10.31341/jios.45.2.6
Open Access
UDC 001.891:004.738.5:378
Survey Paper

A Framework of Social Networks Control in Higher Educational Contexts

Maria Jakovljevic *mariaj@flamewave.net*
Science and Technology Education
University of South Africa, Pretoria, South Africa

Nkopodi Nkopodi *nkopon@unisa.ac.za*
Science and Technology Education
University of South Africa, Pretoria, South Africa

Abstract

Educationists are urged to investigate the effect of social networks control. There is a lack of multidisciplinary studies with a focus on coercive social network control in the higher education sector. This exploratory and descriptive study presents a theoretical contemplation of social network control based on ten key elements that influence teaching and learning in higher education environments.

The paper provides a critical analysis of the impact of an economic model on social networks control and examines social engineering through the tenets of digital presence, psychological strategies and tactics. Insights into user-generated content and the learning process of manipulative assimilation that influence current ways of thinking in higher education contexts are offered through the lens of social networks control mechanisms. A framework for social network control was derived, signifying the flow and dynamics between key elements which might impact on various aspects of social network security and its applications in Higher Education.

Keywords: social networks, security, cyber control mechanisms, social engineering, Higher Education, UGC, digital inclusion

1. Introduction

According to research findings, there is not an appropriate foundation for social networks security in general [3, 54, 85] owing to the absence of a suitable awareness and appropriate defence infrastructure [53]. Social networks are teams of people informally bound together by shared expertise and passion for a joint enterprise [9, 32]. They are platforms for solving problems in that they share knowledge and collaborate [7, 23].

There is an insufficient application of cyber control mechanisms [40, 68] and a lack of cognisance of methods, techniques and tools for social networks control. This may be attributed to powerless educational policies and authorities [38, 43, 69] an inadequacy of training in higher education [61]; and a misunderstanding of the

underlying basic economics principles and their application in education [17]. Moreover, this may be ascribed to a lack of understanding economy and digital economy [71, 83] as a basis for any human endeavour in society. A model of economics with its three levels of economy and its impact on education has not been taught explicitly. Digital economy is the tendency of most organisations to exclusively use digital information in globally connected systems [71, 83].

There is a lack of studies that present an insight into the underlying issues of social networks control. The researchers Gronke and Cook [41] examined trust in online news, Turcotte, York and Irving [84] reviewed information search, while the researchers Ciochină, et al. [23] investigated students' opinions on trust that depends on the recommendations of friends [33, 95]. Furthermore, researchers [28, 95] highlighted the exploitation of user-generated content (UGC).

Currently there is poor cultivation of awareness of philosophical foundations and knowledge inquiry in higher education [34] that influence critical analysis of social networks control. Students and educationists are not acquainted with the learning process involved during coercive influence and the dynamics of manipulation in formal and informal social networks [7, 9, 19, 32].

Researchers Glezou [38, 39, 43] argue that security in online social environments require urgent attention from educational, government and business organisations. Numerous obstacles undermine safe and productive social network activities [29, 79]. Consequently, educational institutions, in collaboration with other social and economy sectors can authorise different solutions for coercive attacks [39].

Based on discussion above, the main purpose of this study was to create a framework for social networks control (SNCF) that would motivate educational, government and business institutions to act proactively towards minimising endangering the security of social networks. This highlights the specific objectives for this study, namely, to derive a theoretical and conceptual background as a basis for the framework; propose a SNCF framework with its major mechanisms; critically analyse the essential components of the framework; and discuss the learning process, dynamics and the flow within the framework.

Based on the discussions above and the purpose and objectives of the study research, the following questions were set for this study:

- RQ1. *What are major mechanisms of the SNCF applicable to educational environments?*
- RQ2. W*hat kind of dynamics and the flow exists within the framework?*

The following section presents the research methodology.

2. Research Methodology

This research can be described as exploratory and descriptive with the literature review of major concepts connected to social networks control. This study utilizes scientific method and researchers' reflective practice. Scientific data processing,

logical methods and the scientific method rely on empirical evidence and utilize relevant concepts from the current research [50]. "The scientific method encourages a rigorous, impersonal mode of procedure dictated by the demands of logic and objective procedure" [11, 14, 50]. The researchers of this study delivered an insightful analysis of multidimensional concepts and derived a framework for social networks control in that they analyzed scientific literature and existing practice.

3. Theoretical Foundation for a Framework of Social Networks Control

3.1. An Overview

The focus of this paper was on the elaboration of psychological and social control factors relevant to social networks in higher education contexts. Furthermore, this paper detailed dynamics of social networks control emerged with multiple aspects, technology and underlying economic modelling. Social control is not visible as a conscious rational phenomenon, but rather as a concept for urgent rethinking of its main power through ever-increasing social networks and exploration.

Furthermore, social networks control is a complex topic that requires a multidisciplinary approach and perspectives from a number of disciplines such as economy, psychology, neuropsychology, cyber security and software engineering. Social networks control is applicable to HE environments through digital inclusion, online discourses, user generated content and an augmented vulnerability level of students and academics. Current curriculum lacks an in-depth analysis of social networks treats and the explicit knowledge of psychological and technological means. In the following sections, we describe how social control appears in different modes of being and doing in the interface between the digital and physical.

3.2. A Basis for Social Networks Control in Higher Education Environments

3.3.1. An Economic Model

A basis for social networks control emerges from an elementary economic default model that applies a homological transfer [62] between the science of energy and economics [77, 69, 83] and exemplifies three levels of economy:

1. Economic capacitance – capital (money, stock/inventory, investments in buildings and durables, etc.)
2. Economic conductance – goods (production flow coefficients)
3. Economic inductance – services (the influence of the population of industry on output).

Relations between these three levels are dependent on the economic capacitance that controls economic conductance and inductance through its monopolistic role and decision-making processes without accommodating the possible reactions of others. Economic inductance includes services to people who are vulnerable to social control, despite the poor quality of education and manipulation of production and peoples'

pursuits and political leanings [28, 69, 77, 71, 83]. This economic model has not been taught explicitly at universities and other higher educational contexts.

3.3.2. The Economic Model in Higher Education

Contemporary research is silent about the economic model and its influence on higher education, but education and economic engineering work in synergy. Higher education policy is related to economic policy objectives [42, 69, 70]. Consequently, universities contribute to economy as moral symbols, social etalons, education providers and innovation facilitators, promoters of entrepreneurial talent, economic and civic leaders and mostly as knowledge pioneers [72]. Furthermore, universities retain their mission of serving the world's hopes: to solve cross-border challenges; to unlock and harness new knowledge and to build cultural and political cooperation [59, 60, 72, 81].

Nevertheless, university curriculum prevents the understanding of interactions between three crucial factors of the economic model and its impact on social networks control, causing a fruitful environment for youths to become an easy prey of destructive collective conscience [15, 55]. It is necessary to embrace education in the existing economic model, specifically the university and its influence across history. Since economy expand to digital inclusion and user generated content (UGC), the economic model underpins these elements.

3.3.3. User-generated Content (UGC) relevant to Higher Education

Ekbia [8] investigated user-generated content (UGC); its role in wealth generation and highlighting the network asymmetry, that does not erase class boundaries through "digital inclusion". Arvidsson and Colleoni, 2012 agree that digital inclusion is exploitation based on the extensive labour time, skills, relationships and commitments.

Ekbia [28, p. 166] states that "the army of digital networkers, gamers, and users keep the powerful computer engines of technology e.g. Google, Facebook companies running the processes of production, distribution, and exploitation that provide for the incessant flow of capital by pervasive computerized information and communication technologies". Sennett [8, p 170, 75] argues that "the archetype of the ideal subject now is the teenage gamer, the obsessed social media member and the permanently reskilled, re-educated, and mobile professional". Although there is a return on investments of in terms of connections, creativity and participation [28], the social crowd lacks control over common pool knowledge, infrastructure and natural resources that contribute to overexploitations, because the creation of value has shifted from paid to unpaid labour [28, 35, 92].

Fuchs [35, 36] in his theory of user exploitation on social media ascertains that the users spend labour time on commercial social media platforms to generate social capital (the accumulation of social relations); create cultural capital (the accumulation of qualification, education, knowledge) and form symbolic capital (the accumulation of reputation). These capitals are in the process of being transformed into economic

capital. This applies to HE contexts through the use of social networking technologies for educational purposes [44, 52, 95, 47, 21]. Educational networking can assist learners in communication and social interactions to perform educational tasks, to publish or share text, photos, videos and music online; be engaged in shopping and studying; and create personal, professional and informal social network contacts.

Based on the economic model and perspectives on the role of universities seven crucial issues of social networks control have been derived, that are applicable to HE environments.

3.4. Critical Aspects of Social Network Control

3.4.1. Psychological aspects of cyber security in higher education

It seems that educators and students have no basic knowledge of psychological aspects that underpin cyber security within social networks [51, 20]. This may be contributed to the stealing of students' private information that happens very often due to their good credit accounts [66]. Attacks are launched by impersonating a scholastic, posing as a known academic figure or a representative of a sponsorship organisation, promising college scholarships and gaining access to campuses without interference [56].

Through immersion and illusion, an intruder becomes an impersonated person, the new personality. It is necessary to create a pretext, the creation of a believable scenario and to build a believable disguise. Additionally, it is important to build a depth of useful expertise, a routine of a suitable language, understanding of the natural features of the victim's facility, knowing psychology how to manipulate targets [90].

The aim of a strategic social network attack is to develop vulnerabilities: create low-quality programmes of education, particularly in mathematics, logic, systems design, technical creativity and economics; and to impose distractions with matters of no real importance and disengagement from matters of real significance [31, 90]. From a strategic point of view, procedural steps are necessary for social network control namely, exploration of current events; disguise, impersonation; infiltration; use of timing; discovering weak points in an area of defences; examination of psychological weaknesses; distraction; the use of concealment devices and covert listening devices; the use of intelligence; surveillance; sabotage; hiding and silent movements [90].

The tactical network attacks rely on existing social network members' vulnerabilities [31, 51, 89, 90]. By homological transfer, in these circumstances, students will be more prone to engage their emotions and increase their self-indulgence in activities of no tangible value to influence the shifting of students' thinking from personal needs to highly fabricate outside priorities [31, 62, 65].

Most studies propose educational, behavioural and structural intervention methods through prevention, education, identification and enforcement [20, 74, 87] and the incorporation of curriculum change in HEIs. Concurrently, education authorities should guard against cyber invasion by passing cyber laws with strong penalties, as done by Germany with its ground-breaking Network Enforcement Act

[68] and software that is able to search, monitor, analyse and manage the content of social media. In order to understand psychological attacks within social networks, it is necessary to elaborate on online language discourse techniques.

3.4.2. Online language discourse and social networks control

Learners communicate through a variety of language discourse techniques in online contexts. The mind, language and creativity are primary tools for producing value [12]. These are particularly relevant to youths who are in a disadvantaged position in that they acquire critical thinking necessary for filtering online information and detecting social coercive attacks to the determinant of their own advancements. Students and youths are exposed to manipulative discourse through the use of abusive symbolic written communication, verbal or textual utterances and non-verbal signals, specific visual features of text and talk [22, 49, 86, 93]. Online auditory discourse interactions include specific features of talk in vocal communications that can be modified such as faster pronunciation, unclear expressions, short messages and repetition of blurred communications to hamper understanding and recall [67].

Partial or incomplete illegitimate presenting of text and understanding to targeted individuals and groups in educational settings is in the best interests of a powerful group [86]. Textual language involves general layout, use of colour, photos, drawings and different forms of phonetic, phonological, morphological, syntactic and lexical operations that can be manipulated in a silent manner [86, p. 366, 94]. Social engineering is a major threat in online social media services, as it uses many forms of coercive discourses [31, 94].

3.4.3. Social Engineering Intrusions

Social engineering is a major threat in online social media services, as it uses many forms of coercive discourses [31, 94]. Social engineering is the art of manipulating people through the use of psychological tricks, baiting, website spoofing, deception, pretexting and phishing, bribes, blackmail and threats [D. Airehrour, D., N.V. Nair, and S. Madanian, 1998].

Social engineering attackers avoid direct contact with their targets. They favour to exploit emails, the internet, and digital media in order to steal information using a variety of deceptive techniques such as kindliness, orthodoxy and empathy. The main causative factors for social engineering attacks [80] are organisational (e.g. insufficient management and security policies), demographic (e.g. gender, age, personality characters and cultural) and human (e.g. uncontrolled emotions, surroundings, habits or physical impairments**.**

Researchers report that an unspeakable number of social engineering attacks occurs on social media on a weekly basis that can be attributed to human vulnerabilities [3, 6, 31, 51, 94]. Students and academics are vulnerable to losing valuable innovative ideas and patents [10, 58]. Fan, et al. [31, p. 1] proposed a defence model to encounter the process of converting human nature into weaknesses by

external influences. Social engineers need to understand some crucial human flaws that endure social network control.

3.4.4. Human flaws in Social Engineering

Researchers Wilhelm and Andress [90] state that social engineers implement deceptive methods to betray victims to gather information and that is easier than to try to compromise a computer network. It is necessary to have a leader who provides financial, resource, or training support for the malicious endeavour [45, 90]. Four crucial human flaws that social engineers need to be aware of during social networks attacks are:

- *Motivation* – develop skills and knowledge; create efficient operating systems; assure workable solutions; have an internal strive to help others, create income.
- *Weaknesse*s – laziness, anger, fear, sympathy and vanity.
- *Desires* – to be helpful, greedy, and afraid, avoid confrontation and avoid embarrassment.
- *Needs* – security, sex, wealth, pride, and pleasure.

System administrators and network security engineers should apply subtle mechanisms such as looking unable, inactive; producing geography distortion, hiding own capabilities, including exercising unawareness of slowing down network security devices [45, 90]. Fan, et al. [31] suggest several defence approaches to be employed to fix human weaknesses. Students and academics should be aware of the fact that most strategies and tactics regarding social engineering appear on sub-conscious level.

3.4.5. Some Subconscious Strategies and Tactics in Social Engineering

There are multiple sub-conscious strategies and tactics in social engineering, such as applying proper timing in terms of attacks; keeping members of social networks ignorant; lowering their defences; controlling their education; preventing their organisation; infusing more self-indulgence; and assuring minimum resistance to control [8, 31, 84, 90].

Knowing the emotional states of target network members allows intruders to classify the target by emotional type or emotional state that gives a starting point when planning an attack. In addition, the timing and tenacity; skill of lying; making sure that the network security engineers are confused, distracted and under stressful emotional conditions are critical components in social engineering attacks [30, 45].

Whether it because of malformed packets; the use of false identity, or mislabelling malicious data to appear legitimate, it is necessary to use subconscious tactics so that the security personnel would focus more on the facilities in which intruders are not interested [31, 63, 84]. Furthermore, by asking numerous questions about firewalls and internet-facing systems, it is possible to subconsciously influence security engineers to focus on the disruption of a person's daily routines that adds additional stress [25, 54, 90].

Research findings in neuropsychology, such as masking phenomena, can serve for human sub-conscious control within social networks. Fahrenfort [30] introduced the model by Di Lollo, Enns, and Rensink [25] to explain the masking phenomenon. In masking, a stimulus is shortly followed by a second stimulus (the mask), rendering the first stimulus invisible.

This happens in their model because the mask replaces the stimulus representation at input level even before a match can be made between the working space and the input; thus, preventing the stimulus from ever reaching consciousness [30]. This happens when subtle methods are applied to members of a social network, causing a loss of memory since the control of stimulus is prevented and therefore only resides in the sub-conscious mind that can influence memory functioning. Social network control is a learning process of a manipulative assimilation.

3.4.6. The Learning Process of Manipulative Assimilation within Social Networks

For any coercive social network control, manipulation processes play the major role. Manipulation can serve political purposes, ideological purposes, and social engineering purposes [20, 24, 78]. Whatever purpose it serves, there is a final assimilation process [65, 88].

The members of a social network ignore the disturbance of manipulative intrusion, gradually developing full trust in an external control; or they are forced to follow the control mechanism to live together with the manipulating system. When progressing to a level of full trust, the members follow every instruction through a sub-conscious process of extrasensory perception and communication and they reach the "mature" level of assimilation with the imposed control mechanism [24, 63, 76].

Thus, there is a learning process that includes submission, ignoring, trusting, interacting, assimilating and synchronisation with silent forces of manipulation [65, 63]. The victims of a social network learn to keep it secret to ignore chaotic events and are forced to accept involuntary events.

The learning process induced through manipulation contains the voiceless stage, ignoring stage and observant stage, reflecting three major learning phases: submission, defensive/reasoning phase and accepting/surviving phase [24, 76]. They emotionlessly learn how to respect, cope and co-exist with the manipulation system that drive sub-conscious progression towards synchronisation between an external control and internal complete submissive state of mind [19, 20, 46]. There are multiple technological means that can be deployed to aid social networks control.

3.4.7. Surveillance and Electromagnetic Frequency (EMF) in Social Networks Control

Social surveillance through the use of technology has caused resistance [3; 7) because of its convert intention to detect or prevent behaviour that is prohibited. Furthermore, technological means include a combination of offline and online monitoring, real-time surveillance, penetration into personal data; utilising voice acquisition; and applying remote technological means.

Surveillance and manipulation systems were devised, exploiting emotions and using contagious methods within social networks aimed at social movement mobilisation to determine the "critical mass" by studying "digital traces" of members [19, 20, 78]. In online environments these could be bots and applications running to provide us with a comprehensive understanding of the target social network [45].

A little research exists on electromagnetic frequencies and their applications in social engineering and social networks control. Technology has double utility, as it can be used as a surveillance online tool but also serves as a means to exert social control, for example, by transferring discourse communications utilising low electromagnetic frequencies. It is not clear how surveillance and EMF influence social network control if learners and academics don't understand the learning process of manipulative assimilation.

In summary, research indicate that the foundation for social network control is not explicitly taught in HE contexts, and academics and students have a fragmented picture and no clear understanding of the whole process. Therefore, they cannot successfully detect and avoid this permanent threat to their individual personalities and their networks.

The role of economics thinking and the model influence seven major factors of social network control that work in a synergy within HEIs as a multidisciplinary context. Based on the theoretical framework and critical reflections originated in literature, ten factors were integrated to elaborate the framework for social networks control (SNCF) as follows.

4. The Framework of Social Networks Control (SNCF) in Higher Education

Because social network control is organised by different entities in order to fulfil a variety of aims, for instance, political, religious, scientific and economic motivations, their interest is to expand influence to educational institutions. A lack of awareness related to social control techniques have profoundly influenced students' and academics incorrect perception of social networks subtle attacks.

4.1. Background and the Rationale of Social Networks Framework

The framework shapes its structure and flow from perspectives on the basic economics model [79, 83] the relationship between the model, economic features and the role of universities [42, 69, 64]; the impact of user-generated content and exploitations [28' 8, 35]; the role of online language discourse [12, 22, 84]; the knowledge of psychological aspects [31,62]; understanding of social engineering intrusions and human flaw [2, 31]; awareness of sub-conscious strategies and tactics in social engineering [25; 13, 26, 27, 28]; characteristics of the learning process and manipulative assimilation [24, 63, 76, 88]; the use of technological means in social networks control [25].

Owing to the presence of multiple aspects of social networks control, it was necessary to elaborate the framework, highlighting the interplay between economic,

psychological, technological and human aspects. This resulted in the identifying crucial mechanisms/elements and structuring the framework for social network control.

4.2. The Structure and the Mechanisms/Elements of the Framework

This section presents the structure and the mechanisms/elements of the framework of social networks control (SNCF) based on the literature analysis. See figure 1.

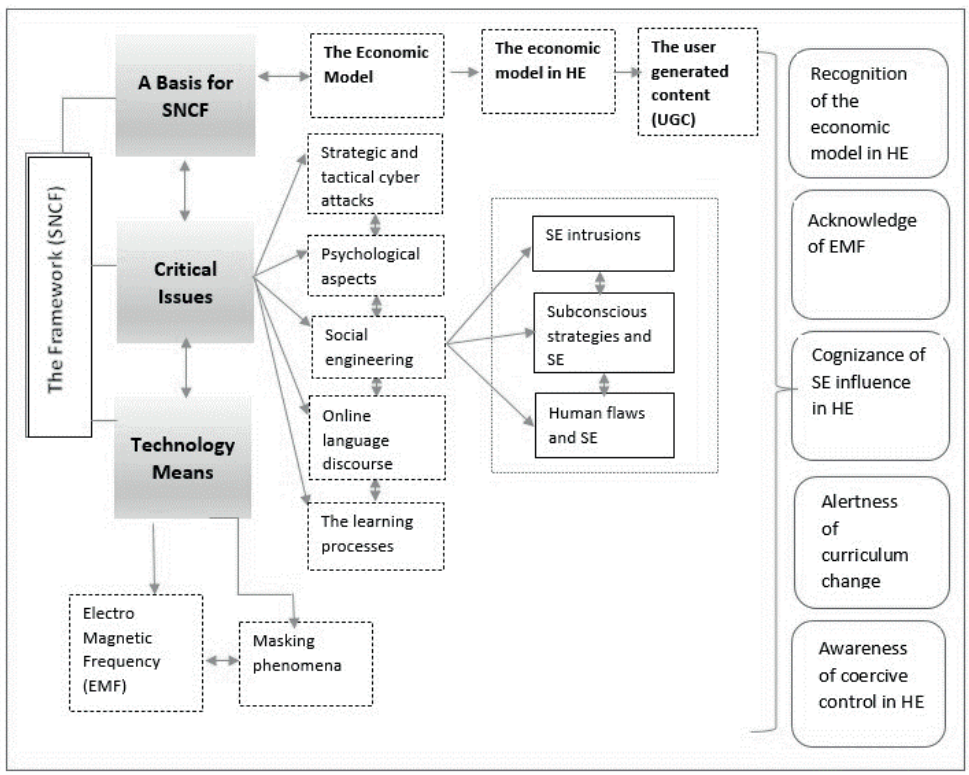

Figure 1. The framework of social networks control (SNCF)

The subsequent mechanisms/elements of the framework were elaborated (see figure 1):

1. A basis for social networks control
   - *a) An economic model*
   - *b) The economic model in higher education*
2. Critical aspects of social network control
   - *i. Psychological aspects of cyber security in higher education*
   - *ii. User-generated content (UGC)*
   - *iii. Online language discourse*
   - *iv. Social engineering as the art of social network control*

v. *Human flaws in social engineering*
vi. *Some subconscious strategies and tactics in social engineering*
vii. *The learning process of manipulative assimilation within social networks*
viii. *Surveillance and electromagnetic frequency (EMF)*

The conceptual framework identified multidisciplinary features of social network manipulation, underpinning the choice of the framework key elements. The 10 key mechanisms/elements of the framework emerged from the voluntary, informal and multidisciplinary nature of social networks control (see figure 1). A synergy between elements is necessary, since they are interrelated and form a complex array of human, technological and organisational issues.

The framework with its mechanisms discloses the covert learning process that is not explicitly noticed by members of a social network including educational networks. Vital psychological features [31, 90] and procedural steps [45] were incorporated in the framework (see figure 1). The framework was created with the aim to deeply engage educationalists, students and stakeholders in conquering the vulnerabilities of social networks [31, 51, 89].

A deeper insight into social networks through the prism of digital economy [13, 83, 71] with their role as "knowledge intermediaries" predisposed the formation of the framework. The framework provides a building block for further examining of social network control elements that could influence HE policy and practice. The framework may promote awareness among educationists to take proactive steps and further interest in social network security features. In the next sections the flow, the dynamics and the process of social network control within the framework will be debated.

4.3. The flow and dynamics within the Framework

The flow of social network control starts from the basis namely the economic model, the role of university and UGC. These three fundamental elements are interconnected and have a profound influence on HE environments. The essential key elements further influence the flow between seven critical factors (*Psychological aspects, online language discourse, social engineering, human flaws, subconscious strategies and tactics, the learning process of manipulative assimilation, surveillance and electromagnetic frequency*). These elements work in a synergy within HE as a multidisciplinary and interdisciplinary environment. The flow designates a logical connection between key elements as motivated previously.

The dynamics of the framework elements are invisible to an untrained observer, because of its sub-conscious features [25, 30]. The aim of covert influence is to induce negative changes, through continuous distractions and clashes, downgrading members' communication skills [73, 86]. The aim is to weaken the network and its members through constant conflicts, blaming, and other intimidating behaviour patterns. This cause the members of a social networks to feel helpless, surrounded and speechless [70].

Social network covert control also include offline attacks and a terrain environmental circumstances must be arranged, in this instance; and the controllers/monitors must be repeatedly present at the same pre-planned places to monitor the movements of member(s) of the network and alternate their actions [76] The social networks are programmed as any establishment unit.

Social network intrusions make no noticeable fiery sounds; cause no apparent physical or mental harms and do not evidently affect daily collective activities [63]. Hitherto, the intrusion creates a distinctive blast, which causes unambiguous physical and mental devastation and undoubtedly affects the daily social routine to a trained observer [71; 25; 65]. The social network intrusion has everlasting consequences, but on completion of the planned intrusion, a memory decay wipes out all traces of evidence. This is achieved through covert actions and the default power of the invisible economic model.

During the learning process, students and educators believe or realise that there is an external human power able to control their behaviour or thoughts. They might instinctively feel that something is wrong, but they cannot express their feeling in a intelligible way with their colleagues as they are not thought to identify sub-conscious manipulative intrusions; and they are not trained how to associate and, how to ask for an assistance [57, 93].

When coercive control is applied gradually, the educators and students adapt to its existence and slowly endure its violation until the psychological pressure via invisible economic means becomes too great to tolerate. The process of social networks control will largely depend on how effective the powerful economic elements have been in controlling the social media; subverting education and keeping the public distracted with matters of no real importance.

Although there are negative consequences of social networks control, the users including learners and educators generate social capital, create cultural capital and form symbolic capital [35, 36]. Also, there is a return on investments in terms of connections, creativity and participation [28].

5. Discussion

The theoretical and conceptual backgrounds provided a basis for forming the social network control (SNCF) that can promote an awareness in terms of solving social network security problems. Through the framework, students and educators are empowered to collaborate on the issue of social networks control, including curriculum and policy changes.

In response to the first research question (RQ1), "*what are major mechanisms/ elements of the SNCF framework applicable to higher educational environments*?", it was ascertained that the following crucial mechanisms/elements emerged from the basic economics model, UGC and the role in higher education: psychological features, online language discourse; social engineering intrusions; human flaws; the learning process of manipulative assimilation; subconscious strategies and tactics; technological means for surveillance and electromagnetic frequency (as the answer to research question one).

In response to the second research question (RQ2) "*what kind of dynamics and the flow exist within the framework*", it can be said that the flow is determined by interactions between key mechanisms/elements that are logically interconnected within multidisciplinary and interdisciplinary HE contexts. The dynamics is reflected through constant conflicts, blaming, distractions, and other intimidating behaviour patterns; downgrading members' communication skills; planned activities, roles, communication modes, outputs and gradual application of covert methods (as the answer to research questions two).

HEIs require a modification of their policies, curriculum in terms of economic tenets and digital economy features to enable students and academics to prevent social network attacks [37, 77, 83, 71]. Decision-makers can be motivated to create secure online environments in collaboration with government, businesses and the community. Understanding the dynamics within social networks and underlying programming features serve as motivation.

6. Conclusions, Limitations and Further Research

This study presented an innovative vision into social networks control and elaboration of the framework and its underlying mechanisms of covert control. The economic model presents a basis for any social network control due to its default features and influence on education and general society. Understanding of connection between educational policies, curriculum and security issues in terms of economic factors is essential to proactively counteract online and offline social intrusions.

The discussion above intensely supports the succeeding general conclusions:

- It is critical to understand the economic model and its influence at universities and other HE contexts
- It is necessary to re-examine philosophical foundations and knowledge inquiry in higher education.
- The nature of educational social networking and coercive intrusions lacks its critical discussions as well as a deeper understanding of ideologies and their doctrines in educational settings.
- Educators and students lack a thoughtful awareness of crucial dynamic, flow and psychological factors that present an entrance to any social invasion particularly in social engineering.
- It is necessary to re-examine procedural steps, strategies and tactics for network control in social engineering.
- Educators and students need an understanding of user-generated content (UGC) and its exploitation features.
- There are many technological means for social network control such as electromagnetic frequencies (EMF), masking phenomena that aid social network intrusion, but its nature is unclear in higher education context.
- Educators and students must recognise their own vulnerabilities and an external attempt to develop further vulnerabilities in order to weaken their social network.

- The learning process of manipulative assimilation have been unknown within HE contexts.
- Curriculum change can fortify students and academics defence against social network control.

Educators and students should have the knowledge of the science of control; they should be aware of the basic economic model and its default influence and know how to apply such knowledge to protect their vulnerable online and offline social networks, due to the lack of economic capacitance and economic conductance and misunderstanding of the role of economic inductance. Social networks control will largely depend on how effective the economic model has been in controlling the social networks and media; subverting education and keeping the public distracted with matters of no real importance.

6.1. Contributions/originality and value added

The conceptual outline provides a solid basis for social networks control framework. Twelve critical key elements of social networks control were derived to form SNCF that could provide a deeper insight into security features of social networking in HEIs.

6.2. Limitations and Recommendations for Further Research

The conclusions of this study should be tentatively applied in educational institutions on a wide scale and the results are rather limited in generalisability due to the requirement for empirical examinations and testing of the framework in real environments. This study doesn't cover semantic aspects and access control features, automation and other hardware and software aspects which present the research limitations.

The framework could be further examined in terms of its strategy, structure, flow and functionalities. Further testing of the framework in the practice is necessary for strengthening the claims for the relevance to HEIs. This conceptual paper and the framework drawn would benefit from its empirical validation.

With our paper we want to highlight the role of social network control features that influence contemporary higher education environments. There is a real treat that this contagious manipulation process can spread within many formal and informal social networks due to its silent spontaneous and gradual intrusion.

References

[1] T. Adorno, T. *Education after Auschwitz. In critical models: interventions and catchwords*, translated by Henry W. Pickford, 191-204. New York: Columbia University Press, 1998.

[2] D. Airehrour, D., N.V. Nair, and S. Madanian, "Social engineering attacks and countermeasures in the New Zealand Banking System: Advancing a

User-Reflective Mitigation," *Information,* 1998, pp. 9-110, doi: 10.3390/info9050110.

[3] L. Althusser, "*Ideology and ideological state apparatuses",* in Lenin and Philosophy and Other Essays, 1970, pp. 85-126. New York: Monthly Review Press, 2001.

[4] Anonymous, (1979). "Silent weapons for quiet wars. An introduction programing material". Operation research technical manual. Available: http://www.law.fulpath.com https://academia.edu

[5] A. Arvidsson, and E. Colleoni, (2012). "Value in informational capitalism on the Internet", *The Information Society,* vol. 28, num. 3, 2012, pp, 135-150.

[6] A.C. Baldry, D.P. Farrington, and A. Sorrentino. "Am I at risk of cyberbullying? A narrative review and conceptual framework for research on risk of cyberbullying and cyber victimization: The risk and needs assessment approach," *Aggression & Violent Behavior,* vol. 23, pp. 36-51, 2015.

[7] A. L. Barabási, M. Newman and D.J.Watts (2006). "The structure and dynamics of networks". Available: https://lief.if.ufrgs.br/pub/biosoftwares/EBB2009/book.pdf.

[8] A. Barbu and G. Militaru. "Determining the differences between companies and customers from the perspective of using social media networks" in proceedings of International Academic Conference Strategica 2018, Bucharest, 10-11 October 2018, Tritonic Publishing house, 2018, pp. 881-893.

[9] A. Barrat, M. Barthelemy and A. Vespignani. "Dynamical processes on complex networks," *Journal of Statistical Physics*, vol. 135, num. 4, pp. 773-774, 2008.

[10] A.V. Beale and K.R. Hall. "Cyberbullying: what school administrators (and parents) can do?" *The Clearing House, vol.* 81, num. 1, pp. 8-12, 2007.

[11] J.E. Bell. Projective techniques: A dynamic approach to the study of personality, New York: Longmans Green, 1948.

[12] F. Berardi, The soul at work: From alienation to autonomy. Boston, MA: MIT Press, 2009.

[13] D.M. Berry, *Critical theory and the digital*. London: A&C Black, 2014.

[14] R.V. Blystone and K. Blodgett. "WWW: The scientific method", *CBE Life Sci Educ*, vol. 5, num. 1, pp. 7-11, 2006.

[15] H. Blumer. "Collective behaviour," in New Outline of the Principles of Sociology, edited by A. M. Lee. New York: Barnes and Noble, 1946, pp. 165-220.

[16] C. Bratianu and R. Bejinaru. "Evaluation of knowledge processes within learning organization," in O. Nicolescu, & L. Lloyd-Reason (Eds.). Challenges, performances and tendencies in organization management pp.125-136, 2016, Singapore: World Scientific. G*overnance,* pp.28-35, 12-13 November 2015, Military Academy, Lisbon, Portugal.

[17] C. Bratianu, A. Zbuchea and A. Vitelar. "Challenging status quo in economics and management", in proceedings of Strategica International Academic Conference (sixth edition), *Bucharest, Romania, October 11-12, 2018*. Tritonic Publishing house.

[18] R.J. Burrowes. (2016). Ideologies: the-psychology-of-ideology-and-religion. Available: http://robertjburrowes.wordpress.com; http://www.ipsnews.net/2016/07/

[19] D.M. Buss (1992). Manipulation in close relationships: Five personality factors in interactional context. *Journal of personality* 60(2), 477–499.

[20] Buss S. "Valuing autonomy and respecting persons: manipulation, seduction, and the basis of moral constraints", *Ethics,* vol. 115, pp.195-235, 2005.

[21] F. Cavozza. (2012). Social media landscape. Available: http://fredcavozza.net/2012/02/22/social-medialandscape-2012/

[22] S. Chaiken. "Heuristic versus systematic information processing and the use of source versus message cues in persuasion", *Journal of Personality and Social Psychology*, vol. 39, num. 5, pp.752-766, 1980.

[23] R.C. Ciochină, D.M. Ccismaru and A. Vîlcu. "The influence of online social networks in the decision- making process of online shopping", in proceedings of Strategica International, Academic Conference, sixth edition, Bucharest, Oct 11-12, 2018, Tritonic Publishing house.

[24] G.R. Collins. "The Manipulation of Human Behaviour", *JASA*, vol. 22, pp. 8-13, 1970.

[25] V. Di Lollo, J.T. Enns and R.A. Rensink. "Competition for consciousness among visual events: The psychophysics of re-entrant visual processes", *Journal of Experimental Psychology General*, vol. 129, num. 4, pp. 481-507, 2000.

[26] H.L. Dreyfus. *On the internet* (second edition). New York: Routledge, 2008.

[27] T. Dufva and M. Dufva. (2018). "Grasping the future of the digital society www.elsevier.com/locate/futures". [Online] Available: https://doi.org/10.1016/j.futures.2018.11.001

[28] H.R. Ekbia. "Digital inclusion and social exclusion: The political economy of value in a networked world", *The Information Society*, vol. 32, num. 3, pp.165–175, 2016. Available: https://www.tandfonline.com/loi/utis20

[29] P. Ekman, P. Emotions Revealed: Recognizing Faces and Feeling to Improve Communication and Emotional Life. New York: Times Books, 2003.

[30] Fahrenfort. J. *Conscious and unconscious vision*. Ridderprint Offsetdrukkerij B.V., Ridderkerk, 2009. ISBN: 978-90-5335-211-3.

[31] W. Fan, K. Lwakatare and R. Rong. "Social Engineering weaknesses for attack and differences investigations", *I. J. Computer Network and Information Security,* num. 1, pp. 1-11, 2017.

[32] C.H.I. Fogg. (2003). "How to motivate & persuade users". B.J. Available: www.chi2003.org › docs.

[33] L.P. Forbes and E.M. Vespoli. "Does social media influence consumer buying behavior? An investigation of recommendations and purchases", *Journal of Business & Economics Research*, vol. 11, num. 2, pp. 107-111, 2013.

[34] M. Foucault. "The Discourse on language (Appendix)", in *The Archaeology of Knowledge*, translated and edited by AM Sheridan Smith, pp. 215-238. New York: Pantheon Books, 1972.

[35] C. Fuchs, "Labor in informational capitalism and on the Internet", *The Information Society,* vol. 26, num. 3, pp.179-196, 2010.

[36] C. Fuchs, "With or without Marx? With or without capitalism? A rejoinder to Adam Arvidsson & Eleanor Colleoni". *Triple C*, vol. 10, num. 2, pp. 633-645, 2012.

[37] H.A. Giroux. *Neoliberalism's War on Higher Education*. Chicago: Haymarket Books. Google Scholar, 2014.

[38] K. Glezou, M. Grigoriadou and M. Samarakou. "Educational online social networking in Greece: A Case Study of a Greek Educational Online Social Network", *The International Journal of Learning,* vol. 17, Issue *3,* pp. 399-420, 2010.

[39] K. Glezou. "Educational online social networking in tertiary education - A teaching intervention", in proceedings Informatics and Telecommunications Conference, University of Athens, Greece 2012, p. 1-99.

[40] A. Grigorescu and R.I. Chitescu. "Cyberspace- a challenge", in proceedings of Strategica International Conference, sixth edition, Bucharest, Oct 11-12 2018, pp. 824. Tritonic Publishing house.

[41] P. Gronke and T. Cook. "Disdaining the media: The American public's changing attitudes toward the news", *Political Communication*, vol. 24, num. 3, pp. 259-281, 2007.

[42] L. Hantrais, L. *Social Policy in the European Union*. New York: Palgrave Macmillan, 2007.

[43] S. Hargadon, S. (2009a). MERLOT MIC August 2009 Presentation: "Educational networking: The role of social networking in education". Available: http://www.educationalnetworking.com/Presentations.

[44] S. Hargadon (2009b). "Educational networking", Available: http://www.educationalnetworking.com/

[45] M. Hatsumi, M. *History and tradition*. Burbank (CA): Unique Publications", editor Ninjutsu, 1981.

[46] D. Holender and K. Duscherer, K. "Unconscious perception: The need for a paradigm shift,"*Perception & Psychophysics*, vol. 66, num. 5, pp. 872-881, 2004.

[47] A.M. Kaplaan and M. Haenlesu. "Users of the World unite! The challenges and opportunities of social media", *Business Horizons*, vol. 53, num. 1, pp. 311-330, 2010.

[48] C. Katz. *Education, technology, and social control*, Macmillan Reference USA, a part of Gale, Cengage Learning WCN 02-200-210) Philosophy: Technology, 2017.

[49] E. Katz and P. Lazarsfeld. Personal influence: The part played by people in the flow of mass communications, New York: Free Press, 1955.

[50] C.R. Kothari. *Research methodology: Methods and techn*iques. New Delhi: New Age International Publishers, 2004.

[51] U. Kuram, U. "Psychological needs as a predictor of cyber bullying: a preliminary report on college student", Educational *Sciences: Theory and Practice*, vol. 9, num. 3. pp. 1307-1325, 2009.

[52] J.M. Ladd. Why Americans hate the media and how it matters. Princeton, NJ: Princeton, 2011.

[53] G. Lawson, A. Stedman, C. Zhang, D. Eubauks and L. Frumkin, L. "Deception and self-awareness", in Engineering Psychology and Cognitive Ergonomics – 9th International Conference EPCE 2011, Heideberg, 2011, Springer, Verlag, pp. 414-423.

[54] P.M.A. Linebarger. *Psychological Warfare*, Washington: Infantry Journal Press, pp. 9-10, 1948.

[55] A. Lloyd, "Guarding against collective amnesia? Making significance problematic: An exploration of issue", *Librarytrends,* vol. 56, num. 1, pp. 53-65, 2007.

[56] S. Low, J.R. Polanin and D.L. Espelage, D. L. "The role of social networks in physical and relational aggression among young adolescents", *Journal of Youth and Adolescence,* num. 42*,* pp. 1078-1089, 2013.

[57] A.J. Marcel. "Conscious and unconscious perception: Experiments on visual masking and word recognition", *Cognitive Psychology*, vol. 15, num. 2, pp. 197-237, 1983.

[58] M. Martinez and S. Schilling. "Using technology to engage and educate youth", New *Directions for Student Development*, num. 127, pp. 51-61, 2010, .doi: 10.1002/yd.362.

[59] N. Maxwell. "What kind of inquiry can best help us create a good world?" *Science, Technology, & Human Values*, vol. 17, num 2. pp. 205-227, 1992. doi: 10.1177/016224399201700204

[60] N. Maxwell*. From knowledge to wisdom* (2nd Ed.). Oxford: Basil Blackwell, 2007.

[61] P.A. McCormick. "Orienting attention without awareness", *Journal of Experimental Psychology-Human Perception and Performance*, vol. 23, num. 1, pp.168-180, 1997.

[62] J. Mende. "Homological transfer", PhD dissertation, Dept. of Information Systems. University of Witwatersrand, Johannesburg, South Africa, 2005.

[63] D.S.W. Mitnick. The Art of deception: controlling the human element of security; Wiley: Hoboken, NJ, US, 2003.

[64] R.P. Mourad. "Social control and free inquiry: consequences of Foucault for the pursuit of knowledge in higher education", *British Journal of Educational Studies*, vol. 66, num. 3, pp.321-340, 2018.

[65] A. Mucchielli. The art of influence. The analysis of the techniques of manipulation, Iasi: Polirom Publishing, 2003.

[66] L. Musselman, L, H. McRae, R. Reznick and L. Lingard. "You learn better under the gun: intimidation and harassment in surgical education", *Med Educ,* num. 39, pp. 926–934, 2005.

[67] U. Neisser and R. Fivush. *The Remembering self: construction and accuracy in the self-narrative*. Cambridge: Cambridge University Press, 1994.

[68] Network Enforcement Act (2017). Act to Improve Enforcement of the Law in Social Networks, Germany. Available: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

[69] M. Olssen and M. Peters. "Neoliberalism, higher education and the knowledge economy: from the free market to knowledge capitalism". *Journal of Education Policy,* vol. 20, num. 3, pp. 313-345, 2005.

[70] S. Olswang and B. Lee. *Faculty freedoms and institutional accountability: interactions and conflicts.* Washington, DC, Association for the Study of Higher Education, 1984.

[71] F. Pînzaru, A. Zbuchea and C. Vidu. "Exploring challenges for managers in the digital economy", in Proceedings of the12th European Conference on Management, Leadership and Governance, ECMLG 2016 pp.328-333, Reading: Academic Conferences and Publishing International.

[72] G. Prelipcean and R. Bejinaru. "Universities as learning organizations in the knowledge economy", *Management dynamics in knowledge economy*, Issue 4, pp. 469-492, 2016.

[73] C. Salmivalli and M. Voeten. "Connections between attitudes, group norms, and behaviours associated with bullying in schools", *International Journal of Behavioural Development,* num. *28*, pp. 246-258, 2004.

[74] R. Sennett. *The culture of the new capitalism*. New Haven, CT: Yale University Press, 2007.

[75] G.K. Simon. In sheep's clothing: understanding and dealing with manipulative people, 1996. ISBN 978-1-935166-30-6.

[76] S. Slaughter and G. Rhoades. *Academic capitalism and the new economy: markets, state, and higher education*. Baltimore: The Johns Hopkins University Press, 2004.

[77] L. Smith. Manipulation and the role of social media. Guardian Australia Dec 2018.

[78] D.W. Smythe. Dependency road: Communications, capitalism, consciousness and Canada, Norwood, NJ: Ablex Publishing, 1981.

[79] Software Engineering Institute. *Unintentional insider threats: social engineering*. EEE Security and Privacy Workshops: San Jose, CA, USA. 2014.

[80] S. Stavrou. "Pedagogising the university: on higher education policy implementation and its effects on social relations", *Journal of Education Policy*, vol. 31, num. 6, pp. 789-804, 2016, doi: 10.1080/02680939.2016.1188216.

[81] D. Tapscott. The Digital Economy. Rethinking Promise and the Peril in the Age of Networked Intelligence, New York, NY: McGraw-Hill, 2015.

[82] J. Turcotte, C. York, J. Irving, R.M. Scholl and R.J. Pingree. "News recommendations from social media opinion leaders: effects on media trust and information seeking", *Journal of Computer-Mediated Communication*, num. 20, pp. 520-535, 2015.

[83] J.L. Tyson. *U.S. International Broadcasting and National Security.* New York: Ramapo Press/National Strategy Information Centre, 1983.

[84] T.A. Van Dijk. *Discourse and manipulation*. SAGE Publications: London, Thousand Oaks, CA and New Delhi. *Discourse & Society* vol. 17, num. 2, pp. 359-383, 2006.

[85] C. Vanlneveld, D. Cook, S. Kane and D. King. "Discrimination and abuse during internal medicine residency", *J Gen Int Med,* num. 11, pp. 401-405, 1996.

[86] M.U. Ushe. "Manipulation of religion and task before the Nigerian Christian leaders", *BEST: IJHAMS,* vol. 1, Issue 2, pp. 23-38, 2013.

[87] J.M. Waller (2012). America's political and information war in Europe following World War II. Available: https://www.academia.edu/34992812/Americas_Political_and_Information_War_in_Europe_Following_World_War_II_Resistance_to_Soviet_strategic_political_and_psychological_warfare_2012_

[88] T. Wilhelm and J. Andress (2010). *Ninja Hacking: Unconventional penetration testing tactics*. Syngress; 1 edition (September 24, 2010). ISBN-10: 1597495883 ISBN-13: 978-1597495882.

[89] J.M. Wing. "Computational thinking". *Communications of the ACM*, vol.49, num. 3, pp. 33-35, 2006.

[90] R. Wodak. "And where is the Lebanon? A socio-psycholinguistic investigation of comprehension and intelligibility of news", *Text,* vol. 7, num. 4, pp. 377-410, 1997.

[91] M. Workman (2007). "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security". *Journal of the American Society for Information Science and Technology.* [Online] Available*:* https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.20779. https://doi.org/10.1002/asi.20779

[92] S.C. Yuen and P. Yuen. "Social networks in education", in *Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, 2008,* pp. 1408-1412. Chesapeake, VA: AACE. Available: http://www.editlib.org/p/29829.