UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Carlos Arturo Martinez Forero

Tabletop Exercise For Cybersecurity Educational Training; Theoretical Grounding And Development

Master's Thesis (30 ECTS)

Supervisor(s): Maria Claudia Solarte Vasquez
Co – Supervisor: Raimundas Matulevičius

Tartu 2016

Tabletop Exercise For Cybersecurity Educational Training; Theoretical Grounding And Development

Abstract:

Education and training aspects are vital components of national cybersecurity strategies, to shape, enhance and test the decision maker's level of preparedness before current and future challenges that can arise from a cyber incident. Decision-making processes in cyber defense and security require crucial crisis management competences capable of generating a comprehensive response where safety, well-being and other public and private assets could be put at stake. The purpose of this thesis is to suggest the improvement of potential and perceived weaknesses on the educational components of cyber security strategies, discussing awareness-training models with significant impact on the participants, focusing on strategic decision-making level personnel that could partake of cyber related incidents. The work supports the use of simulation-based scenarios, and concentrates on the design of Tabletop exercises. This thesis shows when a tabletop exercise could be an effective mechanism to shape, enhance and test the awareness, understanding and preparation for strategic decision makers in cyber related incidents. The thesis draws from a disciplinary integration of learning, human computer interaction, and management theories. A scenario-based training provides a safe and flexible environment where the participant is placed into a critical situation while maintaining a realistic insight into the characteristics of cyber crisis and the threats and attacks that may take place. The simulation represents possible challenges, demanding crisis management capacity and an appropriate response. Tabletop exercises permits that andragogical benefits and educational purposes be realized through an innovative and engaging method. Considering elements from experiential learning and situated cognition the learning outcomes of this training model will be measured, using Bloom's revised taxonomy of educational objectives. The OODA Loop will suggest a thoughtful decision making process that also fits well the dynamic of the current proposal. Additionally, the thesis will contribute with an original modular guide that trainers and educators can use for the implementation of a Tabletop exercise on cyber security. National and international level tabletop exercises experience and participation provided empirical support to the theoretical contribution on theory integration, and informed the modular guide development. The work is qualitative and therefore seeks to observe, interpret and understand, by using documental analysis, and observation methods. The work contributes to the relevant academic dialog on its theoretical grounds and also in practical terms, by providing with tools readily applicable to the creation of simulation based tabletop exercises.

Keywords:

Strategic decision making – Tabletop exercises – Cybersecurity – Cyber related incident – Cyber crisis – Crisis management – Training and education – Effectiveness – Learning outcomes – National cybersecurity strategies – Awareness

CERCS: P175 PHYSICAL SCIENCES – Informatics, Systems theory.

KÜBERJULGEOLEKU KOOLITUSE LAUAÕPPUS; TEOREETILINE ALUS JA ARENDAMINE.

Lühikokkuvõte:

Haridus- ja treeningaspektid on riiklike küberturvalisuse strateegiate vitaalsed komponendid, et kujundada, tugevdada ning proovile panna otsustajate valmisolekut nii aktuaalsete kui võimalike tulevaste küberväljakutsete ees. Küberkaitses ja -julgeolekus on otsuste langetamisel üliolulised kriisijuhtimisoskused suutmaks adekvaatselt vastata juhtumitele, mil era- või avalik heaolu ja turvalisus on ohustatud. Selle lõputöö eesmärk on välja pakkuda küberjulgeoleku strateegiate hariduslike komponentide võimalike ning teadaolevate nõrkuste parandamine, arutledes teadlikkuse väljaõpete mudeleid märkimisväärse mõjuga osavõtjatele, fookusega strateegilise otsustamisvõimega personalil, mis võiks osaleda küberjuhtumis. Töö toetab simulatsioonil põhinevate stsenaariumite kasutamist ning keskendub mudelõppuste kujundamisele. Käesolev tees näitab, kuidas mudelõpe võib olla tõhus viis küberjuhtumites strateegiliste otsuste langetamisel teadlikkuse, mõistmise ja ettevalmistuse kujundamiseks, parandamiseks ning proovile panemiseks. Lõputöö tugineb ditsiplinaarsel ja kontseptuaalsel õpinguteooriate integratsioonil mängustamisel põhinevate ajenditega ning juhtimisteooriatega. Stsenaariumil põhinev treening pakub turvalist ja paindlikku keskkonda, kus osavõtja on pandud kriitilisse situatsiooni, säilitades realistlikku ülevaate küberkriisi tunnustest ning võimalikest ohtudest. Simulatsioon väljendab võimalikke väljakutseid, nõudes kriisijuhtimisoskusi ning kohast reaktsiooni. Mudelõppused võimaldavad andragoogilise kasu ja hariduslike eesmärkide realiseerimist innovatiivsel ja kaasaval meetodil. Selle treeningmudeli tulemused mõõdetakse kasutades Bloomi õppe-kasvatustöö eesmärkide liigituse kontrollitud taksonoomiat, arvesse võttes kogemusõppe ja paiknevustunnetuse elemente. VOOT-tsükkel pakub läbimõeldud otsustusprotsessi, mis samuti sobib antud ettepaneku dünaamikasse. Lisaks panustab lõputöö originaalse modulaarse juhendiga, mida treenijad ning õppejõud saavad kasutada mudelõppe teostamiseks küberjulgeolekus. Riikliku ja rahvusvahelise tasandi mudelõppuste kogemus ja osavõtt varus empiirilist tuge teoreetilisele integratsioonile ning teadustas modulaarse juhendi arengut. Töö on kvalitatiivne ning seevastu otsib vaadelda, tõlgendada ja mõista dokumentaalse analüüsi ja vaatlemismeetodite abil. Tees panustab asjakohasesse akadeemilisse dialoogi selle teoreetilistel alustel ning ka praktiliselt, pakkudes vahendeid simulatsioonipõhise mudelõppe läbiviimiseks.

Võtmesõnad:

Strateegiline otsuste langetamine - Mudelõppused - Küberjulgeolek - Küberjuhtum - Küberkriis - Kriisijuhtimine - Koolitus ja haridus - Tõhusus - Õpitulemused - Riiklikud küberjulgeoleku strateegiad – Teadlikkus

CERCS: P175 REAALTEADUSED - Informaatika, süsteemiteooria

Table of Contents

1 Introduction

The purpose of this thesis is to investigate innovative ways on how decision making at the strategic level in cyber related incidents could be improved through awareness, training and education. Weaknesses of educational and awareness-training models within cybersecurity strategies or the lack of models at the strategic decision-making levels, concerning cyber related incidents seem to concern academics and practitioners [1]. It can be said that innovation and end engagement programs or models with more impact are necessary to implement proper cyber security strategies be them of the national or organizational levels, because both types commit clearly to education and training improvement [2].

The narrow focus of this work is the design of tabletop exercises and their foundation as training models linked to theories deriving from the cognitive, management and computer sciences. A coherent cross disciplinary attempt to associate concepts from these theories should result in significant conceptual and empirical contributions that enhance the value that using TTX can add to decision making skills in cyber related incidents. Improved education and awareness training may turn those skills into competencies. The theories that will be integrated into the TTX from the cognitive sciences are: experiential learning, situated cognition, and Bloom's revised taxonomy of educational objectives; management: crisis management, and OODA Loop. And from the Computer sciences domain, an application of perspective commonly used in human computer interaction (HCI): gamification concepts (engagement, role playing). In addition, cybersecurity incidents is the context where the training will take place.

The participation and observation in a national and international level TTX reaffirms the conceptual work on theory integration, providing with data that matches the theoretical contribution. Further the experience achieved during this two (2) interactions commit to the development of the modular guide for the implementation of a TTX with the particular emphasis on decision making during a cyber security incident. It also adds to the development of the computational social sciences and proposes an innovative area of research. The research question that guides the work seeks to conceptualize that educational and training models that use simulated based scenarios, innovate, increase engagement and should strengthen awareness and competences of participants in cyber related incidents strategic decision-making.

In order to resolve the aforementioned question two (2) tasks were formulated: the first is to proceed with the integration of learning theories as well as gamification incentives and management theories applicable to cyber security simulations. The second is to advance the institutionalization of gamification methods in cyber security educational and training programs based on empirical evidence for Colombia or elsewhere that may deem needed and based on theoretical and empirical evidence a tabletop exercise modular guide will be developed contributing to its implementation.

Strategic management defines the scope of this work, in a context where decisions regarding cybersecurity incidents have an enormous potential to affect people and organizations. Therefore, most arguments relate to the role of "human factors". Saaty, and Hamrick & Mason have discussed the adequacy of judgments and the important role of prior experiences and cognition that may affect interpretation and perceptions in decision making processes [3], [4].

The growing dependency on technology is known to confront organizations and users' wide world in constant and rapid transformation based solutions, and the vertiginous growth in the use of telecommunications and interconnected systems in their everyday life. Cavelty argues that three expressions shape reality today: information, cyber and digital. [5]. This realization has turned into a significant security concern for the private and public sectors as well as for ordinary users. Every natural process is developed or supported by technology and along the way the sophistication of criminal activities as well as ever-increasing threats from individuals, groups and organizations that may aim at using technology for criminal purposes.

The theoretical perspectives used, point out the imperative need for strategic decision maker's expertise and proper training. The use of tabletop exercises as a learning method in this context involving decision makers into cyber related incidents can recreate real incidents while exposing participants to hypothetical situations that will require decision making expertise and capabilities.

Simulations play a predominant role in learning, training and awareness; such phenomenon has been discussed by Vogel who claims the effectiveness of simulation games in learning and teaching [6]. Such is the case in nursing orientation, flight simulators, firefighter simulations, military training simulations, project management, and so on. The specific way in which learners, students or trainees are engaged is crucial when the expected outcome is to enhance the learning, training, comprehending and understanding of certain process, such is the contribution or experience with positive results for the simulation based learning on a recent experiment in which students from United Kingdom were to address strategic management decisions based on learning through simulation games and those same decisions had to be also addressed learning through lectures and seminars, results showed more interest from the students for use of the simulation in problem-based learning and it also concludes that cooperative group work helped to enhance students' attentiveness. [7].

The alarming growth of cyber security incidents and the increasing complexity in the techniques and methods employed by these called "sources of cyber threats" are being considered by countries and organizations to develop comprehensive strategies that include awareness, education and training. Cybersecurity strategies must cover education and training aspects, this statement has been argued by White and Pastor, considering not only the technical approach to face this threat but highlighting the importance of the human factor education, attractive training, and awareness raise to help to solve computer related security issues [1], [8]. Scholars and various international bodies recommend the elements that any national cybersecurity strategy must contain, in which Cybersecurity education and awareness program was highlighted among the core of the emerging international best practices in the field. [2].

Over reliance on computer-based technologies in life processes alerts on how information, a vital asset for government and commercial proper functioning, and an essential part of critical infrastructures is being handled. This topic's relevance is undeniable, and deserves attention from all sectors and stakeholders. An additional characteristic comes to mind when cyber-related incidents are featured in simulations considering the complexity and the unknown scope and range of what can be achieved through computer means. In this light, an additional conceptual contribution will be achieved with research in this field, as it can be argued that simulation based training offers gamification-like incentives such as tabletop exercises. A TTX can propose and speculate about the unknown, suggesting the unaware while testing the established, pointing at gaps and vulnerabilities, and with an outstanding feature that is the engaging method in which all of these outcomes are acquired. Stytz supports the importance of simulation environments in the face of preparation of decision-makers to develop abilities and experience on strategic and tactical level towards cyber warfare [9].

The tabletop exercise which uses a simulated based scenario as the basis for its development can contribute to the expertise building, enhance cognition and more accurate perception of the decision maker, contrasting with the shortcomings of traditional methods, the gamification incentives offered by this type of exercise could increase a higher level of engagement of the participants.

The approach of exposing strategic decision makers to a cyber related incident in which decisions have to be made would contribute to the understanding and awareness of the nature and potential of cyber threats, achieve experience, cognition and perception which will determine the formation, training and education of the strategic decision makers. Exposure to realistic situations could contribute to test the actual state of readiness, the suitability of existing contingency plans, regulations, cooperation channels between public and private sector as well as international cooperation channels, and most importantly could also inspire the quest for novel solutions based on the identified flaws.

This work's argument focuses on the use of TTX as the appropriate educational training awareness model within cyber security strategies addressing decision making in cyber related incidents. While traditional learning models present difficulties achieving engagement, linking theoretic concepts into real world situations, granting the opportunity to employ prior knowledge and experience in the shaping of vital decisions, providing opportunities to assume and understand new roles bridging existing gaps, also setting feedback as an important learning element and evidently showing the potential threats present in cyberspace. This approach seeks to show the benefits of the TTX addressing the highlighted issues and finally assessing the learning outcomes of this model under the light of a worldly accepted assessment framework. A national and international level TTX will be the scenario for participation and observation in order to collect data that can give validity to this theoretical approach. A practical and original modular guide containing the design of a TTX, contributes to the advancement and the institutionalization of gamification methods in cybersecurity educational and training programs for its implementation in Colombia or elsewhere where deemed applicable.

The design of this study follows qualitative methodology principles, and methods, seeking a balance between theoretical and practical applications. For the conceptualization section a document analysis method was employed while for the empirical contribution the observation method was the approach that proved the most efficient. The thesis will be organized in five (5) sections, addressing the research methodology used to carry out this thesis, Theoretical Foundations including concepts and state of the art, followed by the discussion and analysis in which the integration of theories will be discussed. A national and international level TTX experience and observations providing strength to the theory integration, a practical modular guide for the implementation of a TTX will also be presented, the last section includes conclusions, limitations and comments on the paths that are available for further research.

2 Methodology

This section introduces the research design of this work, methodological choices for its development and the methods that were used in the information and data collection processes. Figure number 1 represents the aforementioned.

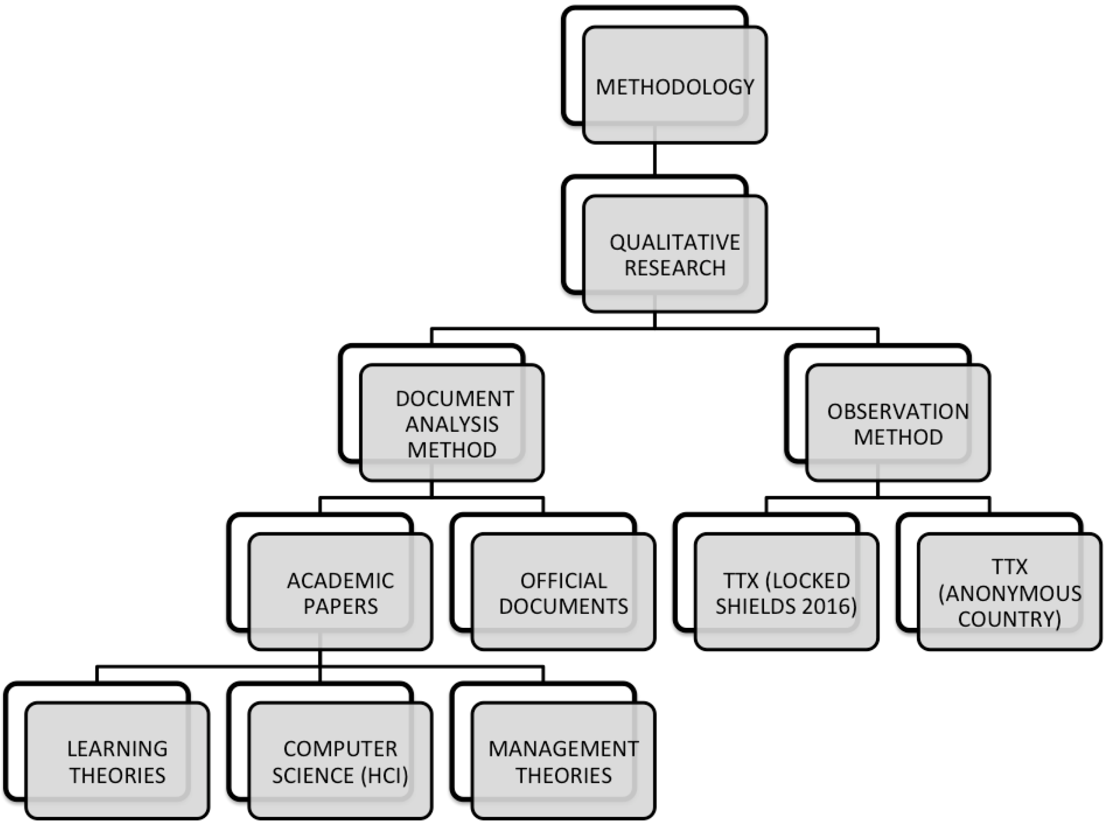


Figure 1: Research methodology

The research design needs emerged after the consolidation of the research problem that was defined as common weaknesses of educational and awareness-training models within cyber security strategies or their absence, in the field of decision-making concerning cyber related incidents. Perceived need for innovation and increased engagement for more effective results and determined a methodology that seeks for a balanced contribution that could combine theoretical and practical applications. A conceptual contribution results from the integrated conceptualization of theories, supported by the document analysis method. The empirical contribution results from the use of the observation method for data collection on the TTX on a national and international level experience, to explore whether the correct approach on the integrated conceptualization of theories. The development of a draft modular guide in the implementation of a TTX in concrete application, will combine the perspectives put forward both contributions.

The document analysis will be processing information relevant to the interdisciplinary approach in which cognitive sciences, management sciences and computer sciences will be integrated to give value to a tabletop exercise designed for strategic decision makers in cyber related incidents. As a result, the main sources of information and data for this method are academic papers and official documents.

On the other hand, the observation method builds around the participation and testimonies of trainees involved in two different tabletop exercises, one of them applied in an anonymous country and the other the strategic track of the international cyberdefense exercise Locked Shields 2016. Each of these exercises featuring different scenarios, events and layouts in what regards to disposition of participants towards the scenario. One of them involved one state and the other seven states, but both assessing the same factors influencing and shaping the decision making process during a cyber crisis. These exercises provide an initial sight at perceptions, concerns and reactions of the participants towards the TTX. In the attempt to assess the outcomes, this work uses Bloom's Revised Taxonomy of Educational Objectives as an additional methodological guide. A draft modular guide on the design of a TTX will also be presented in this research, where the theoretical and empirical results will converge, achieving the balance and application for the implementation of this method.

3 Theoretical Foundations

This paper argues that the design of an effective training course with a tabletop exercise proposal should incorporate elements of gamification such as incentives, [10], [11], experiential learning, [12], [13], and situated cognition [14], [15]. The integration of these theories fit a scaffolding training methodology capable of reaching higher learning levels as Bloom's Revised Taxonomy of Educational Objectives indicates [16]. Because the specific focus of this thesis is strategic decision-making during cyber related incidents, crisis management [17]–[19], and OODA loop principles should be introduced as they can assist any relevant decision making process [20], [21]. In addition to state reports and official documents issued by Colombia or about the Colombian cybersecurity will be revised. [22], [23], in order to support the adoption of this method to meet the needs that may be detected.

Cybersecurity is a current and priority interest of states, organizations and individuals at all level. This opinion is also shared by Franke and Brynielsson, who argue, "*Cyber situational awareness is attracting much attention. It features prominently in the national cyber strategies of many countries, and there is a considerable body of research dealing with it*." [24]. These kind of policy arguments that attempt to increase the awareness of the potential challenges that could emanate from cyberspace, is from where the need for human's abilities improvement, training and reinforcement to confront sophisticated cyber threats in constant evolution gains its importance.

All technology mediated processes that individuals, public and private organizations, and countries develop daily on a functional level involve matters linked to cybersecurity. The dependency on the Internet and the telecommunications systems worldwide is both strength and a weakness. This concern is clearly seen as many countries like United Kingdom, United States of America, Canada, Australia, Estonia, Japan France, Finland, Netherlands and Russia are in the process or have already adopted cybersecurity strategies. Franke and Brynielsson also developed this dependency argument. [24].

The argument of the United States Government Accountability Office states that the sources of cyber threats can be classified or typified in Foreign Nations, Criminal Groups, Hackers, Hacktivists, Disgruntled Insiders and Terrorists [25]. This argument only forces all to become aware of the potential targets we could become, to this approach Klimberg argues that cybersecurity is a concern of individual citizens hence this threat can impact national security. [2].

Dunn illustrates the trend of aggression in cyberspace at national level in less than a decade, this will also add up to the challenges that the world faces. [26]. Table 1 shows the aforementioned incidents.

Table 1: National level aggressions in cyberspace.

Actual Events		
Event	**Attack Method**	**Target**
Estonia (2007)	Website defacements. Distributed Denial of Service (DDOS) attacks using Botnets.	Government
		Private Sector
		Media
Gerogia (2008)	Websites defacements DDOS attacks	Government
		Media
		Private Sector
Ukraine (2013)	Websites defacement. DDOS attacks. Data dumps. Disinformation and propaganda. Campaign. Disruption and infiltration of the Internet and mobile phone traffic.	Government
		Media
		Private Sector
North - South Korea (2013)	DDOS attacks Websites defacement Malware that wiped Master Boot Records (MBR).	Media
		Private Sector
Gaza (2014)	Websites defacement Data dumps DDOS attacks on Israeli targets Spear – phishing	Government
		Private Sector

Adapted from the article "The normalization of cyber - international relations by Myriam Dunn Cavelty".

This diversity of threats and their reach compel states to build a strong cybersecurity strategy including education and training aspects. This strategy component is where simulation based exercises are relevant and pose a different approach to deal effectively with the shortcomings of the traditional classroom training models. Such shortcomings were pointed out by Hammerstein & May, Hernández, Santos, Parra, Tapiador, Peris, López,and Navarrete arguing that Technology evolves at a rapid pace and is in constant demand for new and stronger skills, therefore preparation and education is crucial. However, the traditional models and teaching/training techniques are inefficient because experience is best developed in realistic environments; the classroom training model is time consuming, not scalable enough nor is it cost effective, also not optimal for a rapidly changing field like cybersecurity. Time consumption and no scalability translate into infrequent training opportunities, and as a result the retention and mastery of knowledge is inhibited. [27], [28].

These weaknesses of the educational and awareness-training models within cyber security strategies or their absence, in the field of decision-making concerning cyber related incidents, require innovative techniques for an increased engagement and more effective results. The innovativeness and engaging nature of (Simulated based exercises) SBE was noted by Klabbers, he argued that the complexity of the issues afflicting the world are increasing and the way to address this inevitable phenomenon is through the improvement of our competences through gaming and simulation which have become a powerful combo in treating these evolving issues.

Such phenomenon has also been discussed by Vogel who claims, "*The use of simulation games in learning and teaching has increased due to growing evidence of its effectiveness*" [6]. Such is the case in nursing orientation, flight simulators, firefighter simulations, military training simulations, project management, and so on. The specific way in which learners, students or trainees are engaged is crucial when the expected outcome is to enhance the learning, training, comprehending and understanding of certain process. In this particular case that educational and training models that use simulated based scenarios, innovate, increase engagement and should strengthen awareness and competences of participants in cyber related events strategic decision making, is conceptualized.

Over the weaknesses pointed out in the traditional education models in cyber security, the classification used to list and describe the existing cyber exercises is the Homeland Security Exercise and Evaluation Program [29], which is also shared by Longo in the and the Carnegie-Mellon University [30]. This documents seeks to improve the national state of preparedness by providing a guide to design, develop, conduct and evaluate the different kind of exercises to address the evolving cyber threats. The document lists two general types of exercises; operation and discussion based exercises. Table two and three summarize the categories of exercises and explains them in brief.

Table 2: Definition and types of Operation Based Exercises.

Operation Based Exercises	Focus: Reaction to events presented by the scenario. Outcome: validate plans, policies, agreements, and procedures Features: Role play actual role
· Drills	Involves coordination and supervision, frequently used to assess specific processes in individual organizations. New equipment, plans and procedures as well as appliance on existing ones are on focus.
· Functional Exercise	Conducted in real time and environment, addresses the plans, policies and procedures of management, direction, command and control related members, validates capabilities and functions. A scenario with injects type of exercise.
· Full Scale Exercise	Complex multiple resources, organizations and agencies involved in its planning and execution. Assesses many facets of preparedness, and cooperative systems.

Adapted from HSEEP, 2013 and the Carnegie Mellon University guide by Longo, 2014.

Table 3: Definition and types of discussion based exercises.

Discussion Based Exercises	Focus: on strategy and policy oriented. Outcome: awareness and familiarity with planning and policies. Features: a coached discussion as a follow up.
· Seminars	Conference or meeting: discussion mostly examining, reviewing and introducing concepts such as: authorities, strategies, plans, policies, procedures, protocols, resources, concepts, and ideas. Valuable to develop plans and procedures.
· Workshops	Similar to seminars but with increase participant's interaction. Focus is to create new concepts or ideas. Their effectiveness is achieved by involving large participations of important stakeholders with a very defined agenda including objectives and goals. Outcome: new standard operating procedures, emergency operations plans, continuity of operations plans, and mutual aid agreements.
· TTX	Flowing setting that creates discussion of the many possible issues involved in the hypothetical situation or crisis. TTXs achieve the enhancement of general awareness, validate established plans and procedures works on prevention, protection and mitigation, response and recovery from the crisis generated by an event. Ease conceptual understanding, clarifies strengths and weaknesses. Outcomes: changes in attitude of participants and awareness.
· Games	Operation simulations involving two or more teams in an environment. Includes the standards for any game: rules, procedures and competition, exposition of impact after actions are explored.

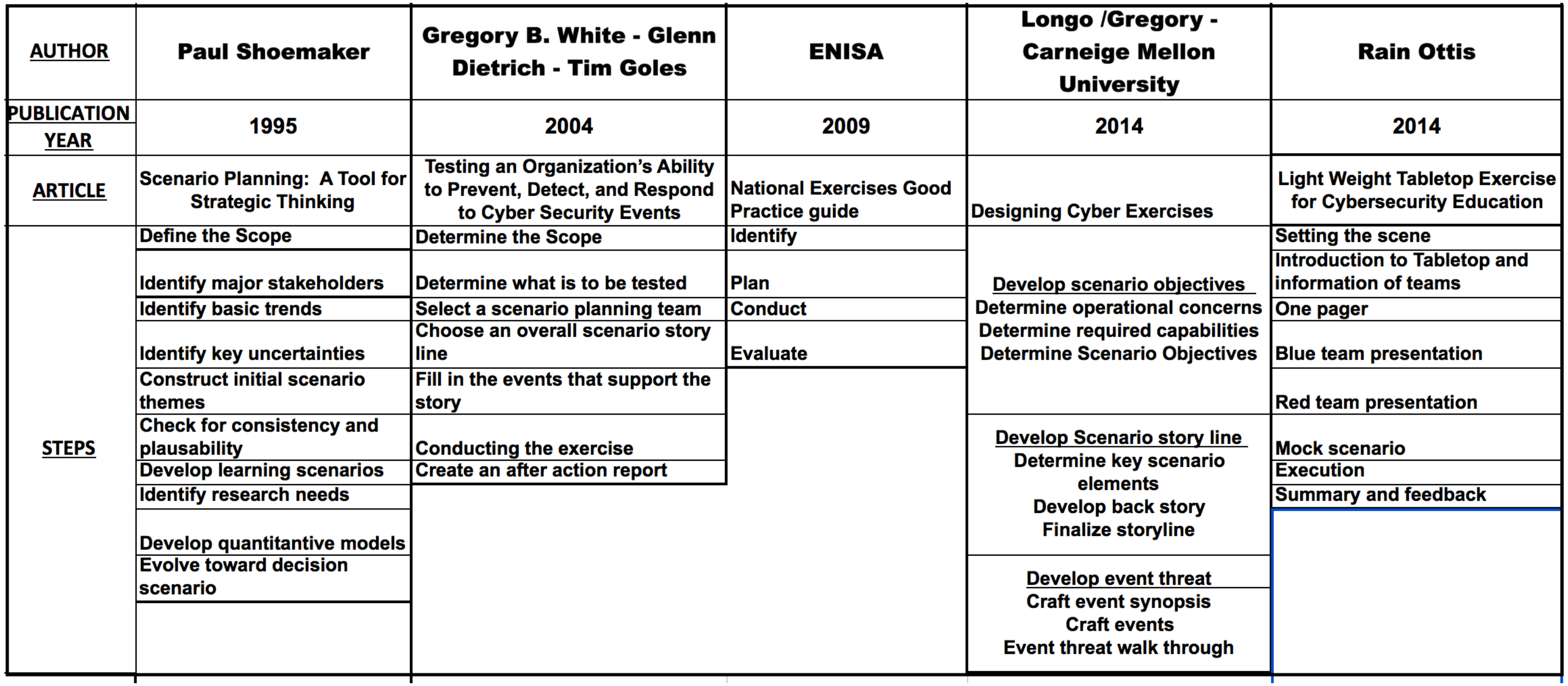
Adapted from HSEEP, 2013 and the Carnegie Mellon University guide by Longo, 2014.

Being the focus selected on strategic decision making in the context of a cyber related incident and considering strategic policy-oriented objectives, the TTX will be the chosen type of exercise that seems the most appropriate because it innovates, is dynamic, increases engagement and strengthens awareness and competences of the participants.

Many authors have written about the design process of these type of exercises, and in spite of minor differences, they all share the same basic, identification of goals and objectives, the planning stage of the exercise, execution it and finally feedback and evaluation. On this could be consulted [1], [30]–[33].

Shoemaker and White referred to SBE's, ENISA and Longo specifically address cyber exercises and proposes a general guide for any cybersecurity exercise, Ottis aims to provide a low load of work high impact and low transaction cost guide for a TTX. Table four presents a comparative chart on the existing guides available to develop exercises. Figure 2 shows comparative data regarding the different approaches on concepts and guides for the development of TTXs.

.



AUTHOR	Paul Shoemaker	Gregory B. White - Glenn Dietrich - Tim Goles	ENISA	Longo /Gregory - Carneige Mellon University	Rain Ottis
PUBLICATION YEAR	1995	2004	2009	2014	2014
ARTICLE	Scenario Planning: A Tool for Strategic Thinking	Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events	National Exercises Good Practice guide	Designing Cyber Exercises	Light Weight Tabletop Exercise for Cybersecurity Education
STEPS	Define the Scope	Determine the Scope	Identify		Setting the scene
	Identify major stakeholders	Determine what is to be tested	Plan	Develop scenario objectives	Introduction to Tabletop and information of teams
	Identify basic trends	Select a scenario planning team	Conduct	Determine operational concerns	One pager
	Identify key uncertainties	Choose an overall scenario story line	Evaluate	Determine required capabilities Determine Scenario Objectives	Blue team presentation
	Construct initial scenario themes	Fill in the events that support the story			Red team presentation
	Check for consistency and plausability	Conducting the exercise		Develop Scenario story line Determine key scenario elements Develop back story Finalize storyline	Mock scenario
	Develop learning scenarios	Create an after action report			Execution
	Identify research needs				Summary and feedback
	Develop quantitantive models				
	Evolve toward decision scenario			Develop event threat Craft event synopsis Craft events Event threat walk through	

Figure 2: Comparative chart on concepts and guides on the development of a TTX

Ottis defines the TTX as a scenario based interactive learning tool where the training audience is role-playing through hypothetical problems [33]. The problems are hypothetical in the sense that no real systems or hands-on lab components are involved (Ref ibidem). However, the scenario and the problems are generally inspired on real life. He also points out the importance of interdisciplinary competences and the need for expertise on law, psychology and political science to contribute to cybersecurity studies. Cyber exercises frame a scalable and flexible method that can be designed to meet specific learning objectives and skills in participants, emphasizing the use of TTX can show interrelations in technical, procedural and human aspects of cyber security within varying areas of expertise and skill levels. (Ref ibidem) The HSEEP argues that participants of a TTX are led to address critical elements in depth and to solve those issues, pointing out the dynamic engagement of participants and their contributions in a safe environment for decision making. [29].

Linking to the aforementioned concerns are the concepts of "involvement" and "engagement" contemplated by the human computer interaction theory of Gamification. Zichermann and Cunningham wrote that "*Gamification is the process of using game thinking and game dynamics to engage audiences and solve problems*" [10], Zichermann stated that the importance of this concept lies in the fact of boredom and argues the effect this causes in the brain, causing resistance and rejection to the process in execution. He points out the habituation phenomenon derived from boredom itself, which causes loss of efficacy decreasing focus on the essential. He also points out the adaptivity games offer to players, framing routine killing reducing the engagement possibilities. [34].

The term gamification was coined in 2008 [35], and since the concept has gained relevance not just in the industry but also in the academia, drawing the attention of researchers of the HCI (Human Computer Interaction) field and game studies; such is the argument from Deterding et al. also noting the "commercial deployment of gamified applications potentially promising new lines of inquiry and data sources for HCI and game studies." (Ref ibidem). Hamari et al explained the growing relevance of the theory and the way in which it increases user engagement ultimately improving the quality of products and services. [36]. The same authors also denote gamification as a next generation term for marketing and customer engagement and present a chart that shows the growing tendency on the topic increase of academic writing and publications during the last couple of years.

To link gamification to the current research, Karl Kapp's contribution is taken too into consideration. It mainly relates to the convergence between games, learning and technology. In his words, "*Gamification is an emergent approach to instruction which facilitates learning and encourages motivation through the use of game elements, mechanics and game-based thinking. In gamification, the student does not play an entire game from start to finish; rather they participate in activities that include elements from games such as earning points, overcoming a challenge or receiving badges for accomplishing tasks. The idea is to integrate game-based elements more commonly seen in video, entertainment focused or mobile games into instructional environments*". [11].

As presented, gamification appears to be mainly a HCI concern highly associated and mostly understood as related to digital technologies. Nevertheless, the term and the contribution it can deliver to the learning environment leaving aside technology aspects seems relevant. Groh, for instance, states that gamification is not circumscribed to digital technologies [37]. This thesis highlights "engagement" which is the key element provided by the gamification concept into the TTX to address strategic decision making in cyber related incidents.

Notwithstanding the previous arguments, gamification incentives alone cannot guarantee the success of the TTX. This work integrates other theories and seeks to affect other aspects of training and education. Learning theories that can be used and identified in proposals of TTX are discussed as well. Experiential Learning, on one hand and Situated Cognition on the other. According to Kolb experiential learning is a process whereby knowledge is created through the transformation of experience, combining experience, perception, cognition, and behavior [12]. Beard and Wilson say that experiential learning could be defined as the understanding of the commitment between the essence of the person and the exterior environment in which he interacts. [13]. The experiential learning seeks to link learning and regular day-to-day behaviors, expecting to improve education through experience. Such is the argument by Kolb when stating that it brings innovation to education methods and techniques, creating an environment in which learning, work and life activities conceive knowledge [12]. Ideas, concepts, knowledge and perceptions can and will be made, shaped, modified formed or reformed, through the interaction with the environment that wants to be improved. Three different models of experiential learning give value to the relation and expected outcome this approach seeks to settle, highlighting experience and feedback as essential elements to consolidate into the TTX.

The Lewinian model of Action Research and Laboratory Training, points out that "*learning is perceived as a four-stage cycle in which immediate concrete experience is the basis for observation and reflection*". These observations are then turned into a theory from which new implications for action can be deducted and this deduction operates as guidance to create new experiences. Two aspects are determining in this model: one is the personal experience of the participants the other narrows down to the feedback of the experience the participant was exposed to, these two aspects are marked as necessary for an effective learning outcome. (Ref ibidem).

The Dewey's model of learning is similar to the Lewinian model, with similar components, mentioning observation, knowledge or perceptions, and judgment as crucial to this method. The process for Dewey in the observation phase has to do with the environment in which situation is evolving on and noticing every existent condition, the phase of knowledge or perceptions regards to events, situations or experiences you know or are aware of, prior to this experience, and the judgment phase relates to bringing together what was observed and the knowledge or experience to the development of a meaning prior applicable to the situation that is being created considered valuable. Feedback is considered valuable. (Ref ibidem).

Piaget's influential work appears to be more specific regarding the identification and classification of stages using age as assessment parameter. Each stage is characterized by unique a developmental process that affects learning. Piaget argues that the learning process takes place in a never-ending interaction between the individual and the environment. (Ref ibidem).

Situated Cognition also connects to the TTXs. According to Brown et al, situated cognition has emerged from theorists who consider the context in which learning occurs as being central to understanding adult cognition, and that this learning model assumes that the knowing and doing cannot be held apart in successful learning. Once this condition is met it brings forth the learner or trainee into an overriding realm to which the method refers to as culture or context. The role of this element is vital, and relates to the specific situation or reality that the individual can potentially face, so he/she will know in which to interpret and use the lessons learned by doing (activity in context). This theory, which differs from the classical learning theories, combines, concept, activity and culture. [14], [15].

Once these innovative elements are present in the learning environment, Bloom's Revised Taxonomy of Bloom Educational Objectives can be used as a scaffolding cognitive technique to assist the learning process progression towards more advanced patterns of knowledge.

Benjamin S Bloom originally conceived this framework in 1956, under the criteria of unifying evaluation standards, establishing a common language on learning goals and remarking effective courses or curriculums across various universities. It became a very accepted framework and has been translated into 22 languages. His model included the following categories from simple to complex and concrete to abstract: knowledge, comprehension, application, analysis, synthesis and evaluation. [16]. This Taxonomy was revised 45 years later and modernized from the previous model. David R. Krathwohl, kept the same number of levels, but three were renamed; knowledge replaced by remember, comprehension was replaced by understand and synthesis was replaced by evaluation. In that order of ideas Remembering, Understanding, Applying, Executing, Evaluating and Creating, are the final levels of Bloom's Revised Taxonomy of Educational Objectives for the classification of educational learning objectives. [16], [38].

This taxonomy as method serves science and education to classify learning activities, and evaluate outcome levels from the very basic to the most complex. Due to its wide acceptance, this paper relies on the same framework and employs it as an already validated reference to assess the effectiveness of the selected methodology.

During TTXs participants are placed under pressure, proposing emergency environments intended to generate discussion while their crisis management skills are put to the test. Extensive literature is found on the topic, from where it can be said that three key components of a crisis are highlighted: threat, uncertainty and urgency. [17]–[19].

The definition provided by Stern exhibits the necessary elements to fulfill the objective of consolidating crisis management into the TTX; he argues that "*a crisis takes place when an experience of a serious threat to the basic structures or the fundamental values and norms of a system, which under time pressure and highly uncertain circumstances necessitates making vital decisions*".

Threat exists when the spark of life, freedom, justice, equality, security, the guarantee of health system and service, monetary activity, confidence in the government and its institutions, and nowadays privacy, are at stake. Uncertainty coexists with each threat, in the sense of lack of information, unclear reactions to situation and a fuzzy picture of affectation. Under the presence of these two components urgency takes place, which translates into time and a rapid response, this is where the decision-making is crucial and the efforts must convert into settling the crisis and stabilizing the organization or the country while time is running. [17].

Decisions define the past and shape the present and the future, the conscious and thoughtful manner in which they are made will have a crucial impact on the development of every specific situation, selecting one option among other several many to resolve or manage a given matter will make a difference. More concretely focused onto the decision making process in this cyber crisis the OODA Loop (Observation, Orient, Decide, Act) can be incorporated, as naturally it takes part of most thoughtful decisions. The Air Force Captain John Boyd during the mid 1970's introduced the OODA Loop in the United States of America. He was tasked to study the air-to-air combat situations during the Korean conflict in which Americans were more successful than Koreans even though American airplanes (F-86) were inferior to its Korean opponent (MiG-15). The results of his theory revealed that the American plan had allowed better observation, and based on better observation and high powered hydraulic controls the possibility to adjust or adapt to every new change in the enemy strategy, allowed him to switch from his activity to another in a timely manner, frequently quicker than the adversary. [20].

This approach claims that acting faster than the opponent translates into a great advantage, so when the adversary acted, a different activity is being held already which could be stated as a rapid and appropriate response to a situation. The observation step regards to the collection of data from the opponent, the environment and yourself. This will make you aware of the specific situation. The Orientation step involves the interpretation of this data, it's processing based on specific perception, which is determined by cultural and experiential elements. After comes the application to update the actual reality creating a clear mental picture of what is currently happening. The Decide step is when the course of action is determined based on the results from the two previous steps and finally the Act step follows through. Since your actions will lead to reactions from your opponent, the Loop or cycle starts again and encourages employing the cycle considering the new inputs. [21].

Considering the different sciences or cognitive domains and their contribution to the TTX in decision making in a cyber related incident, the Colombian case and its current state of cyber security development was extracted after the analysis of official documents regarding this issue.

The growing dependency on technology-based solutions in organizations, and the vertiginous growth in the use of Internet and other telecommunication and interconnected systems for people on their everyday life has become a significant security concern in Colombia as in the rest of the world. Along the way with technical and social advancement come the sophistication of criminal activities and ever-increasing threats from individuals, groups and organizations that may aim at using technology for unlawful purposes. In the year 2011 the Colombian Government designed and produced a document, which was to become the cornerstone of the National Cyber Security strategy roadmap. It was deemed due because the capacity to address threats that compromise national security in cyber-related events was insufficient. This document was named the "CONPES 3701". The text collects all information concerning previous efforts in cyber security formulated by the Colombian Government, and includes statistics on cybercrime that reveal its alarming growth. Significant information was collected and analyzed in order to obtain an up to date understanding of the state of capacity to confront cyber threats and conceive the need to strengthen the cyber-capacities at the state level. It included the rate of growth of internet users between 2005 and 2009, the number of internet subscribers between 2008 and 2010, the rise of online transactions carried out by the end of 2010, the fact of being a target of cyber-attacks to the hacktivist group "Anonymous" on governmental online sites and correlations with the increase in citizen complaints regarding cyber offences. Under these circumstances, added international events such as the 2007 attacks in Estonia; the 2009 attacks against the white house and the mariposa (butterfly) botnet in 2010 that resulted in Colombia having being the fifth most-affected country, were the basis for concluding that flaws required prompt attention. In this thesis the current Colombian cybersecurity state will be presented, drawing from official documents on earlier assessments; gaps or failures regarding performance competences and awareness education will be identified and the use of simulated based scenarios to approach this issue will be suggested.

During the preparation of the "CONPES 3701", three were the problems identified. The document reads:

> - *"Cybersecurity and cyberdefense initiatives and operations are not adequately coordinated,*
>
> - *Insufficient availability and coverage of specialized training in cybersecurity and cyberdefense and,*
>
> - *Weak regulation and legislation on information and data protection".*

The second will be on focus in this thesis, in the same light already shed by the theoretical insights established above. This points to the general research problem that merits the development of a thesis and the aim is to contribute to the strategic level effective preparation for decision-making process, which must be addressed when confronting a cyber-related crisis. The specific goal is to consider ways to address this issue in a more engaging manner, so that expertise can be gained along with increased awareness of the evolving challenges that could pose a threat for Colombia or other countries with similar needs in the future. [22]

The CONPES 3701 also states that "*expertise in the areas of cybersecurity and cyberdefense in both the public and the private sector is limited in Colombia Although a number of higher education institutions in the country offer specialty courses in computer security and computer law, the study noted that the availability of specialized academic programs in these areas is low. Accordingly, a significant number of students who embark on some form of education in the area of information security do so by enrolling in programs offered by foreign institutions that do not address the Colombian reality in any depth*." To approach this issue a revised Bloom's cognitive taxonomy will be considered applying the different levels of knowledge that it proposes, namely remembering, understanding, applying, analyzing, evaluating and creating in regard to cybersecurity safety and awareness [16], and making sure that this kind of simulation exercise will scaffold a process towards higher levels of cognition allowing participants to become creative problem solvers. Colombia's capacities are insufficient and developing at a very low pace if compared to the evolution and complexity at which technology does and disseminates at a global scale; such is the case of The United States of America where projects such as Cyber Storm I, II and III, DARPA National Cyber Range, USCYBERCOM and SIMTEX among others, reach implementation. Other instances are, India's Divine Matrix and France's PIRANET [39].

The "CONPES 3701" and its guidelines have accomplished many of its objectives for the improvement of the Colombian national cyber security such has been considered an appropriate institutionalization consisting on the creation of three entities that form the so called "cybersecurity trident." One operates at the national government level, a second at the military level and the third at the police level. Besides, a legislative development approach has also been followed, so legislation and international cooperation is being established. Nevertheless, the revision to the penal code to typify cyber-related crime has not been completed yet and some efforts are being made in order to be part of the Budapest convention [40]. A re-assessment was executed in the year 2014 by request of the presidency in order to evaluate the current situation regarding the National Cyber Security "(Organization of American States (OAS)). This consisted of a technical assistance mission provided by the OAS in which the Colombian institutions with responsibility on national cybersecurity were visited, presentations from Colombian experts on cybersecurity were held and discussed and finally brainstorming with the relevant authors of cybersecurity in Colombia took place". [23].

The assessment also revealed four key problems, which remained after the development of CONPES 3701 guidelines and proposed to remedy them by:

"- *Strengthening Institutional capacities for cybersecurity and cyberdefense,*

- *The creation of cybersecurity and cyberdefense capabilities,*

- *The establishing and improving a legal framework in cybersecurity and,*

- *International cooperation between interested" multiple parties. Only the first and second are relevant for this thesis*".

Both assessment outcomes have a common denominator and put manifest what can be considered peremptory aspects to be improved: the learning, training and comprehension of cyber-related issues that may compromise the critical elements of cyberspace that qualify as of national interest. Any National cybersecurity strategy must cover education and training aspects; such is the conclusion of G.B White when stating, "Technology alone is not sufficient to solve the computer security problems the nation faces. The human element is present at many places in our approaches to security and these human elements should periodically be tested to see if they could effectively respond to cyber security events. [1]. This contribution is also backed up by Pastor who states that "The best way of improving the reactions of any person when security is threatened is by providing him/her with better education, attractive practical training and raising the general awareness on information assurance". [8].

4 Discussion and Analysis

4.1 Theory Integration

The use of TTX for educational and training purposes and awareness within cyber security strategies and decision making during cyber related incidents is conceptualized in this section. The assumption that these elaborations put forward rest upon the links between training of competences and engagement, rather than between information and cognitive exchange in a vacuum. On one hand, engagement is a real and well-documented challenge in traditional teaching and learning models, while on the other in innovative and gamified proposals such as simulation based and TTXs is not. However, the potential of these last may not be yet uncovered due to what seems insufficient academic backup in applied fields and lack of evidence on that the simulation may be designed to involve the same or more andragogical value than any other instructional design. In the approach that this work advances the priorities are to link theory and real world situations; allow participants the opportunity to employ and test prior knowledge and experience and take decisions that seem and feel crucial; to commit to new roles and assume unfamiliar roles; to bridge existing gaps of understanding via experience; and, to provide feedback with the realization of its importance as a constructive and fundamental learning element. A TTX that is organized for cyber security and defense training is also a cognitive tool to keep participants up to date in the field.

The following pages will explain how to benchmark this perspective, highlighting the combination of concepts relevant for TTX design and presenting a balanced interdisciplinary backup that can persuade on the effectiveness of such methods. Engagement, learning and capacity building can be enhanced with the integration that takes from the cognitive, management and computer sciences and results into a discussion based exercise focused on decision making for cyber related incidents. Figure 3 shows the different disciplines that converge into the TTX.

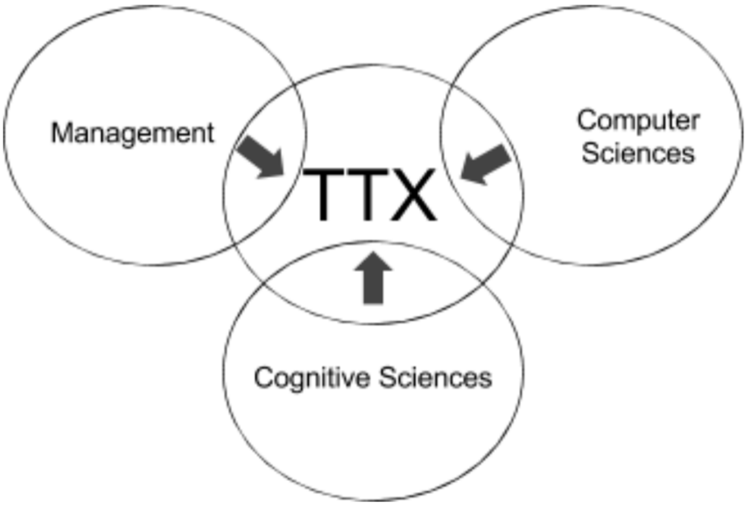


Figure 3: Integration of sciences into a TTX.

The concepts more relevant towards the ends of the study were selected from theories belonging to each of the disciplines mentioned above. The method proposed is claimed to be an appropriate educational training awareness model for decision making in cyber related incidents, via induction, development of theory and reasoning. Table 4 and Figure 4 summarizes the concepts that are useful and relevant to the TTX conception under the light of the Bloom's Revised Taxonomy of Educational Objectives as an assessment framework.

Table 4: Science, theory and concept relation

Science	Theory - Branch	Concepts
Computer Science	HCI - Gamification	Engagement Role playing
Cognitive Science	Learning Theories	Experiential Learning Situated Cognition Revised Taxonomy
Management Science	Management Theories	Crisis Management OODA Loop

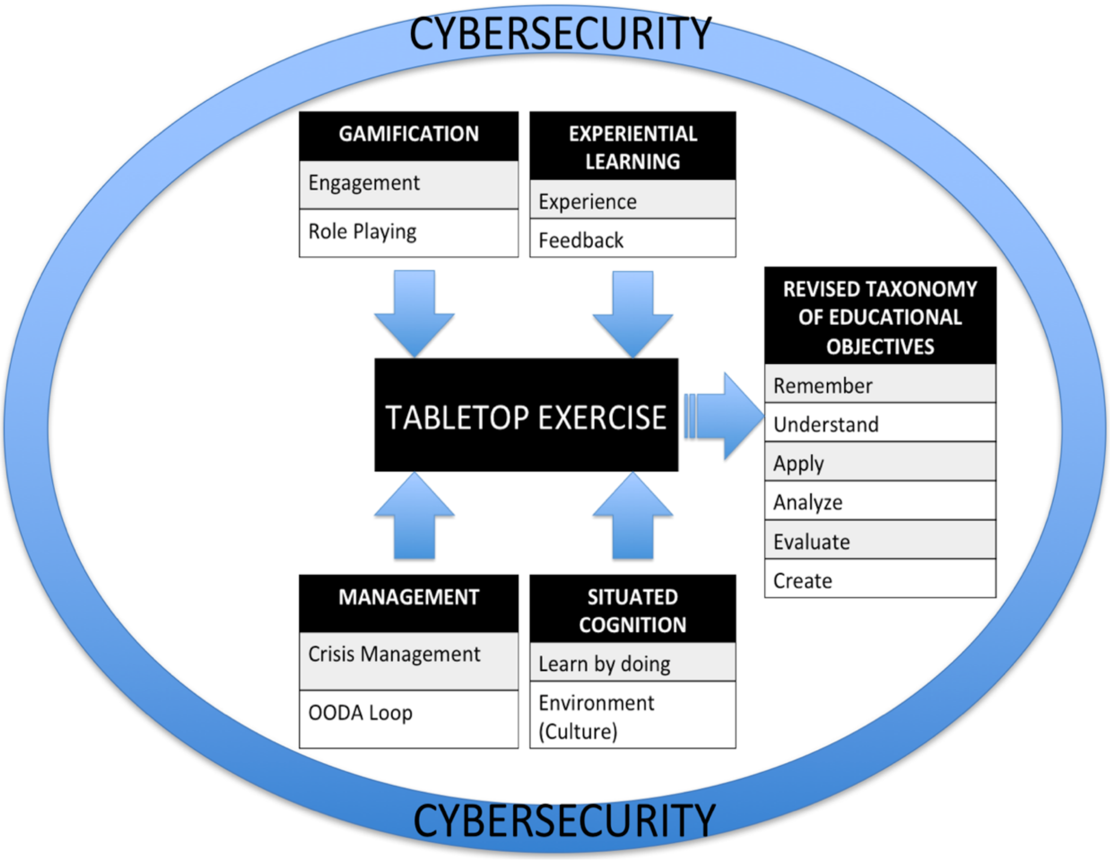


Figure 4: Integration of theories into a TTX.

TTX models can be deconstructed in their essential elements to address the effect that they have on the participant's skills and competences. The main arguments rely on the interaction of these concepts that are present or link to the stages of a TTX. An incident regarding cyber security breaches, vulnerabilities or harm is simulated to trigger a crisis that will put to the test the participants' strategic management decision making competences as well as their knowledge. The consideration of the OODA Loop approach would be convenient for that purpose, being a planning tool that may be well known and consolidated among the most experienced participants. During the time elapsing until the end of the exercise, the need for decision-making processes is triggered with the inclusion of injects. The TTX unfolds a cognitive test, added the experiential learning and situated cognition tactics, while engaging the participants as they role-play through the hypothetical situations in a safe no-fault environment. Consequently, Bloom's Revised Taxonomy of Educational Objectives appropriately fits the assessment phase of the exercise.

During the scenario created by the TTX, DMs (Decision-makers) must urgently respond to the given situation in a complex environment, under the pressure of running time and information scarcity. Crisis management skills and training are necessary in strategic decision-making during real cyber related incidents. The OODA Loop method matches TTX models that feature threat, uncertainty and urgency. The Observation step fits into the collection of information stage after every inject or new incident unfolds; the Orientation step corresponds to the specific way in which participants interpret data and update the crisis scenario they are acting upon; the Decide step also consists of determining the course of action; and, the Act step would be following through as well. Once this process is completed the loop repeats, and the consequences and impact of prior decisions can be observed in regard to the new incidents.

The exercise conducted this way and simulated scenarios in general create an environment beneficial for Experiential Learning. Behavioral change as a byproduct of learning could follow exposure to these methodologies. Individuals when living the events recreated in a realistic manner, could relate to their experiences and reflect on the possibilities that could arise during a cybersecurity crisis. Even though it seems that the most accepted, already validated and common learning theories are the behavioral and cognitive theories, this view captures value (teamwork, experienced participants, diverse methods, complex scenarios, multidisciplinary groups) from the mere exposure and performance departing from the classical instruction models. Current learning models still rely heavily on cognitive reinforcement and other tactics that do not reflect the characteristics of the information society, the fast pace it favors and its widespread appreciation for authentic experiences. Experience learning applications are not limited to the realm of educational strategies in cybersecurity. However, the revival of Leontiev's activity theory, so much concerned with some of the same perspectives, was the inspiration of human computer interaction experts that is, in the context of a recent wave of computer sciences' development.

The role of feedback is highly appreciated in TTXs during their conduction and after their completion. A debriefing stage offers the opportunity to visualize and discuss the issues that arose for strategic decision makers within the working groups during the exercise, supporting sound conclusions and enabling comparison among the different responses generated throughout the game to furtherly achieve the novel search for appropriate solutions to the located deficiencies.

Situated Cognition is also identified during TTXs because the cornerstone elements of this learning theory: concept, activity and culture are marked in simulation exercises. Concept relates to the existent knowledge or experience the individual possesses, activity involves the interpretation and use of such knowledge or experience, and the culture the context or environment in which this process takes place. It is important to remark that the culture, or environment to which the participants will be exposed is related to cyber related incidents, but on the strategic level where decisions have to be made, this note also digs over the integration of learning theories to the TTX. Combining the learning by doing achieves what the simulation is all about, and the participants decide on what can be a challenge then or in the future. They could also recreate a challenge that took place in the past because the decisions and actions that followed at that moment were not the most appropriate ones, or on the contrary, because they generated excellent results and became exemplary. It may be worth to immerse the participants in both types of scenarios, to learn via comparison. The performance of groups and participants is defined by the specific situation that the exercise presents progressively, this is how the culture element would come into the play through the specific environment with the characteristics it represents.

The TTX shall provide participants an opportunity to confront the shortcomings of the decision making process in cyber related incidents, it commands to play the assigned role during the game, so the nature and structure of the exercise requires active participation and serious involvement in the situations that the scenario proposes. Engagement gains importance in order to overcome successfully the challenges and solve problematic situations by opting for the most appropriate decision. When achieved, engagement diminishes boredom common in traditional learning contexts and increases enjoyment during the learning process, which implies there was interest and attention paid to the case.

Bloom’s Revised Taxonomy of Educational Objectives was used in this study as an assessment framework to categorize the learning outcomes of TTXs. The model possesses elements that add value to the learning process conferring comparative advantages that traditional education models do not have. To instruct strategic decision making for cybersecurity purposes, the TTXs should be more engaging and cause a significant impact on the learner. The lower levels of the revised taxonomy (Remember, Understand) are the foundation of knowledge and come first in the learning scale/process. The taxonomy is constructive in a way that each level builds upon the preceding and supports the next. The middle levels (Apply, Analyze) allow the use of concepts and imply understanding in problem solving, adaptation to contexts, appreciation for the parts and the whole of any given situation and logical dissemination of the information that is being obtained. The higher levels (Evaluate, Create) activates the learner's capacity to judge, and evaluate, giving rise to the formulation and production of creative solutions, transformed products, new tools, etc.

TTXs can scaffold learning in analogous ways a methodology based on the taxonomy would, but progressing through role-playing. The way the theory translates into practice, contributing to decision making processes in cyber related incidents, is when participants discover the meaning of what goes on during a crisis and how it is happening; having to decide over incidents; breaking information pieces or reconstructing the whole picture based on pieces for analysis on effects; thinking about the consequences and impact of such decisions; and identifying systemic weaknesses on the legal frameworks, cooperation, communication channels, roles and responsibilities. The exercise should result into creative "products" that could remedy the existent flaws and shortcomings and prevent the damage that cyber-attacks may cause as well as prepare for solutions if harm cannot be prevented.

4.2 TTX Case Study 1 – National Level

This case study consisted of a TTX that focused on strategic decision-making during cyber related incidents. The simulation was conducted with participants from a European Country, under the auspice of the ministries of defense of the country and Estonia. The exercise was part of a training project that the Cyber Security Consultancy firm, BHC Laboratory, developed and administered.[1] Similar exercises have been conducted in different countries around the world with comparable set ups. The description and dynamics of the exercise used during this first simulation are presented first, and a section with the observations, findings and discussion follows. The main sources of information and data, besides the documents objects of analysis, were the participants.

Description and Dynamics of the Exercise

The TTX in which the participation and observation was held belongs to a private Estonian cyber security laboratory, involved with exercises and cyber ranges. The first interaction exercise of this company where simulations of cyber security crisis and strategic decision-making were proposed took place in 2012. These simulations now are based on a model scenario and set up where strategic decision-making is assessed. The goal is to experience the events and incidents presented in a simple to complex flow, and exploring teamwork capacities. The environment and general scenario conditions is the same for all teams but each working group, while exposed to the same event, receives details that are relevant to the role being played. Every group has to decide on the information that was specifically dispensed by the facilitators and therefore engages differently towards the outcome.

The exercise is geared to assist strategic decision makers, which means that it is not presumed or required that the participants have a technical background. (In real life situations senior level decision-makers face situations where they must decide on issues that involve technical or very specific expertise they hardly ever possess). Besides, the exercise is focused on policy issues and the decision making process during crises such as one caused by large-scale cyber-attacks. The common response to a cyber crisis tends to rely on technical capabilities, and this is why strengthening the human, social and organizational component or crisis management competences becomes crucial. Important decisions that affect different sectors, and may or not be described in regulations or standards have to be taken and implemented. In attention to these sectors and most stakeholders, the exercise proposes a division of the participants into 4 groups of influence that would be identified with the functions and capacities required to perform realistically: Central Government; Military and Intelligence; Police and Justice; and, the Private Sector.

The exercise foresees that discussions are to take place within the groups and communication will need to be maintained across groups as well. The organizers assist and support the information exchange dynamics throughout the session. Two types of questions

[1] Consult the company's site at
http://bhclab.com

are asked during each incident presented by the scenario: substantive that are asked first, and framework questions that are elaborated upon second.

Examples of Substantive Question are:

- How does the group decide over a particular situation? (on the payment of ransomware, should it be paid or not? Must a web domain be brought down and/or restored?)

Examples of framework questions are:

- How long in your country or organization this decision would realistically take?
- Are decisions and processes confidential? Are they public or classified; if classified, on what level, and what were the basis for such decision?
- Whom do you cooperate with (at the national and international levels if that is the case), and what is your preferred cooperation mechanism?
- Who holds the authority to decide, in what cases, and why?

The event was held in the National Military Academy of the Country with 47 participants representing the Ministry of Defense (MOD), North Atlantic Treaty Organization members (NATO), The Country's Armed Forces; MOD, the State Security and Crisis Management Council; the Parliament; the Ministries of Finance, Justice, Foreign Affairs, and Energy, and, the Government Special Communication Agency.

The TTX was conceived to last two days. During the first, the scenario was presented and played between 09:30 and 18:30. The second day, consisted on a coached reflection, a feedback session and a series of talks regarding cybersecurity strategy policy development. These last covered legal issues of cybersecurity regulations in the country and the current threat environment.

For the TTX, the participants were divided into the groups, taking into consideration their actual working responsibilities. The first group represented the Central Government, the ministry of foreign affairs and also the parliament; group two had representatives from the military and intelligence agencies; the third group held the role of the Police, the ministries of Justice and internal affairs and the last group represented the private sector.

Observations: Findings and Discussion

The observation method allowed an unobtrusive groupal interaction with the participants and direct one to one conversation. These volunteered testimonies took place during exercise and later, when the feedback session was held. The researcher focused on observation, and a line of inquiry that repeated each time contact took place. The same question was presented in the same manner, according to the same approach and text. The process lasted as long as the exercise did and up to 2 minutes long. The observation went according to the standard methodological practices as follows:

After a personal introduction, the group was informed about the role and activities that the researcher was going to be performing, the purposes of the study, and formalities of the method. An explicit mention on that any interaction is voluntary was added. The participants were told that the data and information or testimony provided was going to remain anonymous and is very much appreciated.

The researcher focused on taking notes, writing comments and expressions, and understanding the participants' thoughts, perceptions, concerns, needs and reactions about the TTX. Signs of interest, active participation (constant discussion), engagement (total involvement and immersion in the scenario), involvement (constant solutions for decision making in the scenario), and leadership (leads on the decision making process, and agreement within the group) were recorded to determine the relevance of the simulation for the trainees and the impact of this training model in terms of helping the participants upgrade their cognitive development (Bloom's Revised Taxonomy of Educational Objectives), and increased engagement. The comments on the exercise were positive. The inquiry was unstructured but based on preconceived theoretical assumptions embedded on a list of questions that were responded during a conversational exchange with the participants. All data collected consisted on natural thoughts and personal accounts about the exercise rather than an organized list of responses. Nevertheless, the information provided in this manner reinforces even more persuasively, the theory integration efforts consigned on this thesis that argue the convergence of concepts from different disciplines into the TTX.

The observations together with the feedback collected directly from the participants, allowed to draw that people were interested, motivated, engaged, and understood the challenges they were facing. The TTX also made it clear what are some of the security flaws prevailing in their organization and the relevance of strategic decision-making competences during cyber related incidents. The testimony of the following participants is representative of the opinions expressed by the group: P25 stated that "*the exercise is interesting, and interactive, I love it. It is very realistic, innovative, easy to follow and involving. Relevant and significant for decision makers and opened my eyes to the potential of cyber threats. This is the best experience I have had so far in my years of training*"; P15 said "*the TTX is realistic and interesting, dealing with this kind of problems brings forward the participants to appreciate the importance of strategic decision making, it is a very good experience*"; and, P36 added that "*This is how decision making training should be addressed, the technical have many tools and have developed many skills, the strategic field has being forgotten, this experience is significant to improve our actual organization, legislation and procedures*".

In respect to the organization and delivery of the TTX, including the facilitation and coaching, the feedback revealed that it was a very well runned exercise, participants mostly agreed on the observations that were pointed out, understanding how everything is related and the effects that cyber related events can pose to the national picture, the potential critical challenges that arise proceeding from cyberspace and the useful and relevant experience that the exercise came out to be.

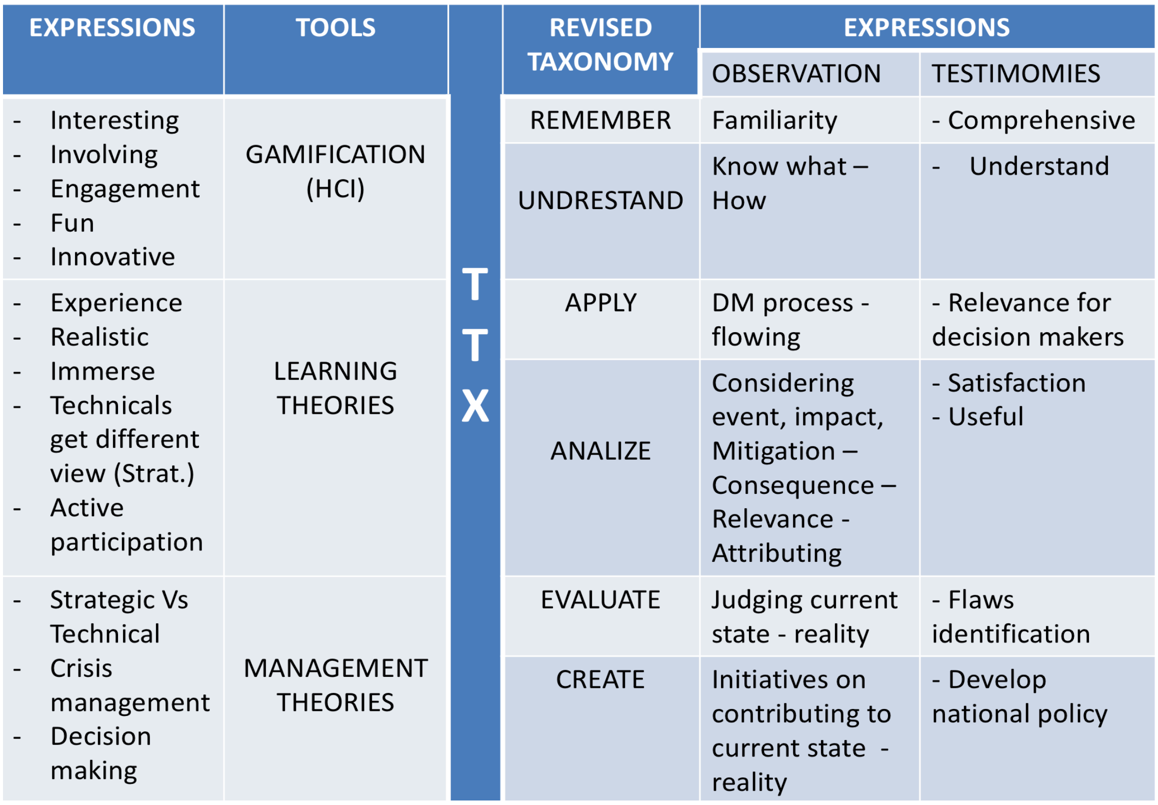
The testimonies were characterized by repetition of certain expressions, which were used as codes, further permitting the detection of categories of reactions and the associations between words, and the converging disciplines. Table 5, can explain the connections between the theory and the practice, suggesting the impact that the simulation had on the groups.

Table 5: Expressions. And connection to disciplines I

Expression	**Theory & science - domain**	**Explanation**
Interesting Role play Fun Innovative Engagement	Gamification (Computer Science - HCI)	Catchy, involving (observed and reported), bringing game elements into the play when assuming a specific role on the TTX, killing the usual boredom engaging users and providing fun, overcoming the shortcomings of traditional learning models.
Discussion Realistic	Situated Cognition (Cognitive Science)	Placing the participants under pressure, believable context for example lack of information, time constraints and threats are present. Promotion of discussion, contradiction and debate in the decision making process.
DM learn DM Experience	Experiential Learning (Cognitive Science)	Learning by doing, enhance DM process making decisions in a realistic possible crisis situation.
Strategic Vs Technical Strategy Importance Cooperation	Management (Management Science)	Focus on DM hence they hold responsibility for actions during a cyber crisis offers the technology experts a new political perspective and vice versa. The assistance and alliances are encouraged during the TTX.
Relevance for DM Develop Nat. Policy Understanding Comprehensive Satisfaction Flaws Identification Useful Significance	Revised Taxonomy (Cognitive Science)	Complete cognitive learning process involving the six levels from the taxonomy. Achieving the know what - how, in the crisis situation, proposing solutions for such event, analyzing effects and consequences, identifying flaws and suggesting new improvements after experience. Very good acceptance from the participants.
Active participation Interactive	Gamification & Experiential Learning (Computer – HCI & Cognitive Science)	Constant involvement of participants in every event in a flowing scenario development.
Leader	Situated Cognition & Management (Cognitive & Management Science)	Need and presence of leaders to lead the way, not always chosen but rather accepted.
Immerse Involving	Gamification & Situated Cognition (Computer HCI & Cognitive Science)	Taking the participants into the flowing scenario in a realistic and engaging way.
Complexity	Revised Taxonomy & Management(Cognitive & Management Science)	Judging the events and triggered reactions, under the presence of crisis standards
Key players Problem dealing	Gamification & Management (Computer – HCI & Management Science)	Vital stakeholders in the DM process in a cyber crisis, role-play the complex evolving scenario trying to solve the issues that arise.

The first column lists the word codes under the title “Expressions”, that associate to the theories on the second column that has the title “Science Domain”. The last, with the title “Explanation”, shows the experience in context, for better understanding of the effects of the exercise. The highlighted concepts, embedded into the exercise innovate, increase engagement, simulate the experience of the real world and push the development of a crisis situation.

The effectiveness of the TTX is legitimized by the use of Bloom’s Revised Taxonomy of Educational Objectives as an assessment framework and progressing scaffolding methodology for achieving advanced learning objectives. Figure 6 illustrates the convergence of disciplines into TTXs explaining learning outcomes in a national simulation case.



EXPRESSIONS	TOOLS		REVISED TAXONOMY	EXPRESSIONS	
				OBSERVATION	TESTIMOMIES
- Interesting - Involving - Engagement - Fun - Innovative	GAMIFICATION (HCI)	T T X	REMEMBER	Familiarity	- Comprehensive
			UNDRESTAND	Know what – How	- Understand
- Experience - Realistic - Immerse - Technicals get different view (Strat.) - Active participation	LEARNING THEORIES		APPLY	DM process - flowing	- Relevance for decision makers
			ANALIZE	Considering event, impact, Mitigation – Consequence – Relevance - Attributing	- Satisfaction - Useful
- Strategic Vs Technical - Crisis management - Decision making	MANAGEMENT THEORIES		EVALUATE	Judging current state - reality	- Flaws identification
			CREATE	Initiatives on contributing to current state - reality	- Develop national policy

Figure 5: Learning assessment under the Revised Taxonomy of Educational Objectives

The learning outcomes illustrated in Figure 5 towards the right of the table, show that the simulation experiences bear the progression to the highest cognitive levels according to Bloom’s Revised Taxonomy of Educational Objectives (explained in detail in section 4.1, page 24). The left side of the table replicates in brief the categories used to analyze observation results, because they converge on the TTX, that is marked in the middle column. The observations and testimonies together are located next to the learning objective that the groups showed to have reached. The claims of the thesis are demonstrated on theoretical and empirical grounds. The Awareness of the potential threats, as their arise in the given scenario correspond to remembering and the understanding upon which decisions were planned and made. The events that unfolded were perceived and thus, the abilities to apply the concepts to the concrete case could also be evidenced. The analytical skills were verified once participants could differentiate the parts from the whole and determine what were the effects, impact, relevance and consequences of cyber incidents. Clarified this information, a proper judgment of the schemes and conditions surrounding each team became possible. At this point the participants were able to self-reflect identifying flaws, poorly plan aspects, unnoticed threats, legislation gaps, problematic cooperation and communication patterns, and ultimately evidence their lack of strategic management competences when handling cyber crisis decision making. Advances onto the highest level of creativity were manifest on testimonies about the development of national policy. The point of convergence after the TTX experience were focused on the creation, enhancement and rehearsal of plans, a more complete understanding and awareness of the potential challenges in a cyber crisis, proposals of legislation and modifications to the existent one, leads to improve the cooperation and communication channels on national and international level, and awareness and consideration of importance of strategic decision making in cyber related incidents. During the exercise, observations sought to detect the presence of the concepts that were integrated into the TTX, focusing on interactions, behaviors and attitudes. Signs of engagement were noticed from the onset, it was seen that the participants were interested, curious and aware about the incidents and the impact they could have on the state level. Actively discussing every event resulted in tensions derived from a power struggle within each working group. Some members within the groups exhibited their status and tried to impose decisions in disregard of the rest of the capacities of other team members. Settling internal working group disputes did not seem an easy task to accomplish. Agreements, in the larger group, between the teams were not easily accomplished either if at all. The factors that kept participants focused during the exercise were a sustained time pressure, the constant need for interaction, the injects posing dilemmas that required decisive action, and the agreement process within the groups, which was difficult to achieve. The participants with technical backgrounds leaned towards technical solutions without foreseeing the implications that these may entail, participants with the expertise in other fields do not have the capacity to elaborate on the technical aspects at play. These two categories fail to assess the complexities of the domains other than theirs but the majority of participants possessed no technical background.

A scale of “0” to “5” was used to determine engagement. It was based on the involvement during each discussion, the commitment in trying to agree on the decisions to be made, and the interest perceived. The engagement ranking scale kept a nominal track where “0” was the lowest ranking value assigned to participants who withdraw or do not contribute to the exercise and lack all interest; “1” is given to participation (interest) without involvement; “2” designates interest and passive involvement; “3” is the value assigned for active participation without commitment to lead on decisions making; “4” is assigned to people who contributes to decision making processes; and, “5” being the highest score, is reserved for participants who play their roles actively, become leaders within the teams, and plan, propose and decide. The records obtained show that 0% of participants obtained a “0” and “1” mark; 2.12% of participants obtained a “2” mark; 4.25% of participants obtained a “3” mark; 6.38% of participants obtained a “4” mark; and, 87.23% of participants obtained a “5” mark. Table 6 shows the participants engagement levels.

Table 6: Participants engagement ranking scale for the National level TTX.

Team and participants	**Ranking Scale**					
	0	**1**	**2**	**3**	**4**	**5**
Team 1 = 11 members	0	0	0	0	2	9
Team 2 = 14 members	0	0	0	1	0	13
Team 3 = 11 members	0	0	0	0	0	11
Team 4 = 11 members	0	0	1	1	1	8
Total = 47 participants	0%	0%	2.12%	4.25%	6.38%	87.23%

Considering the organization this country has developed in the cybersecurity field, it became evident during the exercise and the feedback session that the communication channels were not established, the position or person with the right and authority to make decisions in the kind of cyber related incidents presented by the scenario was also not clear, and the huge effect that this cyber incident can cause in the bigger was also not quite clear. The decisions were pushed to higher instances with the complexity evolution of the scenario, the time for response (decision making) was expected to be shorter, the involvement of national and international organizations was stronger and the information acquired the highest level of classification.

To conclude the description, observation, analysis and discussion of this chapter, the interdisciplinary approach proposed in the previous chapter was legitimized. The concepts of experience and feedback from experiential learning theory, the concepts of culture and learning by doing from the situated cognition theory, both theories from the cognitive sciences. The crisis management and OODA Loop concepts from the management theories and science, and the engagement and role-playing concepts from gamification theory and computer science are contained in the TTX. The learning outcomes and effectiveness of the TTX, assessed through the employment of Bloom's Revised Taxonomy of Educational Objectives, also suggested the great value that TTXs can pose to strategic decision making in cyber related incidents, regarding training and education strategies. Furthermore, the data dispatched in this text could present great value to parties interested in this topic.

4.3 TTX Case Study 2 – International Level

This case study consisted in the conduction and facilitation of the first run of the Locked Shields Strategic Track Exercise (LSSTE) that focused on strategic decision-making during cyber related incidents. This TTX was proposed by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) and administered by BHC Laboratory and the CCDCOE between the 27 and 28 of April 2016. The methodological approach and process of data collection was planned and performed according to the same standards and practices that were applied during the first simulation exercise. In the following, a description and dynamics of the exercise will be presented, followed by a section with the corresponding observations, findings and discussion.

Description and Dynamics of the Exercise

The LSSTE is a TTX that simulates a scenario of an escalating cyber crisis, designed to recreate complex decision making processes occurring at the inter-state level. This TTX can be divided into four phases: Planning, design, conduction and evaluation. The exercise seeks to increase awareness and skills in decision makers with involvement in cyber related incidents responses hence it is poorly addressed and experienced, considering the lack or nonexistence training and education strategies for such grounds and it is as crucial as the technical capabilities tackling threats emanating from cyberspace. The specific goals of this simulation were listed on as follows:

1. "To develop insight and awareness of the consequences of cyber incidents on the national and international decision making processes,
2. To gain insight into the complexities of national and NATO wide decision-making processes in response to cyber-attacks,
3. To gain insight into the role of civilian and private entities in these processes;

4. To gain insight into the temporal elements of the response to a cyber-attack (i.e., will decision making processes be able to keep up with which the technical scenario that develops?),
5. To compare decisions and processes between the technical and strategic teams,
6. To compare variations in national decisions."

Seven (7) countries (United States, Czech Republic, Finland, Netherlands, Estonia, Switzerland and United Kingdom), participated in this international level TTX. The exercise asked each participating state to build a team and to provide an official response to the crisis, while articulating other coordinated reactions to the incidents the scenario presents on injects. This international TTX was designed by BHC and the CCDCOE around the technical specifications (technologies, networks and attack methods) that the Locked Shields technical exercise 2016 (LSTE) had used. To take part of the exercise, participating states had to send at least two (2) representatives from the crisis coordination department of the country and the MOD, a legal advisor with expertise on crisis response (protocols, procedures and rules of engagement), and a cybersecurity crisis response individual knowledgeable on policy. The exercise is conducted in a webmail environment, with the injects and situational reports being delivered through email within a secure NATO CCDCOE Wi-Fi environment, thus participants had to use their own computers.

The exercise was held in a local hotel and lasted a day and a half. The exercise took place on the first day while the second was devoted to a feedback session where the results were discussed with the participants. One of the challenges of the strategic LSSTE 2016 is to present a scenario that could convincingly reflect the strains and complexities that strategic decision makers should face when in the presence of a crisis that is determined by technical factors in the way the LSTE 2016 embarks on.

A short introduction is presented to the participants on the details about the logistics of the TTX as well as instructions on how the simulation will progress such as the escalation of incidents that will complicate the decision making process. Similarly, to the TTX case study 1 at the National level, to every inject two type of answers must follow, one on substance and the other concerning decision making framework issues.

The exercise was to be managed by a so-called White Team that administers the events. Although this group does not have a fixed numeric composition, this proposal involved a team leader, a media expert, a legal expert, technical experts and up to seven assistants and observers. Inputs delivered in the format of a situational report from every incident proposed by the scenario were, for instance: By whom and at what level? What are the implications of decisions? How will it impact mission, society and government?

The exercise is meant to assess stress levels, disagreement within the groups, time constraints during the decision-making process and courses of action considered before every decision. The scenario is composed by 7 stages that escalate in a constructive sequence where complexity is increased on every stage.

Media is assigned an especially important role in the exercise. The media expert and assistants should apply pressure on the groups as the scenario unfolds. The response assessment on this variable was constructed by the expert taking part in this TTXs on the basis of six criteria: transparency, self-interest, accuracy, consistency, newsworthiness and media friendly format.

The exercise evaluation phase is based on the discussion and feedback collected from the participants that follows a visualized explanation with the records from the previous day. The comparative analysis on the responses implemented by each team is relevant to highlight the legal framework available, and the existence of cooperation schemes that could be used during the decision making processes in cyber related incidents.

Observations: Findings and Discussion

Also for this exercise, the observation method was selected for the convenience and idoneity in the data collection process. The observations' criteria was planned and developed obeying to the same considerations that framed the case study 1 (National level exercise explained in section 4.2). The researcher was also focused on taking notes, writing comments and expressions, and understanding the participants' thoughts, perceptions, concerns, needs and reactions about the TTX. Signs of interest, active participation (constant discussion), engagement (total involvement and immersion in the scenario), involvement (constant solutions for decision making in the scenario), and leadership (leads on the decision making process, and agreement within the group) were recorded to determine the relevance of the simulation for the trainees and the impact of this training model in terms of helping the participants upgrade their cognitive development (Bloom's Revised Taxonomy of Educational Objectives), and increased engagement.

The White Team and participants appeared satisfied with the exercise if to take into account the comments expressed during the debriefing or evaluation phase where feedback was exchanged between the groups. For instance, P2 from Team 1 stated *"this is a challenging scenario, time pressure and acceleration catch all of our attention and efforts, it is quite fun. The complexity raises the insight in terms of technical Vs strategic. We are definitely learning a lot."* and P1 from Team 2 said *"awesome experience, very well runned, the flow of information is great and we love the format of the game"*. Participants from every team discussed the performances of others and offered the recommendations to the organizing team to have all decisions taken, the outcomes and other reflections around the injects reviewed. A closer look at all actions during the TTX would, in their opinion, effectivize the learning and capacities building potential of the experience. These observations, together with the feedback collected from the participants, allowed to conclude that people were interested, motivated, engaged, and understood the challenges they were facing.

The first observations recorded are on the composition of teams. The requirements on participation were not met by three of the teams that composed the group in the absence or excess of what was indicated. While the White team expected to work with 28 official representatives, 26 were present. More pressure and workload distinguished the experience of those teams with less members although it appeared that this did not interfere with a good performance. Every participating country operated within their decision making frameworks and based on their crisis management procedures and standards. All the participants played along, and according to their roles, adapting to the scenario with no apparent difficulties processing the injects provided by the white team.

The results presented in a table format, were too elaborated under the same criteria applied to the case study 1 (National level exercise explained in section 4.2). Testimonies were characterized by the repetition of certain expressions which were used as codes, which allowed the detection of categories of reactions, and association between words and the disciplines shown to converge on a TTX exercise. The results can explain the connections between the theory and the practice, suggesting the impact that the simulation had on the groups, as illustrated in Table 7.

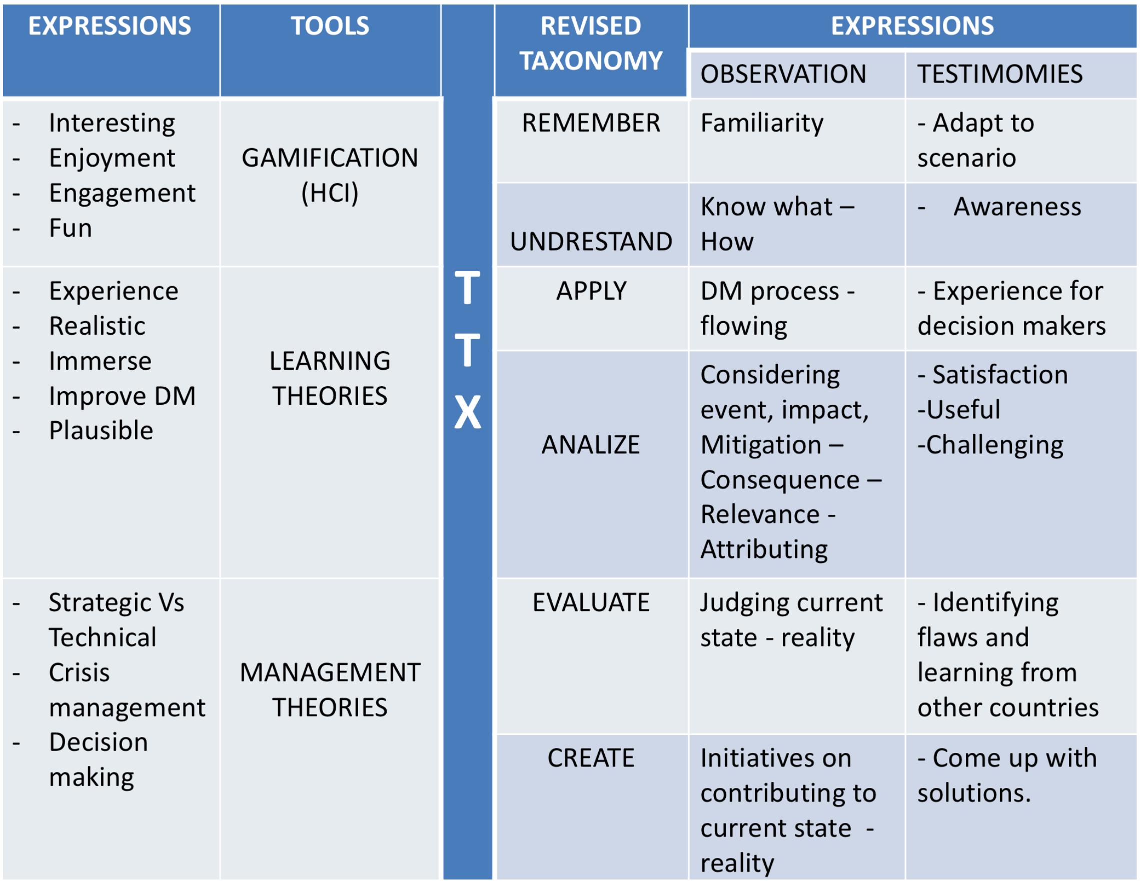
Table 7: Expressions and connection to disciplines II

Expression	**Theory & science - domain**	**Explanation**
Engagement Fun Role play Enjoyment Interesting	Gamification (Computer Science - HCI)	Catchy, involving (observed and reported), bringing game elements into the play when assuming a specific role on the TTX, killing the usual boredom engaging users and providing fun, overcoming the shortcomings of traditional learning models.
Realistic Discussion Plausible Immersion	Situated Cognition (Cognitive Science)	Placing the participants under pressure, believable context for example lack of information, time constraints and threats are present. Promotion of discussion, contradiction and debate in the decision making process.
Experience Improve making decisions	Experiential Learning (Cognitive Science)	Learning by doing, enhance DM process making decisions in a realistic possible crisis situation.
Strategic Vs Technical Crisis Management Decision making	Management (Management Science)	Focus on DM hence they hold responsibility for actions during a cyber crisis offers the technology experts a new political perspective and vice versa. The assistance and alliances are encouraged during the TTX.
Complex Challenging Learning Raise insight Relevant Useful Awareness Big Potential Come up with solutions	Revised Taxonomy (Cognitive Science)	Complete cognitive learning process involving the six levels from the taxonomy. Achieving the know what - how, in the crisis situation, proposing solutions for such event, analyzing effects and consequences, identifying flaws and suggesting new improvements after experience. Very good acceptance from the participants.
Placing people in real cyber crisis situation	Situated Cognition & Experiential Learning (Cognitive Science)	Exposing the participant to the environment in which a cyber crisis would evolve in, allowing the experience of such complex scenario.
Pressure Cooperation Pushing	Situated Cognition & Management (Cognitive & Management Science)	Some of the elements that characterize a crisis shape the decision making process.
Education Opportunity	Revised Taxonomy, Situated Cognition & Experiential Learning (Cognitive Science)	Offering a realistic environment to learn, actually doing what is expected from a decision maker in a crisis and gazing at the

In this table too, the first column lists the word codes under the title “Expressions”, that associate to the theories on the second column that has the title “Science Domain”. The last, with the title “Explanation”, shows the experience in context, for better understanding of the effects of the exercise. Results are quite similar to the case study 1 (national level exercise), many words and expressions were repeatedly mentioned by participants on both experiences. There were also new words and expressions, which also committed to the interdisciplinary efforts revealing the convergence of disciplines in the TTX. The highlighted concepts, embedded into the exercise innovate, increase engagement, simulate the experience of the real world and push the development of a crisis situation.

The results of the method differ from the national level exercise's results very little, corroborating the assumptions that are upheld in this work. The same words and expressions were repeated by participants on both simulations and although new words and expressions were detected in the analysis of this second TTX. For instance, unlike in the first case, after this exercise, "Enjoyment" came up, but it too relates to HCI; "Plausible", "Immersion", "Complex", "Challenging", "Learning", "Raise insight", "Big Potential" and "Come up with Solutions" are all new but they all are associated to the learning theories revised from the cognitive sciences, and so forth. Being committed to the same fields shows once more the convergence of disciplines in the TTX. The highlighted concepts, embedded into the exercise innovate, increase engagement, simulate the experience of the real world and push the development of a crisis situation to which the participants could relate.

The effectiveness of the TTX is legitimized by the use of Bloom's Revised Taxonomy of Educational Objectives as an assessment framework and progressing scaffolding methodology for achieving advanced learning objectives. Figure 6 illustrates the convergence of disciplines into TTXs explaining learning outcomes in the international simulation case.



EXPRESSIONS	TOOLS		REVISED TAXONOMY	EXPRESSIONS	
				OBSERVATION	TESTIMOMIES
- Interesting - Enjoyment - Engagement - Fun	GAMIFICATION (HCI)	TTX	REMEMBER	Familiarity	- Adapt to scenario
			UNDRESTAND	Know what – How	- Awareness
- Experience - Realistic - Immerse - Improve DM - Plausible	LEARNING THEORIES		APPLY	DM process - flowing	- Experience for decision makers
			ANALIZE	Considering event, impact, Mitigation – Consequence – Relevance - Attributing	- Satisfaction -Useful -Challenging
- Strategic Vs Technical - Crisis management - Decision making	MANAGEMENT THEORIES		EVALUATE	Judging current state - reality	- Identifying flaws and learning from other countries
			CREATE	Initiatives on contributing to current state - reality	- Come up with solutions.

Figure 6: Learning assessment under the Revised Taxonomy of Educational Objectives

The learning outcomes illustrated in Figure 6 towards the right of the table, show that the simulation experiences bear the progression to the highest cognitive levels according to the Revised Taxonomy of Educational Objectives (explained in detail in section 4.1, page 24).

The left side of the table replicates in brief the categories used to analyze observation results, because they converge on the TTX, that is marked in the middle column. The observations and testimonies together are located next to the learning objective that the groups showed to have reached. The testimonies of the TTX Case Study II-International level demonstrate that this does not differ in intensity or meaning from the earlier case discussed, even if the expressions and words utilized by the participants were not the same. The claims of the thesis are confirmed on theoretical and empirical grounds. The design of both exercises conceived the achievement of the highest cognitive levels under the light of Bloom's Revised Taxonomy of Educational Objectives.

The Awareness of the potential threats, as their arise in the given scenario correspond to remembering and the understanding upon which decisions were planned and made. The events that unfolded were perceived and thus, the abilities to apply the concepts to the concrete could also be evidenced. The analytical skills were verified once participants could differentiate the parts from the whole and determine what were the effects, impact, relevance and consequences of cyber incidents. Clarified this information, a proper judgment of the schemes and conditions surrounding each team became possible. At this point the participants were able to self-reflect identifying flaws, poorly plan aspects, unnoticed threats, legislation gaps, problematic cooperation and communication patterns, and ultimately evidence their lack of strategic management competences when handling cyber crisis decision making. Advances onto the highest level of creativity were manifest on testimonies about the search for novel solutions.

It was observable that during this second exercise, contrasting with the first, the countries assumed the roles without struggling with internal divisions, unified. Nevertheless, the tendency in which decision making during cyber crisis is forwarded to the higher authorities, under the most classified information considerations, with expectations for the minimum time on response (decision making), and involving national and international organizations, was confirmed in the TTX Case Study II-International level. That shortcomings exist in traditional education models in the field of strategic decision making during crises can be safely concluded. In some educational systems this type of training is not even available, especially for cyber security enhancement purposes.

Continuous involvement characterized the LSSTE; From the commencement of the exercise the groups discussed, were enthusiastic and engaged with the TTX. The factors that kept the teams focused were controlled by the administrators: sustained time pressure, and exposure to hypothetical but plausible situations mainly. Time management was noted and recorded as a constant difficulty in all groups, the observations include 2 examples. One on the inability to cope with the rapid development of events, a the second on the uninterrupted string of incentives and communication. The observations also include that participants were stressed and motivated to plan and decide but had no time to consider options, becoming uncreative and responding in predictable ways The first and last three (3) stages of the scenario seemed to cause the most stress to participants of this TTX, the participants evidenced rush, and had to rationalize their involvement because of the lack of time, also the feedback collected and presented during the second day by the White Team brought out the same. This argument was also evidenced in the feedback session. The timing and pace of the events ran exactly as planned to recreate a realistic crisis scenario. In addition, this pace disallowed participants from attending some other activities.

The nominal range scale employed in section 4.2 explained in p.30 was also used to rank the participants' engagement in this case. Table 8 shows the participants engagement levels.

Table 8: Participants engagement ranking scale for the LSSTE.

Team and participants	**Ranking Scale**					
	0	**1**	**2**	**3**	**4**	**5**
Team 1 = 4 members	0	0	0	0	1	3
Team 2 = 2 members	0	0	0	0	0	2
Team 3 = 4 members	0	0	0	0	1	3
Team 4 = 4 members	0	0	0	0	0	4
Team 5 = 5 members	0	0	0	0	0	5
Team 6 = 3 members	0	0	0	0	0	3
Team 7 = 4 members	0	0	0	0	0	4
Total = 26 members	0%	0%	0%	0%	7.69%	92.30%

The table shows the records obtained throughout the exercise in the rating scale in six columns per team and percentages at the bottom, showing that 0% of participants were assigned "0", "1", "2", and "3" marks, implying that the minimum actual engagement during this exercise marked already high in the general scale: 7.69% of participants obtained a "4" mark, active participation and contribution to decision making while 92.3% of the participants obtained the maximum mark, a "5" because of the active role they played, leading strategic decision making processes with proposals and decisive choices.

Comparing the two (2) exercises, in what respects participants' engagement ranking scales (study case 1-2), it could be argued that the smaller the groups the more engaging the exercise may become. Even though the results on both experiences show high levels of engagement, the study case 2, ranked higher possibly due to the commitment that can be reached when teams are composed by fewer members that must collaborate towards the same ends like the work style of this experience imposed as the TTX unfolded. Another comparable set of observations regard the patterns for assigning responsibilities within teams and valuation of the course of actions. As the scenario unfolded and complexity levels rose teams preferred to leave decision-making responsibilities to the highest instances possible, which delayed the response as more time is required in those cases. The TTX Case Study I-National level displayed the same tendencies. Similarly, and also coinciding, the interest in other stakeholders' involvement delays the response and reactions while sacrificing confidentiality (because of the need for information sharing, cooperation and collaboration), but the participants expect to maintain the maximum level of confidentiality while wishing to interact with the most possible international and national organizations. These contradictory expectations show that the goals and needs of the teams were incompatible and to reframe the evaluation given to these simulation components, strategic decision making competences must be enhanced. A more efficient strategic decision making move during a crisis would involve lower level decision makers' empowerment, that can produce faster responses, and that confidentiality would only be sacrificed to the degree that can be proven to favor cooperation.

The opportunity to expose themselves to hypothetical realistic and plausible cyber crisis situations offered by the TTX was appreciated by the participants, that explicitly brought up the concepts of awareness, understanding, experience, improvement, solutions, big potential, learning and education among many others that were collected not only during the conversations with the observer but also picked up while the events were taking place. Only one group refrained from volunteering comments. All of the rest, by the other participants, are registered in the observation notes. A great diversity of crisis management styles was observable. Every country approached communication, cooperation, collaboration and interaction with others in particular ways but cultural variables and perspectives within groups were not variables that this study sought to estimate. On the notes few lines describe the attitude of some of the participants within groups, for example the ones that most respected or the most experienced. In team one, every participant seemed to feel at ease, playing the roles vividly and communicating extensively within and with others. This team also completed all tasks the first. This is not to mean that the team that came last presented a lower quality work. Understandably, to each country correspond unique priorities and considerations in the processes of reaching decisions as they were commanded to act in their best interest and respecting their own legal and political systems. This is also the reason why the observations remained such, neutral and objective, with no other pretension than analysing a phenomenon or situation without taking sides or allowing value judgments. Observation methods in qualitative research do not typically award points or reward participants. Also the TTX as methodological feature in principle does not have the capacity to issue an assessment. Designating winners and losers in strategic decision making is a superfluous task due to the multifaceted nature of the activity in itself. Strategic management theories and models are evaluated quantitatively only in time, and not primarily so. What really matters in the assessment of performance is the institutionalization degree that some models can reach, how these can potentialize the competences of stakeholders and the deep understanding of the factors affecting scenarios and agents, all in context During the LSSTE the teams were not competing and the state conditions or systems were not under scrutiny either. Each team is tasked to reflect on their own, whether improvements are needed and where, to further bring them in from the TTX experience into their national policies, practices or statutes and necessary independently.

In spite of the participation of seven (7) states with different organizations and sophistication levels in the cybersecurity area, the need to strengthen efforts in strategic decision-making training and education to deal with crisis was repeatedly remarked. This was noted during the feedback session of the LSSTE, replicating the discourse present in most National Cyber Security Strategies.

To conclude the method described and discussed in this section along with the case study 1, produced results that endorse the theoretical contributions of this research. Consequently, the interdisciplinary approach that this thesis proposes produces legitimate theory development. The experiential and situated cognition, management, and gamifications theories from the cognitive, management and computer sciences fields, converge in the TTX through the concept specified: experience and feedback; culture and learning by doing; crisis management and OODA Loop (strategic planning); and, engagement and role playing, respectively. The learning outcomes and effectiveness of the TTX, assessed with the help of Bloom’s Revised Taxonomy of Educational Objectives, underpin the value that TTXs have as training and educational models regarding strategic decision making competences for cybersecurity.

4.4 Modular Guide to Implementation of Strategic Decision-Making TTX

A modular guide for conceiving and helping to implement TTXs is presented in view of addressing the research task number two (2). The results should advance the institutionalization of gamification methods in educational and training programs in cyber security for Colombia, or elsewhere that may be deemed needed. In any case it is fundamental any methodological adoption to be based on theoretical and empirical evidence, not in trend alone.

The guide divides the process of implementation into four (4) main stages or modules, each containing several elements to choose from to complete tasks that the stage presupposes. This modular guide represents and embodies the concepts that the theoretical section identified and connects theory and practice. At the same time is a usable tool that makes the design process more efficient, when grouping the building blocks guarantees well established standards and principles in clear.

The guide is thought as a system of blocks so that the interested parties need to assemble, add a context and create their own TTX. The four modular categories are: Identification of goals objectives and scope; Planning upon considerations; Execution; Feedback and discussion.

Identification of Goals, Objectives and Scope

The establishment of the expected outcomes of a cyber related incident decision-making TTX, correspond to cognitive purposes but not only; Competences' enhancement is also compatible end. Vision on these respects are the first to consider

Table 9: Expected outcomes of a cyber related event decision-making TTX.

TTX Expected Outcomes	Revised Taxonomy
Enhance awareness and understanding of the potential challenges contained in the cyber realm.	LEVEL 1-2
Bring the participant into a potential real life scenario, experiencing the complexity of decision making in a cyber crisis.	LEVEL 1-2-3-4
Becoming aware of the existing legislation frameworks, identifying gaps if any and triggering intentions to strengthen them.	LEVEL 1-2-3-4-5-6
Create verify and/or enhance the national and international cooperation and communication channels.	LEVEL 1-2-3-4-5-6
Illustrate decisions between different stakeholders over same situation, motivating discussion and self-evaluation on current state stimulating novel solutions.	LEVEL 1-2-3-4-5-6

.

In the column on the left side the expected outcomes of a strategic decision making TTX are presented. On the right side each expected outcome is tied to the learning objectives from the revised taxonomy discussed in sections above. The alignment of the two would show at least the cognitive advancement achieved after the completion of the exercise.

The selection of the stakeholders that could become involved in a cyber related incident, is listed, indicating the decision making framework issues that may arise when the scenario develops. This step can help complete the assignation of roles and settings for cases when these are predetermined for the participants of the exercise. This choice is on the designers and developers of the simulation.

Table 10: Stakeholders of a cyber related event decision-making TTX.

Whom To Test	
Central Government	Authority, Cooperation, Timeline, Transparency
Justice (Ministry of Interior, Justice)	Authority, Cooperation, Timeline, Transparency
MOD (Military - Intelligence)	Authority, Cooperation, Timeline, Transparency
Private Sector (ISP, CI, Hospital, etc)	Authority, Cooperation, Timeline, Transparency

In the column on the left, the potential stakeholders are listed and on the column on the right are the links to the decision making framework issues that will likely arise in a pre-set scenario.

The Following figure illustrates the components contained in a cyber crisis and from where the decision making framework was adopted.

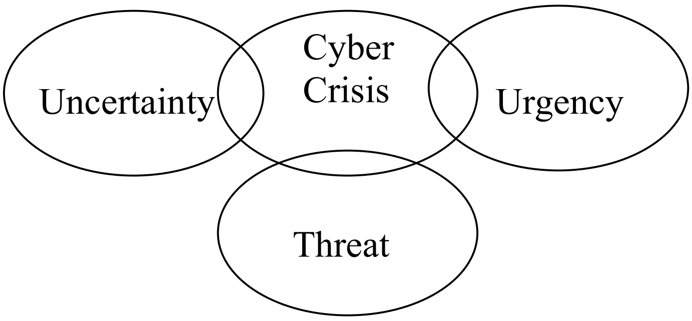


Figure 7: Cyber crisis components

Uncertainty refers to transparency, Urgency recalls for Timeline, and Threat concerns authority and cooperation. An extended explanation on these aspects is available in section 3 p.17.

After the adoption and processing of the components of a crisis, the establishment of the decision making framework in an exercise of this nature, is linked to the decision making framework issues that arise when the aforementioned scenario presents itself. Table 11, next summarizes the possibilities.

Table 11: Decision making framework of a cyber related event decision-making TTX.

What To Test - Decision Making Framework	
Authority	Who has the right and obligation to make decision
Cooperation	Nationally and internationally who else is involved
Transparency	Information classification (public, restricted, confidential, secret, ultra-secret)
Timeline	Real time for response

The arguments on the who and what to test, respectively derive from considering the parties that would be involved in the decision making process under a cyber crisis situation and the concept of crisis, in which a threat calls for a decision, who has the right and/or responsibility to make the decision? (Authority), and who else is involved in such decision? (Cooperation). The urgency for a decision to be made addresses the limited time in which decisions have to be made under a crisis situation (Timeline), and the uncertainty regards to constant need and right of information from citizens and stakeholders, but will the information be public, restricted, confidential, secret, ultra-secret? (Uncertainty). In this last element media plays a very important role and can influence up to some point the decision making process. Figure 8, below presents the interconnections of the considerations on this stage.

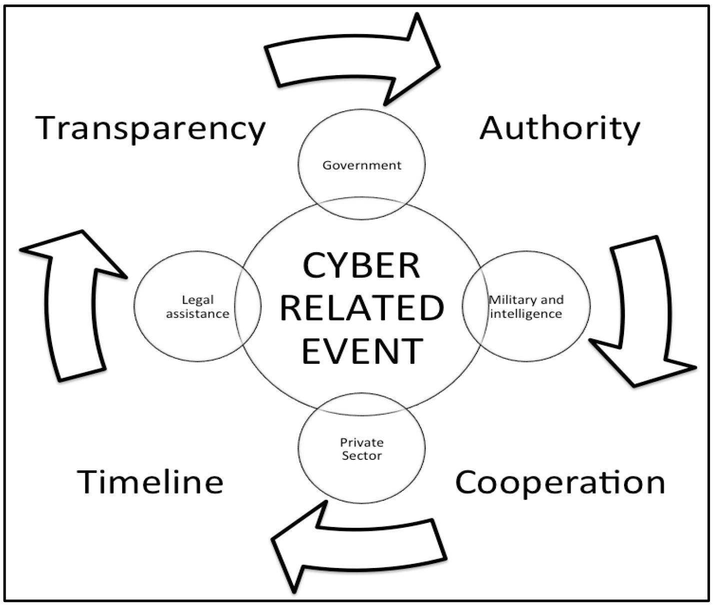


Figure 8: Cyber crisis flow

Planning Upon Considerations

Building the experience should prepare for a realistic scenario in order to engage participants without interfering with the engagement features of the TTX. The participants should not be given incentives to discuss/doubt the scenario. A balance should be reached ensuring that the flow of the TTX is maintained and the stress levels and pressure on the participants could be escalated across constructive learning tasks. Manageable situations should become more complex ones. To achieve one of the objectives of the specific model in Table 12, it has to have international reach. This basic components chart was built on the basis of the state level events that have taken place already and on the actual trends and current global concerns of the international community. With the selection of components from each column together incidents or events can be formulated as injects. The incidents will bring up issues for discussion and decision making throughout the TTX.

Table 12: Component chart for scenario building of a cyber related event decision-making TTX.

Building The Scenario			
Possible Authors	**Attacks**	**Trends**	**Targets**
NATIONAL LEVEL / INTERNATIONAL LEVEL			
❏ Criminals ❏ Terrorists ❏ Patriot hackers ❏ Hacker groups ❏ Hacktivism ❏ Nation - State ❏ Organized crime	❏ Cyberespionage ❏ Ransomeware ❏ Leak to media ❏ Defacement ❏ Misinformation ❏ Insider ❏ APT's ❏ DDOS ❏ Targeted attacks ❏ Information stealing ❏ Kinetic attack	❏ Cloud computing ❏ Infrastructure ❏ Mobile devices (BYOD) ❏ IoT (A.I. - Drones - Health) ❏ State compliance ❏ Social networking ❏ EMV ships ❏ Bulletproof hosting	❏ Government ❏ Private sector ❏ Media ❏ Police

The concepts displayed on the table can be adopted for national or international simulations which connotes the borderless attributes of the cyber domains. Under the "Possible authors" column, a list of the potential originators is presented, followed by the: "Attack" column considering some of the possible strikes in the given scenario. A "Trends" column indicates current tendencies that could be attacked at any time. The last column illustrates the potential targets of any of the previous concepts.

The outline is adaptable, each audience is tailored and scheduled that will suit it's needs. The time frame would depend on the number of injects distributed during the exercise. On the dynamics of the exercise, this proposal also considers necessary the formulation of a substantive and the decision making framework question after each inject. The question will be delivered and addressed every fifteen (15) minutes in order to give way to the other. The reason for the time specification falls under the need to guarantee the continuity in which people should not be provoked to invest time in other activities. The substantive question asks for the way to proceed on the specific situation the scenario presents (every inject), and subsequent to this, the framework questions are presented for elaboration, expecting a short answer addressing how the decision making framework elements (Authority, Cooperation, Transparency, Timeline) would be covered or addressed under a similar situation on real life crisis.

Table 13: Scenario outline and dynamics of a cyber related event decision-making TTX.

Scenario Outline And Dynamic	
Time	**Event Description**
DAY 1	
09:00 - 09:30	Introduction, description, rules, directions, and dynamic
09:00 - 10:00	Two (2) injects, each every 30 minutes
10:00 - 10:15	Coffee break
10:15 - 11:45	Three (3) injects, each every 30 minutes
11:45 - 13:30	Lunch break
13:30 - 15:00	Three (3) injects, each every 30 minutes
15:00 - 15:15	Wrap up for the day
DAY 2	
09:00 - 10:30	Feedback and discussion session.

In the column on the left side an adjustable timeline for the development of the agenda for TTX is presented on the right these are linked to a description of events that may be taking this each time slot.

Execution

The administration of the TTX is carried out by a white team, composed of a coordinator, in charge of the dynamics of the exercise; a legal expert on national and international regulatory systems; a technical expert at least; and, an observer as a minimum. The white team should be at reach for any question from the participants' side. The legal and technical experts, address the questions that fit their expertise respectively while the coordinator processes the answers and inputs from the participants or groups and begins to adapts it to the feedback and discussion model. The observer takes notes records events, assists with general arrangements (logistic support) but could be also involved assisting the coordinator. The observers' notes on perceptions, and reactions are useful for improving the TTX for future interactions. All of the tables that compose this modular guide must be be compiled in a handout and provided to the members of the white team to guarantee they all have the same bird eye view on the whole TTX. The modular guide can be used also as a communication and cooperation enhancing tool.

The sequence on the injects would happen as follows: the groups participating in the TTX will receive a sheet of paper with the substantive question on the exercise almost immediately after each inject. After 15 minutes the decision making framework questions will be delivered in a separate paper. The teams should address both of the questions handed in to them on the papers providing a reasoned solution to the questions. This data will be the basis to prepare the feedback session. A set basic rules listed on table 14 could guarantee the successful completion of the simulation exercise.

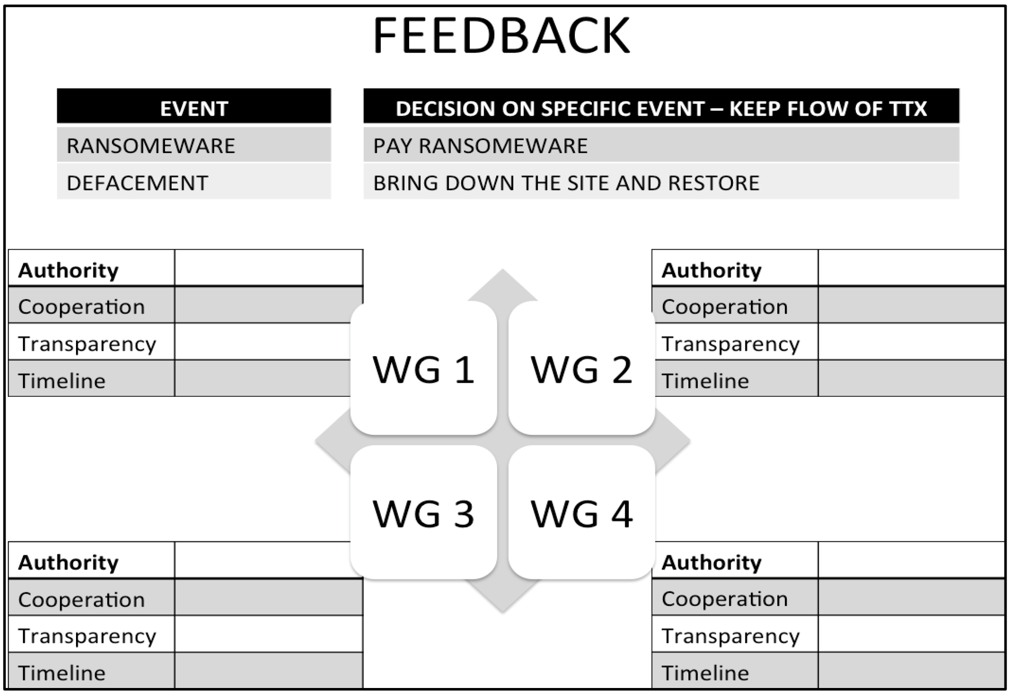
Table 14: Rules for a cyber related event decision-making TTX.

Rules	
Do not fight the scenario	The scenario could present realistic but not so probable events, accept the inject and play through.
Have fun, enjoy the TTX	Do not take anything personal; try to keep discussion under terms of kindness in a pleasant environment.
There are no right or wrong answers	Feel free to bring innovative solutions; do not hold back on your thoughts towards the scenario.

In the table to the column of the left correspond the basic rules with brief explanations that appear under the column at the right side of the table.

Feedback and Discussion

The feedback and discussion session must refer to the inputs collected from the participants' regarding each inject, but also containing reflections on the records and notes that the observer may have recorded. Visualization methods for communication of the feedback are recommended at this stage not only they are less intrusive but might appeal to participants and improve understanding of the flow of events during the exercise. The proposed decision making framework "the what to test" is filled out on the template that the figure 9 presents. The different reactions that the participants, teams or working groups displayed will feature comparisons about each event. Both answers to the substantive questions and the decision-making framework questions are to be discussed one by one. During this stage, participants should be encouraged to discuss any issue that may have arisen, point out gaps, failures, shortcomings, flaws, strengths and basis in their existing legislation, cooperation and communication channels, decision making process, crisis management, and information diffusion, this should trigger the search for novel solutions with all the participating stakeholders (working groups) involved in the decision making process upon a cyber crisis.



FEEDBACK

EVENT	DECISION ON SPECIFIC EVENT – KEEP FLOW OF TTX
RANSOMEWARE	PAY RANSOMEWARE
DEFACEMENT	BRING DOWN THE SITE AND RESTORE

Authority	
Cooperation	
Transparency	
Timeline	

Authority	
Cooperation	
Transparency	
Timeline	

Authority	
Cooperation	
Transparency	
Timeline	

Authority	
Cooperation	
Transparency	
Timeline	

Figure 9: Visualization method for feedback and discussion session for a cyber related event decision-making TTX

The proposed visualization method should contain the solutions for the substantive and framework questions proposed by this model, revealing each of the approaches from the participants to each of the provided injects.

5 Summary and Concluding Remarks

The use of simulation exercises could seem familiar to those who have been acquainted to those methods in the last years. Also, the popularity of the experiential learning and learning by doing messages' steady growth may seem too obvious. However, the former is a systematic approach to teaching and learning that has been conceptualized only very recently and the context of current studies on co-innovation. project management and other fields but remains an incipient issue in the wider theoretical landscape (for instance in cybersecurity studies). The later reflects the revival of theories half a century old but that fit the current techno-socio-economic paradigm and the so called experiential age. Exploring the application of a combined approach to a new field proposes a new interdisciplinary dialog with merits in itself. This has been the effort of this thesis that tackles the perceived lack of of academic legitimization required for grounding theory.

This research was inspired by the need to improve strategic decision making competences in cyber related incidents. It conforms to National Cyber Security Strategies' formulation standards in what regards the interest in raising awareness, and improving training and education effectiveness. The weaknesses of traditional models, still prevailing, were addressed and discussed, and the need to show an innovative, more engaging model concept with significant impact could be affirmed. TTXs were claimed to be suitable mechanisms to overcome the perceived flaws of conventional approaches. These simulations can be said to have capacity to shape, enhance and test the awareness, understanding and preparation levels required to respond strategically to cyber security incidents.

The theoretical contribution achieved to produce an interdisciplinary construct where three fields were involved: education, computer sciences and management. From these, the learning theories (situated cognition and experiential learning), human computer interaction theories (gamification) and strategic management theories could be shown to converge through the concepts that characterize TTXs: These were culture, learning by doing, experience and feedback; engagement and role playing; and, crisis management and OODA loop, respectively. The initial grounded theory exploration was successfully explained using Bloom's revised taxonomy of educational objectives, and further, its practical value was confirmed. Nevertheless, this thesis' arguments and integrative perspectives warrant further study.

An empirical section that involved the participation and observations in national and international level TTXs, expanded the contributions by putting manifest how this novel model corroborates all departing conceptual assumptions. The collection of data does not only legitimize conceptual claims, but also adds to the development of the computational social sciences. An additional outcome of the work consists of a modular guide for the implementation of any TTX. Convenient to determine the what, the who, the how, and the what for to-do? in all phases of the exercise (Identification of goals, objectives and scope; Planning upon considerations; Execution; Feedback and discussion).

Two (2) experiences in national and international level TTXs could be few and arise as the most evident limitation of this research. Having access to these types of audiences again was unrealistic in the short run. However, the extent of the involvement and data collection during the planning, designing, execution and assessment phases yielded ample fruit. Participation and observation in other TTXs, using the same criteria, is recommended to assess the general applicability of the approach, also to examine the usability attributes of the modular guide to implement decisions during cyber related incidents simulated in TTXs.

In sum, this study achieved to conceptualize that educational and training models that use simulated based scenarios, innovate, increase engagement and should strengthen awareness and competences of participants in cyber related events strategic decision-making. The visions herein contained emphasize the importance of developing theories and the theoretical relevance in fields heavily and mostly concerned with technical aspects. The conceptual and empirical contributions of this thesis could be held as institutionalization tools to assist strategic crisis management competences building for cybersecurity in Colombia or elsewhere where the legal framework and the National Cybersecurity Strategies may call.

References

[1] G. B. White, G. Dietrich, and T. Goles, “Cyber security exercises: testing an organization’s ability to prevent, detect, and respond to cyber security events,” *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 00, no. C, pp. 1–10, 2004.

[2] K. P. Newmeyer, “Elements of National Cybersecurity Strategy for Developing Nations,” *Natl. Cybersecurty Inst. J.*, vol. 1, no. 3, 2015.

[3] T. L. Saaty, “Decision making with the analytic hierarchy process,” *Int. J. Serv. Sci.*, vol. 1, no. 1, p. 83, 2008.

[4] “Hambrick, D., Mason, P. (1984) Upper Echelons The Organization as a Reflection of its Top Managers.pdf.” .

[5] M. D. Cavelty, “Cyber-Security and Threat Politics,” *Secur. Stud.*, p. 182, 2008.

[6] D. Vogel, C. A. Bowers, and C. A. Bowers, “Computer gaming and interactive simulations for learning : A meta-analysis,” no. October 2015, 2006.

[7] M. Loon, J. Evans, and C. Kerridge, “Learning with a strategic management simulation game: A case study,” *Int. J. Manag. Educ.*, vol. 13, no. 3, pp. 227–236, 2015.

[8] V. Pastor, G. Díaz, and M. Castro, “State-of-the-art simulation systems for information security education , training and awareness,” *Eng. Educ.*, pp. 1907–1916, 2010.

[9] M. R. Stytz and S. B. Banks, “Toward Attaining Cyber Dominance,” *Strateg. Stud. Q.*, pp. 55–87, 2014.

[10] G. Zichermann and C. Cunningham, *Gamification By Design*. 2011.

[11] K. M. Kapp, *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education*. John Wiley & Sons, 2012.

[12] D. A. Kolb, “Experiential Learning: Experience as The Source of Learning and Development,” *Prentice Hall, Inc.*, no. 1984, pp. 20–38, 1984.

[13] C. Beard and J. P. Wilson, *Experiential Learning: A Handbook for Education, Training and Coaching*. Kogan Page, 2013.

[14] A. L. Wilson, “The promise of situated cognition,” *New Dir. Adult Contin. Educ.*, vol. 1993, no. 57, pp. 71–79, 1993.

[15] J. S. Brown, A. Collins, and P. Duguld, “Situated Cognition and the culture of learning,” *Educ. Res.*, vol. Report # 6, no. December, pp. 1–30, 1988.

[16] D. R. Krathwohl, “A Revision of Bloom’s Taxonomy. An Overview.,” *Am. J. Psychol.*, vol. 122, no. 1, pp. 39–52, 2009.

[17] E. K. Stern, *Designing Crisis Management Training and Exercises for Strategic Leaders*, vol. 42. 2014.

[18] A. Boin, P. ’t Hart, E. Stern, and B. Sundelius, “The Politics of crisis management: Public leadership under presure,” 2005.

[19] E. Stern, L. Newlove, and L. Svedin, *Auckland Unplugged: Coping with Critical Infrastructure Failure*. Lexington Books, 2003.

[20] F. Thompson, “Business Strategy and the Boyd Cycle,” *J. Contingencies Cris. Manag.*, vol. 3, no. 2, p. 81, 1995.

[21] G. M. Schechtman, “Manipulating the OODA loop: The overlooked role of information resource management in information warfare,” no. December. pp. 1–116, 1996.

[22] Ministerio de Interior y Justicia, Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones, Departamento Administrativo de Seguridad, Departamento

Nacional de Planeación, and Fiscalía General, "Lineamientos de Política para Ciberseguridad y Ciberdefensa," p. 43, 2011.

[23] O. (Organization of A. S. States, "CYBER ! SECURITY ! TECHNICAL ! ASSISTANCE ! MISSION !," 2014.

[24] U. Franke and J. Brynielsson, "Cyber situational awareness – a systematic review of the literature," *Comput. Secur.*, vol. 46, p. 41, 2014.

[25] G. C. Wilshusen, "Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies," *GAO Highlights*, 2015.

[26] O. Thränert, M. Zapfe, M. D. Cavelty, J. Grätz, M. Haas, P. Mahadevan, and M. Zapfe, "Strategic Trends 2015," 2015.

[27] J. and C. M. Hammerstein, "The CERT Approach to DOD Cyber Workforce Development," no. December, 2012.

[28] J. L. Hernández-ardieta, D. Santos, P. Parra, J. E. Tapiador, P. Peris-lópez, J. López, and G. F. Navarrete, "An Intelligent and Adaptive Live Simulator : A New Concept for Cybersecurity Training," *Futur. Secur.*, pp. 558–565, 2014.

[29] U. S. O. A. H. S. DEPARTMENT, "Homeland Security Exercise and Evaluation Program (HSEEP)," no. April, 2013.

[30] L. Gregory, "Designing Cyber Exercises (ISC) 2 Pittsburgh Chapter CERT | Cyber Workforce Development October 2014," no. October, 2014.

[31] P. J. H. Schoemaker, "Scenario Planning : A Tool for Strategic Thinking," *Management*, no. JANUARY 1995, 1995.

[32] ENISA, "Good Practice Guide on National Exercises," p. 80, 2009.

[33] R. Ottis, "Light weight tabletop exercise for cybersecurity education," *J. Homel. Secur. Emerg. Manag.*, vol. 11, no. 4, pp. 579–592, 2014.

[34] G. Zicherman, "ABOUT: Gabe Zichermann - Gamification Co," in *Closing Keynote GSummit 2014*.

[35] S. Deterding, D. Dixon, R. Khaled, L. Nacke, M. Sicart, and K. O'Hara, "Gamification: Using Game Design Elements in Non-Game Contexts," *Proc. 2011 Annu. Conf. Ext. Abstr. Hum. Factors Comput. Syst. (CHI 2011)*, pp. 2425–2428, 2011.

[36] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work?--a literature review of empirical studies on gamification," *Syst. Sci. (HICSS), 2014 47th Hawaii Int. Conf.*, pp. 3025–3034, 2014.

[37] F. Groh, "Gamification: State of the Art Definition and Utilization," *Res. Trends Media Informatics*, pp. 39–46, 2012.

[38] T. Ben-zvi and T. C. Carton, "Applying Bloom's Revised Taxonomy in Business Games," *Business*, vol. 35, 2014.

[39] S. P. Leblanc, A. Partington, I. Chapman, and M. Bernier, "An Overview of Cyber Attack and Computer Network Operations Simulation," *MMS 11 Proc. 2011 Mil. Model. Simul. Symp.*, pp. 92–100, 2011.

[40] CCIT - Fedesarrollo, "Avances y retos de la defensa digital en Colombia," 2014.

I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Carlos Arturo Martinez Forero**,

1. Herewith grant the University of Tartu a free permit (non-exclusive licence) to:
   - 1.1. Reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and
   - 1.2. Make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Tabletop Exercise For Cybersecurity Educational Training; Theoretical Grounding And Development,

supervised by Maria Claudia Solarte Vasquez, Reimundas Matulevičius

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **26.05.2016**