requirement for a collective successful co-adaptation amongst various actors is of utmost importance. A technology-human co-adaptation model is proposed. It is processual in nature, with a holistic reach driven inspired by various adaptation dynamics such as power, identity, ethics and technology; that are driving the overall co-adaptation. Knowing what it takes for a better co-adaptation will allow cybersecurity stakeholders, managers and practitioners to bring more focus on pre-adaptation efforts facilitating the co-adaptation processes therefore allowing the acceleration of the much needed success of cybersecurity systems deployments or any other controversial but required technology.

Keywords: Co-Adaptation, Adaptation, Adaptation Dynamics, Cyberspace, Cybersecurity, Surveillance, E-crime, Privacy, Power.

1. Introduction

Adaptation is the prime and general condition of all existence.

Edgar Morin

This paper addresses co-adaptation between human and technological actors in the context of Information Systems (IS) adoption in a Governmental Organisation (GO). While evolution and adaptation have been widely explored in biology, psychology and environment fields, this can't be said for Information Systems (IS). There are nevertheless few notable attempts of examining evolution and adaptation between organizations and technologies based on existing IS theories. For instance Grabowski and Roberts (2011) applied adaptive structuration theory to study co-adaptation between organization and technology; (Richard and Simon 2006) used complex adaptive system theory to explain evolution between software and organization, and (Nima Herman et al. 2016) used the activity theory to address context driven co-evolvement between tools and practices in organizations. While these and other authors (Barley 1986; Giddens 1984; Orlikowski 1992) made significant contributions to understanding the concept of change and interaction between technology and organisations there is a paucity of research that explicitly examines and theorizes the concept of adaptation and co-adaptation among human actors (including organizations) and technologies (Cecez-Kecmanovic et al. 2014; Leonardi and Barley 2010).

While co-adaptation processes are evident in most IS in practice they are particulary critical in turbulent environments such as cyberspace where cyber threats are imminent (Kan 2017; Lohrmann 2016). Cybersecurity counter attacks (Gelbstein 2016) require rapid, profound and integrated technological and organizational changes (Andres 2016; Balleste 2016; Delibasis 2016; Kulesza 2016; Weber and Staiger 2016) that can only be sustained by an effective and ongoing co-adaptation among various involved actors.

Indeed, increasing number of new security threats and e-crimes has been introduced by the ever interconnected digital world showing daily explosion of information and communication technologies (Durbin 2016). These threats relate virtually to every aspect of our life including businesses, critical infrastructures (Kan 2017) and national security. Cyberattacks on power grids and other significant infrastructure made headlines in 2016 (Lohrmann 2016). According to CNBC, an IBM study found that ransomware spiked 6,000% in 2016 and most victims paid the hackers; 70 percent of business victims paid the hackers to get their data back and ransomware reached almost $1 billion in 2016 (Taylor 2016). Attacks in 2017 affected both private and government organizations. The examples include attacks on railways systems in Germany, NHS systems in the UK and USA's 198 millions voters data leaked from Amazon servers (Newman 2017). Faced with imminent threats and risks becoming higher every day, many organizations are being urged to adopt cybersecurity tools (Adelstein 2006; Hay et al. 2009). So much so that cybersecurity has become the focus of most governments (Belot 2017).

This paper aims to advance understanding of co-adaptation processes among technological and social actors in the context of cybersecurity by drawing on and extending concepts and theories of adaptation from biology and environment studies. This is important for all kinds of organizations but in particular for government organizations. This aim is achieved by i) presenting empirical findings and analysis from the longitudinal case study of the adoption of cybersecurity technologies in a government organization; ii) developing a grounded theory in the form of a model of co-adaptation among cybersecurity systems and various social actors (individuals, groups and the organization); and iii) dicussing its contribution and future research.

2. Literature review

Adaptation as defined by the English dictionary (http://www.thefreedictionary.com/adaptation) means: a. the act or process of adapting, or b. the state of being adapted, or c. something, such as a device or

mechanism that is changed or changes so as to become suitable to a new or special application or situation. The field of origin of adaptation is biology where adaptation is a process by which an animal or plant species becomes fitted to its environment (Gittleman 2017). Henri Laborit introduced the idea that, if a being lives and reproduces, it is because it has adjusted its biological functions to its external conditions (Simonet 2010). Adaptation was also widely studied in climate change and psychology sciences (Hoffmann 2011; Maner and Kenrick 2010; Pelling 2011; Wilson et al. 2008).

In the IS literature, there were attempts to theorize mutual influences between an IS and its organizing context which addressed adaptation in an indirect or incomplete manner (Grabowski and Roberts 2011; Richard and Simon 2006; Vessey and Ward 2013). Furthermore, the evolutionary theory has been used to study organization survival by continuously adapting technology (Ahire 2000; Anderson and Tushman 1990; Arnott 2004; Cragg and King 1993; Piccoli et al. 2004). However these studies have been critiqued for one-sided theorizing of technology adaptation while not considering changes made by human actors to adapt to technology (Helin et al. 2014b). Other theories such as the structuration theory of technology (Giddens 1984; Orlikowski 1992), technology imperative models (Markus and Robey 1988), the strategic choice model (Child 1997), and the model of technology-triggered structural change (Barley 1986) focused with various degrees on interactions between human agents, technology and structures. They attempted to explain how technology shapes and is shaped by institutions and the role of human agent in this process. While adaptation was implicitly addressed by studying changes to structures and technology, what was kept silent in these theories is the co-adaptation and co-evolution that human and nonhuman actors go through during these interactions. In other words, the central process of co-adaptation contextually linking, constructing, transforming and deconstructing various human and technological actors wasn't explicitly addressed.

The understanding of the co-adaptation processes is particularly critical in the case of rapidly changing environments characterized by shocks and turbulences that are threatening the very existence of organisations and institutions. For IS, cybersecurity threats are a paradigmatic example. Organizations need to be continuously on alert in order to protect IT infrastructure, minimize cyberattacks risks and counter attacking daily renewed threats. According to Gartner: "Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries" (Walls et al. 2013). Example of such cybersecurity tools are security information and events management technologies such as HPE ArcSight, IBM's QRadar, Intel Security McAfee Enterprise Security, EventTracker and BlackStratus's LOGStorm (Mello Jr 2016).

The implementation and use of such cybersecurity tools and systems have been studied in IS from a technical perspective (Cohen et al. 2011; Gelbstein 2016; Hunton 2009; Turner 2007). It has also been studied from the social perspective focusing on intrusiveness, surveillance and power disruption (Andres 2016; Balleste 2016; Coudert 2010; D'Arcy et al. 2009; Delibasis 2016; Weber and Staiger 2016). The importance of addressing the human factor in cybersecurity has been increasingly acknowledged. "No matter how advanced technology seems to get or how many cyberthreats emerge, it all comes down to people—real, individual people" (O'Rourke 2017). Tanium in its report showed that 91% of existing executive employees still lacking basic knowledge on how to read and interpret cybersecurity reports (Olver 2016). The same report gives some alarming figures illustrating that cybersecurity is not being well handled within organisations. These problems were identified in both cybersecurity awareness and in cybersecurity readiness folds.

Although these studies reveal numerous technological and human/social aspects of the implementation and use of cybersecurity systems they have not addresses the mutual adaptation of the social and the technological. In the digital world with increasing frequency, sophistication and ruthlessness of cyberattacks it is not only cybersecurity technology that must continuously advance but the whole technology-organization complex has to continuously co-adapt to prevent and counteract the attacks. There is a gap in the IS literature in understanding these complex processes of co-adaptation between various heterogeneous (human, social and technological) actors. To address it this paper seeks to answer the following research question: how do human and technological actors change and co-adapt in turbulent and complex environments? The question is answered by drawing from a longitudinal

case study of the adoption of cybersecurity systems in a government organization using grounded theory methodology that is discussed next.

3. Research site and methodology

To explore co-adaptation between human/social actors and technology and answer the research question we chose the case of cybersecurity systems that was introduced by the Cybersecurity Centre of a Middle-Eastern African country to provide cybersecurity of all governmental digital infrastructures. Initially, in 2010 cybersecurity systems operated within the Ministry of New Technologies and then in 2013 transferred to the Ministry of Defence. The creation of the Cybersecurity Centre at a national level and implementation of cybersecurity systems resulted from a cybersecurity partnership with an industrialized country that had already its equivalent centre in operational mode. Cybersecurity systems were deployed and gradually integrated with all governmental IT infrastructures in order to provide comprehensive cybersecurity protection. The project went through major phases since its inception in 2010 and was still running after the end of this research in 2014 (Figure 1).

The Ministry of New Technologies consisted of several departments, including the Department of Digital Trust and the IS Department. Under the Department of IS, the IS Division comprised several IS services: Network and Security Service, Assets Management Service, Governance and Regulation Service, and Software Development Service. The GO witnessed several changes and adaptation to its structure and roles throughout the project of cybersecurity systems acquisition, implementation and use.

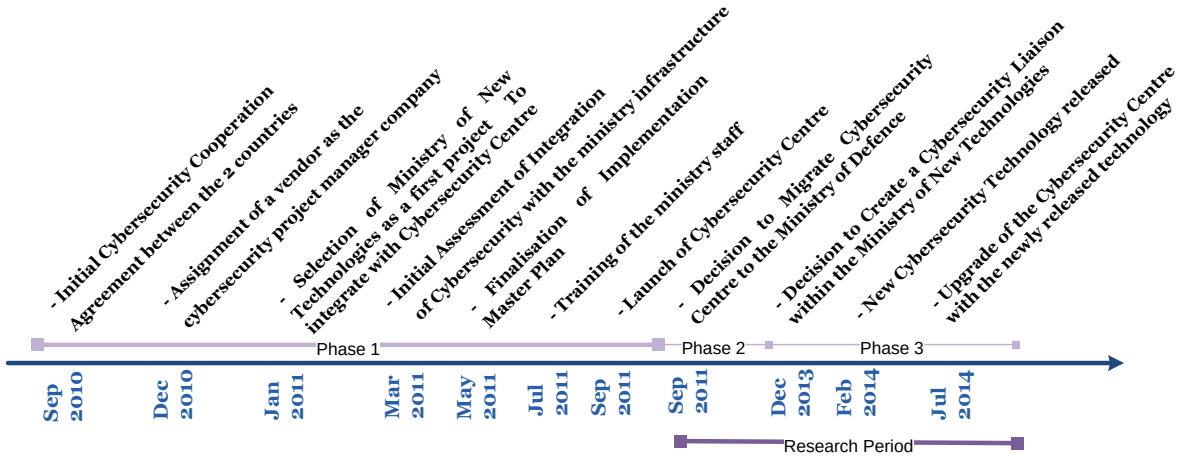

Figure 1: Historical Overview of the Cybersecurity Project

Phase 1 consisted of the initial cybersecurity systems acquisition and implementation lead by the Department of Digital Trust. When cybersecurity systems were implemented it was agreed that it will be the responsibility of the Department of IS and integrated with existing IT infrastructure. In particular, the Network and Security Service team was responsible of its integration with the entire IT infrastructure managed by the Ministry of New Technologies. As part of this implementation the Department of IS worked closely with one main security vendor which provided the appropriate training to its staff.

Phase 2 was marked by the migration of the Cybersecurity Centre to the Ministry of Defence. For this purpose a new unit, The Department of National Information Security has been created along with its appropriate divisions. As part of this Department, the Cybersecurity Division was responsible for the operation of the Cybersecurity Centre and the relationship with the cybersecurity vendors. In some sense, this phase can be seen as an attempt to increase security awareness and strategic importance of cybersecurity systems by granting the ownership of the Cybersecurity Centre and the responsibility for the cybersecurity project to the Ministry of Defence.

Phase 3 involved complex organizational change in GO (in particular in the Ministry of New Technologies and the Ministry of Defence) as a result of the changing responsibility for cybersecurity and specifically cybersecurity systems. There was also a release of a new cybersecurity technology that had to be implemented. In order to facilitate the communication between the two ministries and the migration of the cybersecurity systems in 2014 a new unit was created under the Department of Digital Trust. The key role of the new unit was to liaise between the two ministries – facilitate knowledge sharing and transfer of knowhow and experience. In addition a new vendor was hired to implement newly released cybersecurity systems and tools.

As part of a security team in the Cybersecurity Centre, the author spent sixteen months (from May 2013 to September 2014 in the field as a full participant. This allowed him to conduct an in-depth longitudinal case study: observe first-hand what was going on in the GO, engage with staff in work processes and informal conversations, observe changes going on in different departments, review documents (including archived records and reviews), inspect the technology (cybersecurity systems) and its performance, and formally interviewing members from different units. 30 in-depth formal interviews were conducted with 17 key actors: 9 project participants, 5 senior managers and 3 middle managers (13 of them are interviewed twice). They represented the majority of the key actors in the project. Notes from observations, informal discussions and documents comprise 11000 words. Thanks to access to important actors, technology and documentation from multiple sources the data collected are extensive and rich.

Data analysis followed Grounded Theory approach by Charmaz (GT) (Charmaz 2014). The analysis of data started during the field study and in turn informed data collection, especially interviews. Interviews were in-depth and unstructured to allowed new ideas and themes to flow and questions to emerge in relation to new categories and themes. After the completion of data collection, the analysis of data continued first through open-coding using qualitative analysis software NVivo. The analysis and comparison of open codes lead to formulation of categories and then to identification central themes. Relationships among the codes were recorded in memos and later used during theory building (Charmaz 2014; Corbin 2015; Glaser and Strauss 1967). Furthermore, potential relationships were hypothesised along the way and tested against collected data following an abduction process (or in other words, seeking 'inference to the best explanation') (Bryman 2015; Douven 2011). The abductive reasoning also engaged theories that could help explain the complex changes of organization structure, power relations, work practices, professional identities, technological changes and their ongoing mutual influences. In this sense, theory development was in the final stage informed by evolutionary theory and the concept of co-adaptation. Seeing the observed complex processes of cybersecurity systems implementation in GO as processes of adaptation and co-adaptation turned out to be the best explanation.

4. Findings and Analysis:

Resulting from the GT analysis (Charmaz 2014), the story of cybersecurity systems implementation during the 3 phases, is presented as a series of events (round shapes) and experiences (square shapes) summarized in Figure 2. Arrows illustrate their interconnections. Both events and experiences are colour coded to indicate which phase they pertain to. Also, interconnections are numbered from 1 to 3 indicating the respective phase.

The following analysis briefly describes adaptation dynamics including co-adaptation processes in which various human and technology actors act and thus change the situational context. The changes in the situational context prompt adaptation dynamics of different actors and so on. Due to space limitation we present here only illustrative examples of these co-adaptation processes.

During all phases, there was shared awareness by all human actors of the cyber threats and the agreement on the enforcement of cybersecurity as well as the need for collaboration between all involved actors. In phase 1 managers of the Ministry of New Technologies were particularly concerned with cyber threats as they held direct responsibility for cyber protection of the GO. The implementation of cybersecurity systems was considered of highest importance and critical to

cybersecurity as one of the managers explained: "It is very important and we needed it especially with all what we hear about from security breaches, high hackers' activities and the risk they are presenting... Imagine the government infrastructure has been attacked and confidential information has been stolen, the consequences could be immeasurable on both material and immaterial levels. So, definitely a Centre to monitor all activities in order to protect and detect is a very good idea" (Senior Manager #3). This was indicated on the diagram by the category of "Criticality of Cybersecurity and Necessity of Cooperation" that was relevant across all phases.

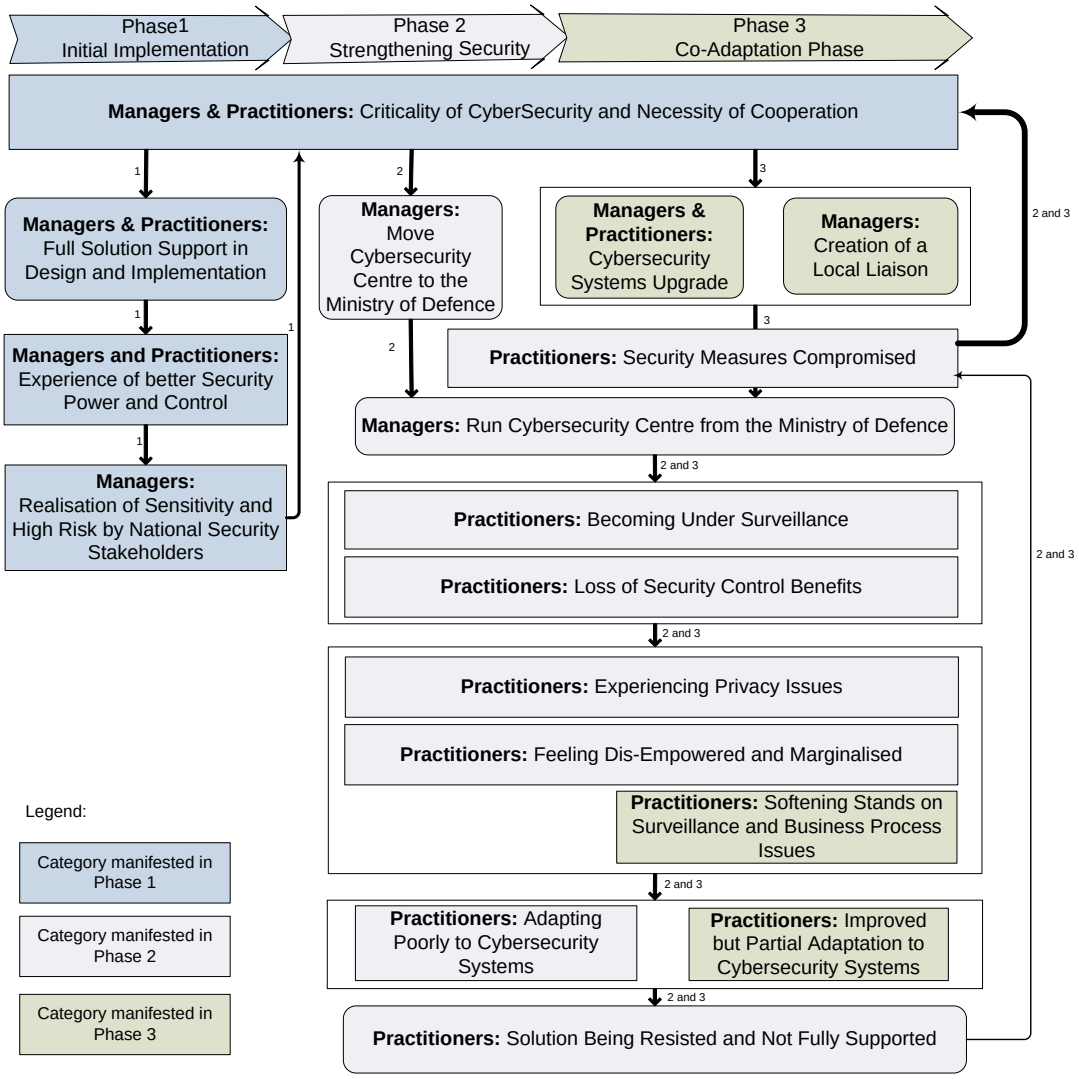

Figure 2: Co-Adaptation View of the Processes Involved in three Phases (developed using GT)

During phase 1, cybersecurity systems were implemented by a third party vendor with a full cooperation of the Ministry of New Technologies security team members. The security team was excited and was looking forward to operating the new system. The IT team collaborated with all the actors related to cybersecurity systems and also undertook the required trainings. "It was very exciting (experience) as we were able to access the server dashboard and we were able to run different reports and monitor traffic ourselves. It is our environment and we are responsible of making it as secure as possible, any tools that could help us detect threats and attacks and protect our IT assets were very welcome. We really needed a comprehensive tool that allows us viewing what is being exchanged on our network and cybersecurity solution sounds as the perfect answer to this…" (Middle Manager #1). This could be explained by that they were already adapted to security tasks and roles. This means that we witnessed the introduction of technologies into a structure that is pre-adapted to the nature of threats these technologies addressed. It is important to note that power structures haven't been affected

at that time; teams' identities haven't been influenced and hence no major change or adaptation was required by any of the actors. One fact has changed though, it is the level of power and control that the security team had and that was strongly increased by the ownership of cybersecurity solution centre.

In Phase 1, the security team had then a greater power and control that allowed access to GO's private and confidential data. Moreover, this access could be broadened beyond the particular GO the security team reports to when cybersecurity systems would be integrated with subsequent GOs of the country. The National Security Committee felt that there was a security risk regarding the initial setup of cybersecurity systems project and wanted a stricter control of it. It decided to revoke the ownership of Cybersecurity Centre by the Ministry of New Technologies and grant it instead to a military of Ministry of Defence. This marked the start of a new phase of the adaptation process in the project that is indicated in the diagram above as "Phase 2: Strengthening Security". We can describe this structural change as an adaptation process in response to the assessment of cyber risk by the National Security Committee. By adapting to this risk, the National Security Committee acted upon the actual situational context of the project which is shared by various other human and technology actors. Indeed, the change to the situational context is described by the 2 categories: "Move Cybersecurity Centre to the Defence Ministry" and "Run Cybersecurity Centre from the Defence Ministry". This made the IT team in particular to be under watch as showed by the category "Becoming Under Surveillance". This was a real concern as an IT team member explained: "I'm not comfortable having or knowing that someone is watching or listening to every single action I do. I like my privacy".

Furthermore, it made not only the security team lose the benefits of Cybersecurity Centre but added a parallel entity (Cybersecurity Centre at Ministry of Defence) sharing the security responsibility of the Ministry of New Technologies and intervening in the security team role. This had implications for the security team as expressed by staff member: "We don't identify ourselves as the main security team anymore; all teams receive cybersecurity systems reports and think they report to cybersecurity systems regarding security tasks...Security decisions were made by us for us, now a third party got involved and taking over this" (Security Practitioner #1). This created new reality on the ground that modified the context in which teams in the Ministry of New Technologies were working. The enacted changes to this context triggered several adaptation processes related to various actors namely the security team and IT team. It made them engaged in several adaptation dynamics of both the social and technical nature. The categories "Experiencing Privacy Issues" and "Feeling Dis-empowered and Marginalized" reflects these dynamics. As employees in the Ministry of New Technologies (especially the IT team and security team) felt being under surveillance, they expressed increasing awareness of being watched and concerns of being exposed and embarrassed. In particular Manager #7 explained, with cybersecurity systems in place, professional mistakes would be known to everyone, inside and outside the Ministry of New Technologies: "…before, if there is an incident, it could be hidden; now it is not the case as everyone will know about it. Before, it could be hidden even at the lowest of the hierarchy and sometimes even the immediate manager will not know about it". The IT team was also asked to deal with technical issues that cybersecurity systems detected, but felt powerless since it was impossible to fix some of them "we can't (comply with cybersecurity systems) because it means we have to start new projects for upgrades and we can't do that… the people who used to work on this applications are already gone. We only do maintenance of these applications. Some of them are so old we won't be able find the proper people to upgrade them" explained a System Administrator #5.

Moreover, the security team experienced a mixture of dynamics, those that are related to their roles and identities while being responsible for security within the Ministry of New Technologies and those that are related to being controlled and watched by an entity outside of the Ministry. They were subject to role change and experienced secrecy and mistrust from some actors: "Unfortunately once the solution was put in place and ownership was passed to the Ministry of Defence, our access to the dashboard was blocked. We couldn't even have web interface to monitor our own traffic or even know what is being watched about us" said Senior Manager #3. This deprived local practitioner from monitoring rights at local traffic of their network. Some security practitioners also felt that their role and career objective became misaligned "it reduced our jobs to execution of instructions. For me, the most interesting part of my job was the daily challenges, the meetings, brainstorming and the solution

design…Now all the fun is gone; all we do is get to the reports and try to execute instructions." security practitioner #5 explained. What made things even worse was that the communication from the Cybersecurity Centre to the Ministry of New Technologies was unilateral and that their security teams weren't coordinating security tasks with each other.

The analysis at this stage suggests that various actors were engaged in several social and technical dynamics that relate mainly to trust, roles and responsibilities, power/resistance, identity, technology and ethics. These adaptation dynamics drove the adaptation of each actor or the co-adaptation of all of them. The adaptation of the Ministry of New Technologies practitioners to the cybersecurity systems project setup was poor. The level of communication and cooperation with Cybersecurity Centre was very low as explained by Senior. Manager #3: "It is easier to interact with civilians even at the governmental level. The military follows strict rules. They are very rigid and communication with them is almost impossible. Errors are not tolerated". There were many dis-coordination issues and rejection of responsibility. Role confusion and competition between the Ministry of New Technologies' security team and Cybersecurity Centre left many security tasks compromised. The power of the Ministry of New Technologies and especially its security team had diminished and their role of enforcement and control; along with its image within the GO; have been undermined. This was illustrated in the diagram by the category "Adapting Poorly to cybersecurity systems". The outcome of this poor adaptation got manifested in several signs of resistance among practitioners ending up in not supporting the cybersecurity systems solution. "I tried to get them (members of my team) involved in discussing the cybersecurity systems reports on many occasions, the attitude is very negative. They don't want to talk about it" mentioned Senior Manager #6 who manages several IT practitioners not involved in cybersecurity systems project. The categories "Solution Being Resisted and Not Fully Supported" and "Security Measures Compromised" illustrate this outcome in the diagram.

The outcome of this poor adaptation and resistance affected the situational context of the project and got the attention of management of the Department of Digital Trust that were keen to making the project a success and ultimately defend the Ministry of New Technologies and promote cybersecurity systems experience. In phase 3, the social and technical problems that the Ministry of New Technologies practitioners were facing and their actions/inactions were noted by management of the Department of Digital Trust. As a result more adaptation dynamics took place between several actors of the project. Practitioners have realized that technology was an issue and they had to adapt to it. Mangers on the other hand realised they had to adapt the technology. Therefore they've decided along with Ministry of Defence to enforce cybersecurity systems with newer and more powerful technologies that would be easier to use. Thus new cybersecurity systems tools were acquired, sensors and points of integration with the Ministry of New Technologies infrastructure became easier to manage by the IT team primarily because they became software based. Generated cybersecurity systems reports became more targeted, addressing more precisely and specifically the applications being ran by the Ministry of New Technologies. Time to perform security task was improved due to unprecedented storage capacity and events reconstruction time.

Beside this technical adaptation, there was an organizational adaptation. Management realized the tasks miss-coordination and communication issues between cybersecurity systems and the Ministry of New Technologies. They've then decided to create a new entity within the Ministry to play the role of a Liaison between Cybersecurity Centre and the Ministry. This organizational adaptation tried to control the flaws of communication and coordination between them. However for the practitioners in the Ministry it only increased the complexity of communication since there was a new actor involved that was in the Ministry but didn't belong to the IT team. "The Department of IS is not happy about the Department of Digital Economy. The latter is supposed to be at the same level in the hierarchy; however the Department of Digital Economy is now driving the show (regarding cybersecurity systems) … and now electing a liaison among its facility to oversee cybersecurity systems operations..." said Senior Manager #1 from the Department of IS. Again by trying to adapt to previously affected situational context, management of the Ministry of New Technologies took actions related to both technical and organizational aspects, thus affecting the situational context of relevance to other players. Mainly the security and IT practitioners within Ministry of New Technologies had now to

assess and attempt to adapt to new context. The actions of management are illustrated in the diagram by the 2 categories: "Creation of a Local Liaison" and "cybersecurity systems technology Upgrade".

Regardless of these changes by management, the practitioners of the Ministry of New Technologies were still involved in previous adaptation dynamics as described in Phase 2. These changes solved neither the issues their security team experienced regarding their role and identity as a team, nor the issues of the control and power that has been shifted by the restructuring of the Cybersecurity Centre. Likewise privacy issues were still persistent and the new changes didn't solve them. However they've assisted few employees to change their minds, soften their opinions and making them adapt to the new cybersecurity systems context. They've been more willing to accept the situation and to do what was needed to assist with the project. Other members of the security team facing this situation couldn't adapt and preferred to leave the team, thus ending their roles of security specialists in the Ministry of New Technologies. In addition, several technical difficulties were still encountered preventing full security compliance. Simply speaking, some technologies were too old and couldn't be adapted to new requirements. This was captured in the diagram by the category "Improved but partial adaptation to cybersecurity systems".

In sum, in this last phase, the co-adaptation between technology, management and practitioners became more pronounced and clear. Co-adaptation of practitioners reached breaking points when few practitioners couldn't adapt and left the organization or their team. But in few other cases, practitioners changed their stands on moral issues especially regarding privacy and co-adapted by deciding to support the project. Technology was adapted to deal with various technical limitations and challenges; the same applies to the Ministry of New Technologies organization structure that was modified to deal with coordination and communication issues. These two actions reflect management co-adaptation process to technology and to practitioners. It also reflects technology co-adaptation to organizational and practitioners issues. The overall co-adaptation was still weak and the Ministry of New Technologies security was still compromised.

To summarize this analysis, during the cybersecurity systems acquisition, implementation and use there were numerous actors involved. The contextual situation of the project makes actors engage in co-adaptation process. Each actor is subject to project situational context and tries to adapt to the changes enacted by the other actors in the context by taking certain actions. This co-adaptation process is driven by adaptation dynamics of the social and technological nature. Social dynamics identified involve power, ethics, identity and technologies. The process is an ongoing and continuous one regardless of the adaptation phase. Thus, from this analysis and while focusing on the main concept of adaptation of different human and technology actors, we could notice that these high level categories relate to either situational context, adaptation process, adaptation dynamics and actors' actions.

5. Discussion

The case of cybersecurity systems acquisition, implementation and use presents an example of co-adaptation of human and technological actors in a turbulent and complex environment. As evidenced from our analysis above, actors act upon the situational context. The situational context changes in turn trigger adaptation dynamics of different actors. These dynamics lead to a certain degree of adaptation of affected actors; adaptation of actors itself is reflected back to the situational context either assisting or impeding the accomplishment and success of the project and so on. Extending the GT analysis and theorizing by an abductive theory building led to a new co-adaptation model. As a result, the presentation of co-adaptation processes in the concrete case of the GO acquisition, appropriation and use of cybersecurity systems in Figure 2 is generalized further and presented in Figure 3 below. Figure 3 presents the co-adaptation processes among the main actors – cybersecurity systems, managers, and practitioners – in the situational context. As these actors continually change and co-adapt as part of situation context, the adaptation dynamics involves power reconfiguration, identity changes, technology (IT infrastructure) changes, and ethical concerns and responses (only briefly analysed above due to space limitations).

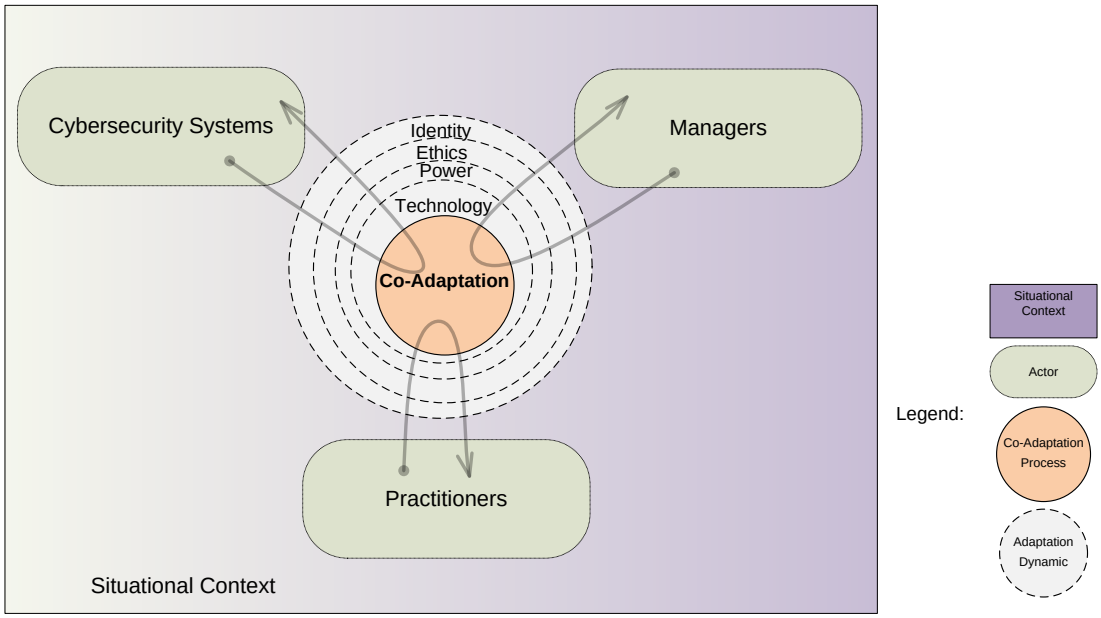

Figure 3: Human/Technology Co-Adaptation Model

This represents a new process model of human-technology co-adaptation. It is defined as the survival process of human actors offering the ability to adjust to challenging situational contexts by using and adapting technology, the process by which various actors (human and nonhuman) of cybersecurity systems engage in its constitution but also in reconstitution of social structures by introducing new sociomaterial realities. This new model helps to explain the mutual co-constitution between cybersecurity systems and human actors within the social and technical context through co-adaptation dynamics. It helps us demonstrate how the cybersecurity systems implementation, use and adaptation draw from, and impact on, social relations by generating various social and technical adaptation dynamics in the organization continuously fuelling actors' co-adaptation.

Unlike extent adaptation and evolution theories, the co-adaptation process introduced here is multidirectional. Adaptation is not a change of an actor to fit an environment; nor are forces exercised upon an actor a natural selection process according to the Darwinian account (Bock 1980). Instead, it is a co-adaptation process that involves multiple actors adjusting to each other in their complex and uncertain context. In other words each actor is part of other actors' environments; and change might take place in all involved actors as an outcome of this co-adaptation process. Natural selection process is not applicable as co-adaptation here is a result of all actors exerting forces upon each other during the adaptation dynamics.

This process model hence presents distinct dynamics driving co-adaptation between technology, practitioners and managers and ultimately organizations. Each of these actors is adapting to changing situational context and is also part of the adaptation dynamics driving other actors' adaptations and so on. Adaptation is a process of becoming of each actor (human or technological) that ensures survivability in a given situation. The becoming of each actor is different depending on the nature of the actor and its capacity to cange and adapt.

In case of technology actors, adaptation aims for viability of an actor. Adaptation is fuelled and driven by various adaptation dynamics of other actors as part of the situational context. An actor adaptation to the situational context is influenced by adaptation dynamics created either accidently or intentionally as tactics or a strategy belonging to the same actor or different actors.

Actors in the becoming are part of these contexts. Situational Context could also be seen as a set of social and material (technological) actors that could constitute an intake of adaptation dynamics or be part of the outcome of the adaptation driven by these dynamics or both. Adaptation assumes modification and change. It is driven and enacted by actors, but conditioned and limtied by situational context. It is in-line with process thinking as it explains actors (or entities) in terms of recurring

interactions of events dynamics (Cecez-Kecmanovic 2016). It is a continuous, open ended process, sustaining survival or viability of actors. The adaptation trajectory or path can be of outmost historical value in studying the archaeology of experiences making adaptation also as an explanation and necessity for evolution (Maner and Kenrick 2010).

We define an actor adaptation dynamics as the forces or the energy aiming to guarantee the actor's survival by producing change in the actor's becoming or situational context or both. The actor's situational context includes all actors with wich it is connected or by which it is influenced. These dynamics relate to various social concepts such as: power, resistance, ethics, agency, knowledge, actions, discourses, partnerships, memberships, associations, subjectivation, control, discipline, strategies, tactics, and politics. They are relational by nature. They are subject to interpretation and intentions and do overlap and co-construct each-others. In the case of cybersecurity systems, main social dynamics identified related to power, identity, technology and ethics where negotiations of these dynamics took place between several groups and individuals.

An actor's adaptation situational context is subject to simultaneous influences from different adaptation dynamics belonging to actors of various natures. These influences can collide, compete or synergize. Situational context is influenced when the outcome of these dynamics is concretized or enacted making the situational context sociomaterial in nature. Concretization of the change doesn't mean necessarily it has been formalized or institutionalized; it can be of an informal nature (workarounds, informal role playing, informal teaming, values pretention…etc.). Likewise, situational context change can be undeclared which could be captured by the politics dynamics. In the cybersecurity project, the double stand of some middle managers is one example. They they sided up formaly with senior managers; but informaly with practitioners resisting the implementation.

Adaptation type depends on the type of the actor. We can differentiate between 2 distinct types for adaptation: technology adaptation and human adaptation. Technology adaptation is the process of technology modification by an individual or group of individuals in order to achieve some goals (e.g. desirable funcitonality). Human adaptation is self-driven as individuals or groups face all kind of challenges and make several adjustments to their behaviour and take actions while being engaged in several dynamics (adaptation dynamics) at the same time seeking to attain their own goals. This would mean sustaining the survival of the actor (an individual) or a group it identifies as. Human adaptation can involve one or more technology adaptations. In order to adapt to a certain situation, an actor will adapt one or more technology tools to assist him/her with this adaptation. In a bigger scheme, technology adaptations serve human adaptations. Technology adaptation ensures the actor's viability in performing the desired functions and providing reasons for its appreciation and retention by actors that are its stakeholders (individuals or group of individuals).

A human actor is constantly engaged in a set of networks of adaptation dynamics. This engagement requires constant negotiation within the actor himself and with other actors as well (Emirbayer 1997). An example of self-negotiation is the questioning of one's values and ethics and the possibility of giving up ground on certain believes or principles or the opposite by taking a harsher stand on certain believes and values or may be even adopting new ones. This constitutes the moral and ethics adaptation dynamics. When this self-negotiation ends up with a change in the actor's believes and moral, this could affect his/her overall adaptation process making the actor adapted to new context and ultimately assuring his/her survival. This was the case when few employees changed their view on privacy invasion by cybersecurity systems.

Similar to moral and ethics adaptation dynamics, agency adaptation dynamics involved negotiation with other actors and can lead to new agency stand for example. Going through agency dynamics in an organization, an actor can accept new role he/she will be playing in the organization structure in order to satisfy goals of different actors (for instance, becoming a security proxy of the cybersecurity centre in the Ministry of New Technologies). Likewise, the change in agency stand affects the actor's whole adaptation process in a way that could ensure the actor's survival. The way these two types of adaptation dynamics co-affect the adaptation process of the actor differs depending on whether the dynamics overlap, collide or synergize. In other terms, these dynamics co-construct each other. As an

example, the ethics and moral dynamics can prevent the agency dynamics from reaching a certain outcome. Likewise, changes in ethics and moral dynamics can get rid of a deadlock in the agency dynamics and together generate a positive adaptation outcome. What was said about moral and ethics and agency dynamics can be said about all sorts of adaptation dynamics. It is a certain co-construction of these dynamics along with the corresponding unfolding timing of it that will lead to a better adaptation or not.

Technology adaptation is the change of technology in order to include and/or exclude certain features to be used in a certain manner with an expected performance in order to accommodate the requirements of human actors in a particular context. Human actors have power over technology but the opposite is true as well. These changes to technology is can be seen as tactics used by human actors in order to ensure their own adaptation to their context. If outcome is achieved more or less as expected, the human actors would apprehend that their survivability was sustained by relying among other factors on technology. On the other side, adaptation of technology in such manner to assist human actors to survive justifies and demonstrates the role it plays as an actor and hence sustains its viability and retention. During cybersecurity systems project, technology has been upgraded and new tools acquired and put to use, making the overall integration more complex.

The power that technology has over human actors is can be seen as offering them allowances and opportunities to better engage in social experiences, and also presenting them with specific constraints. Technology has specific instructions to be followed during its operations and has limitations on what it can do, when it can do it and how it will do it. The scope reach of technology and the time required to fulfil such reach represents its limitations and at the same time limitations to human actors depending on it as well. However technology doesn't have goals of its own. The power it has over human actors making them doing things in a certain way it is either a reflection of power of different human actors who have designed, configured and implemented this technology in a specific and strategic manner in order to satisfy their goals and preferences (Foucault 1981), or this power is accidently and inevitably presented by the technology due to its intrinsic technical nature requiring certain ways of operations and careful dealing with random and unpredictable technical faults if and when they happen.

Exactly as adaptation to climate change, in the example of cybersecurity, actors' adaptations are interdependent. Indeed, cybersecurity is a collective matter and it is as strong as its weakest actor, it is only with successful negotiations among various social adaptation dynamics that a successful adaptation of each actor would take place allowing successful deployment of the solutions. In fact, co-adaptation is a collective process. Organization adaptation success depends on how each and every individual actor adapts. It needs to be said that even though these adaptations are affecting each other, every actor's adaptation to situational context is distinct and subject to local interpretation (Cecez-Kecmanovic 2004). On the other hand, even if some actors' adaptation is successful, a failed adaptation of an actor who is critical can lead to a series of failed adaptations. As an example, technology being an actor, failure of legacy technology to be adapted and integrated with cybersecurity systems posed high risk to the whole project and could be seen as jeopardising practitioners, managers and the GO adaptation to hostile cyberspace. From the theoretical model, failure of an actor adaptation means a change in the situational context of related actors whereby they can or cannot adapt to such a change.

Nonadaptation of an actor might lead to its end. In the case where the new role didn't align with a practitioner' career goal, the practitioner couldn't accept the role reduction and the adaptation was just impossible and has led to the end of this actor.

Adaptation outcome depends on the level of adaptability of the actor and the time taken by this adaptation process. Some adaptations take a longer time and might just happen too late to ensure survivability, for instance when one of the Ministry of New Technologies service team decided to improve communication with cybersecurity centre but after key practitioners who've complained about the communication problems have already left the organisation. This leads us to talk about adaptation timing and sequence of a certain set of adaptation dynamics with a certain set of interpretations by various actors, and a certain set of actions executed in certain intended and

unintended ways by various actors combined with the context of a particular situation. Adaptation constitutes timing and at the same time is subject to timing. Good timing leads to good adaptation and the opposite is true. Timing of unfolding of these influences marks the outcome of these influences on the situational context.

Finally, co-adaptation becomes more relevant and critical when there is an unfavourable situational context threatening the existence of the actors. When situational context is favourable, there is no need for adaptation. That was the case where the Security team in the Ministry of New Technologies was granted the security tool. We can also read it in that case that the actor is already adapted or pre-adapted to the situation which leads us to include the concept of pre-adaptation to this discussion.

6. Conclusion

While adaptation was addressed in several disciplines such as biology and climate studies, the same couldn't be said for IS. Adaptation and co-adaptation of the human/social and the technological in IS was implicitly acknowledged but lacked explicit theorizing and conceptualization. This study makes a contribution to IS literature by theorizing the processes by which human and technological actors change and co-adapt in turbulent and complex environments. Based on the longitudinal case study of the deployment, implementation and use of cybersecurity systems in a Government Organization, this paper first demonstrates the existence of several adaptation dynamics that drive the overall co-adaptation. These dynamics relate to power dynamics between different involved cybersecurity stakeholders; to identity dynamics taking place within the local security team; to ethical dynamics triggered by the invasive nature of cybersecurity technologies; and to technology dynamics posed by technical requirements of cybersecurity technologies and need of integration with existing technologies. Second part of the answer was provided by demonstrating that all actors were continuously involved in these adaptation dynamics and this involvement led to an overall co-adaptation. The proposed holistic theoretical co-adaptation model while focusing on processes such as adaptation and adaptation dynamics. Co-adaptation process is the focal point of this model where all actors linked to their contextual situations are being continuously constructed, transformed or deconstructed.

This paper puts emphasis on the co-adaptation process and demonstrates its central position in the happening and becoming of events and actors while highlighting the role of the evolution and becoming of the context on one hand and resisting dualism advocated by several IS theories on the other (Child 1997; Giddens 1984; Orlikowski 2003). The GT study of cybersecurity systems acquisition, implementation and use in a GO allowed the capture of several concepts related to co-adaptation such as pre-adaptation, adaptation, adaptation dynamics, co-construction of adaptation dynamics, timing within and of adaptations, situational contexts and adaptation sensitivity to contexts, dependencies between adaptations and importance of collective adaptations outcome for an overall co-adaptation success. This model could be used as a theoretical lens to study eco-change in any phenomenon by examining co-adaptation process and adaptation dynamics driving it. From the practical angle, understanding these processes (co-adaptation and adaptation dynamics) will assist in efforts identifying co-adaptation required among various human and technology actors during new adoptions. As a consequence it will also serve pre-adaptation exercise in order to facilitate new rules, structures, technology acceptance, before even its acquisition. This is particularity critical in the case of controversial but required technological acquisition which is very likely to cause undesirable consequences in organisations.

Further research should be undertaken to study adaptation dynamics by identifying their taxonomy and understanding how they overlap, collide and co-construct each other. This should also be extended by focusing furthermore on social adaptation dynamics' build up and inter-actions constituting potentialities and possibilities (Helin et al. 2014a) and how it leads, sometimes by a very fine grained detail, to human actors' mutual action after social negotiations and bargaining (Emirbayer 1997) seeking survival and allowing overall co-adaptation.

References

Adelstein, F. 2006. "Diagnosing Your System without Killing It First " *Communications of the ACM* (Vol 49:No. 2), p. 4.

Ahire, S. G., Garrison;Gupta, Ajay;Terwilliger, Mark. 2000. "Workforce-Constrained Preventive Maintenance Scheduling Using Evolution Strategies," *Decision Sciences* (31:Fall 2000).

Anderson, P., and Tushman, M. L. 1990. "Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change," *Administrative Science Quarterly* (35:4), pp. 604-633.

Andres, R. B. 2016. "National Security and Us Constitutional Rights : The Road to Snowden," *Cybersecurity and human rights in the age of cyberveillance*), pp. 147-167.

Arnott, D. 2004. "Decision Support Systems Evolution: Framework, Case Study and Research Agenda," *European Journal of Information Systems* (13:4), pp. 247-259.

Balleste, R. 2016. "In Harm's Way : Harmonizing Security and Human Rights in the Internet Age," *Cybersecurity and human rights in the age of cyberveillance*), pp. 39-63.

Barley, S. R. 1986. "Technology as an Occasion for Structuring: Evidence from Observations of Ct Scanners and the Social Order of Radiology Departments," *Administrative Science Quarterly* (31:1), pp. 78-108.

Belot, H. 2017. "Cyber Security 'the New Frontier of Warfare, Espionage', Malcolm Turnbull Says," *URL: http://www.abc.net.au/news/2017-01-24/turnbull-declares-cyber-security-the-new-frontier-of-warfare/8207494 / (Visited 21/04/2018*).

Bock, W. J. 1980. "The Definition and Recognition of Biological Adaptation," *American Zoologist* (20:1), pp. 217-227.

Bryman, A. 2015. "Business Research Methods," E. Bell (ed.). Cambridge, United Kingdom

New York, NY, United States of America : Oxford University Press.

Cecez-Kecmanovic, D. 2004. "A Sensemaking Model of Knowledge in Organisations: A Way of Understanding Knowledge Management and the Role of Information Technologies," *Knowledge Management Research & Practice* (2:3), pp. 155-168.

Cecez-Kecmanovic, D. 2016. "From Substantialist to Process Metaphysics – Exploring Shifts in Is Research," *Chapter in Beyond Interpretivism? New Encounters with Technology and Organisation, Introna, L. Kavanagh, D, Kelly, S, Orlikowski, W, Scott, S* ((eds):Springer), pp. 35-57.

Cecez-Kecmanovic, D., Galliers, B., Henfridsson, O., Newell, S., and Vidgen, R. 2014. "The Sociomateriality of Information Systems: Current Status, Future Directions," *MIS Quarterly* (38:3), pp. 809-830.

Charmaz, K. 2014. "Constructing Grounded Theory." London: London : Sage.

Child, J. 1997. "Strategic Choice in the Analysis of Action, Structure, Organizations and Environment: Retrospect and Prospect," *Organization Studies* (18:1), pp. 43-76.

Cohen, M. I., Bilby, D., and Caronni, G. 2011. "Distributed Forensics and Incident Response in the Enterprise," *Digital Investigation* (8, Supplement:0), pp. S101-S110.

Corbin, J. M. 2015. "Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory," A.L. Strauss (ed.). Thousand Oaks, California SAGE.

Coudert, F. 2010. "When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies," *Computer Law and Security Review* (26:4), pp. 377-384.

Cragg, P. B., and King, M. 1993. "Small-Firm Computing: Motivators and Inhibitors," *MIS Quarterly* (17:1), pp. 47-60.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Delibasis, D. 2016. "Cybersecurity and State Responsibility : Identifying a Due Diligence Standard for Prevention of Transboundary Threats," *Cybersecurity and human rights in the age of cyberveillance*), pp. 17-39.

Douven, I. 2011. "Abduction," *Stanford Encyclopedia of Philosophy Archive* (Summer 2017 Edition).

Durbin, S. 2016. "Securing Executive Buy in as the Cyber Security Threat Landscape Expands,").

Emirbayer, M. 1997. "Manifesto for a Relational Sociology," *American Journal of Sociology* (103:2), pp. 281-317.

Foucault, M. 1981. "Foucault (Berten), Un Entretien," *Universite Catholique de Louvain*).

Gelbstein, E. 2016. "Is Audit Basics: Auditing Is/It Risk Management, Part 1," *ISACA Journal* (Volume 2, 2016).

Giddens, A. 1984. "The Constitution of Society : Outline of the Theory of Structuration." Cambridge [Cambridgeshire]: Cambridge Cambridgeshire : Polity Press.

Gittleman, J. L. 2017. "Adaptation," *Encyclopædia Britannica* (URL: https://www.britannica.com/science/adaptation-biology-and-physiology / (Visited 11/04/2018).

Glaser, B. G., and Strauss, A. L. 1967. "The Discovery of Grounded Theory." London: London : Weidenfeld and Nicolson.

Grabowski, M., and Roberts, K. 2011. "High Reliability Virtual Organizations: Co-Adaptive Technology and Organizational Structures in Tsunami Warning Systems," *ACM Trans. Comput.-Hum. Interact.* (18:4), pp. 1-23.

Hay, B., Nance, K., and Bishop, M. 2009. "Live Analysis: Progress and Challenges," *Security & Privacy, IEEE* (7:2), pp. 30-37.

Helin, J., Hernes, T., Hjorth, D., and Holt, R. 2014a. "Process Is How Process Does."

Helin, J., Hernes, T., Hjorth, D., Holt, R., and Linstead, S. 2014b. "Henri Bergson (1859–1941)."

Hoffmann, A. A., & Sgrò, C.,M. 2011. "Climate Change and Evolutionary Adaptation," *Nature* (470: 7335), pp. 479-485.

Hunton, P. 2009. "The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model," *Computer Law & Security Review* (25:6), pp. 528-535.

Kan, M. 2017. "Experts Worried About Ransomware Hitting Critical Infrastructure," *URL: http://www.networkworld.com/article/3169465/security/experts-worried-about-ransomware-hitting-critical-infrastructure.html / (Visited 11/04/2018*).

Kulesza, J. 2016. "Defining Cybersecurity : Critical Infrastructure and Public-Private Partnerships," *Cybersecurity and human rights in the age of cyberveillance*), pp. 1-17.

Leonardi, P. M., and Barley, S. R. 2010. "What's under Construction Here? Social Action, Materiality, and Power in Constructivist Studies of Technology and Organizing " *The Academy of Management Annals* (Vol.4:1), pp. 1-51.

Lohrmann, D. 2016. "The Dark Side of the Force: Hacktivism Takes Center Stage in 2016," *URL: http://www.infosecisland.com/blogview/24866-The-Dark-Side-of-the-Force-Hacktivism-Takes-Center-Stage-in-2016.html / (visited on 02/02/2017*).

Maner, J. K., and Kenrick, D. T. 2010. "When Adaptations Go Awry: Functional and Dysfunctional Aspects of Social Anxiety," *Social Issues and Policy Review* (4:1), pp. 111-142.

Markus, M. L., and Robey, D. 1988. "Information Technology and Organizational Change: Causal Structure in Theory and Research," *Management Science* (34:5), pp. 583-598.

Mello Jr, J. P. 2016. "Gartner Magic Quadrant for Siem 2016: Not Just for Compliance Anymore," *URL: https://techbeacon.com/highlights-gartner-magic-quadrant-siem-2016 / (Visited 18/04/2018*).

Newman, L. H. 2017. "The Biggest Cybersecurity Disasters of 2017 So Far," *URL: https://www.wired.com/story/2017-biggest-hacks-so-far/ / (visited on 18/04/2018*).

Nima Herman, S., Margunn, A., and Faraja, I. 2016. "The Role of Context in the Co-Evolution of Work and Tools: A Case from the Primary Health Sector in Tanzania," *Information Technology & People* (29:4), pp. 850-875.

O'Rourke, M. 2017. "The Impact of Individuals," *Risk Management (00355593)* (64:11), pp. 3-3.

Olver, R. 2016. "The Accountability Gap: Cybersecurity & Building a Culture of Responsibility," *URL: https://www.informationsecuritybuzz.com/study-research/accountability-gap-cybersecurity-building-culture-responsibility/ / (visited 18/04/2018*).

Orlikowski, W. 2003. "The Duality of Technology : Rethinking the Concept of Technology in Organizations," *IDEAS Working Paper Series from RePEc*).

Orlikowski, W. J. 1992. "The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organization Science,").

Pelling, M. 2011. *Adaptation to Climate Change : From Resilience to Transformation*. London

New York: London

New York : Routledge.

Piccoli, G., Brohman, M. K., Watson, R. T., and Parasuraman, A. 2004. "Net-Based Customer Service Systems: Evolution and Revolution in Web Site Functionalities," *Decision Sciences* (35:3), pp. 423-455.

Richard, M. K., and Simon, M. K. 2006. "Interpreting Socio-Technical Co-Evolution: Applying Complex Adaptive Systems to Is Engagement," *Information Technology & People* (19:1), pp. 35-54.

Simonet, G. 2010. "The Concept of Adaptation : Interdisciplinary Scope and Involvement in Climate Change," *Sapiens* (3.1).

Taylor, H. 2016. "Ransomware Spiked 6,000% in 2016 and Most Victims Paid the Hackers, Ibm Finds," *URL: http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html / (visited 02/02/2018*).

Turner, P. 2007. "Applying a Forensic Approach to Incident Response, Network Investigation and System Administration Using Digital Evidence Bags," *Digital Investigation* (4:1), pp. 30-35.

Vessey, I., and Ward, K. 2013. "The Dynamics of Sustainable Is Alignment: The Case for Is Adaptivity," *Journal of the Association for Information Systems* (14:6), pp. 283-311.

Walls, A., Perkins, E., and Weiss, J. 2013. "Definition: Cybersecurity," *URL: https://www.gartner.com/doc/2510116/definition-cybersecurity / (visited on 20/12/2016*).

Weber, R. H., and Staiger, D. N. 2016. "Privacy Vs. Security : Identifying the Challenges in a Global Information Society," *Cybersecurity and human rights in the age of cyberveillance*), pp. 63-85.

Wilson, D. S., Vugt, M. V., and O'Gorman, R. 2008. "Multilevel Selection Theory and Major Evolutionary Transitions:Implications for Psychological Science," *Current Directions in Psychological Science* (17:1), pp. 6-9.