UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Alex Duran

Organizational Interaction Mechanisms Affecting Strategic Decision-Making During Cybercrime Investigations

Master's Thesis (30 ECTS)

Supervisor: Maria C Solarte Vasquez

Co-Supervisor Raimundas Matulevičius

Tartu 2016

Organizational Interaction Mechanisms Affecting Strategic Decision-Making During Cybercrime Investigations

Abstract:

The aim of this thesis is to understand and explain organizational interaction in law enforcement decision-making spheres, as a phenomenon that involves the concepts of collaboration, cooperation and information sharing, and the way that these affect cybercrime investigation processes. The problem research steams from the insufficient interdisciplinary work and theoretical developments of social sciences within technical fields and more specifically the lack of conceptualizations that could guide managerial functions related to cyber crime investigations. As a result, Law Enforcement Agencies (LEAs) face increasing difficulties concerning processes, communication, and collaboration derived from complex information sharing needs, and in particular, issues of timely delivery and mistrust. The thesis is concerned with a classification of impediments that may obstruct investigation processes and impact strategic decision-making, and with the formulation of the necessary conditions to generate an optimal and collaborative information-sharing environment for fighting against cybercrime.

The methodological approach includes qualitative content analysis, surveys, a case study and the use of secondary data. First, the work defines terms and differentiates concepts via interpretation, to help to establish an accurate mapping of the current situation within a cybercrime ecosystem from the stakeholders' point of view and determine their interaction mechanisms. Then, it progresses onto the identification of the main obstacles and needs that the investigative process reveals, and proposes a new optimized model of cybercrime investigations analysis. This analytical tool can inform and report on the stages of the process that would require greater intervention. Last, the case of the Police Cybercrime Center (CCP) of Colombia is studied; to illustrate how these perspectives may apply.

The results of this work suggest that by including management elements at the preparatory stage of the investigative process, functional aspects could be improved, and the interaction with stakeholders and the provision of information to support the criminal investigation can be facilitated. Furthermore, that via administrative procedures, trust relationships can be improved as well as information flow patterns and ultimately increase organizational efficiency in the fight against cybercrime.

This thesis contributes with theoretical development, clarification of key terms resulting from the interdisciplinary integration of concepts and theories, and practical instruments applicable to guide managerial organizational interaction mechanisms in cybercrime investigations. Other contributions of meaningful implications are the results of the analysis of needs, the guidelines for the implementation of best practices, and the proposal of implementation of an optimized model of investigation based on the need of organizational interaction. Those conform a toolbox of practical instruments for the implementation of managerial techniques to enhance effectiveness and support decision-making in combating cybercrime.

Keywords:

Cybercrime, investigation, organizational interaction, collaboration, cooperation, information sharing, decision-making,

CERCS: T175 PHYSICAL SCIENCES – Informatics, Systems theory.

Organisatsioonidevaheliste suhete mõju küberkuritegevuse uurimise strateegiliste otsuste langetamisele

Lühikokkuvõte:

Antud lõputöö eesmärk on mõista ja selgitada organisatsioonide vahelist suhtlust õiguskorra tagamisel otsuste langetamise valdkondades kui nähtust, mis hõlmab koostöö ja teabe jagamise kontseptsioone ning viise, mis mõjutavad küberkuritegevuse uurimise protsesse. Uurimisobjekti probleem tuleneb ebapiisavast interdistsiplinaarsest tööst ja teoreetilistest sotsiaalteaduste arengutest tehnika vallas ning täpsemalt kavandatud lahenduste puudumisest, mis võiks suunata küberkuritegevuse uurimisega seotud juhtimisfunktsioone. Selle tulemusena seisavad õiguskaitsebürood (ÕKBd) silmitsi üha kasvavate raskustega, mis puudutavad nii protsesse, kommunikatsiooni kui koostööd, mis tulenevad keerulise teabe jagamise vajadusest. Eelkõige tekitavad raskusi küsimusi õigeaegne teabevahetus ja usaldamatust. Lõputöös on liigitatud takistused, mis võivad pidurdada uurimisprotsesse ja mõju strateegiliste otsuste langetamisel. Samuti püüab lõputöö sõnastada tingimused, mis on vajalikud optimaalse ja koostööl põhineva teabevahetuskeskkonna loomiseks, et võidelda küberkuritegevuse vastu.

Metoodiline lähenemine hõlmab kvalitatiivset sisuanalüüsi, uuringud, juhtumikirjeldust ja teiseste andmete kasutamist. Esiteks, määratleb töö terminid ja eristab mõisted tõlgenduste kaudu, et aidata luua täpne olukorra kaardisus küberkuritegevuse ökosüsteemis. Antud kaardistus hõlmab nii ökosüsteemi sidusrühmade vaatepunktist ja määratleb nende koostoime mehhanismid. Seejärel määrtaletakse lõputöös põhilised takistused ja vajadused, mille uuriv protsess paljastab, ja tehakse ettepanek uue optimeeritud küberkuritegevuse uurimise analüüsi mudeliks. See analüütiline tööriist saab teavitada ja raporteerida protsessi etappidest, mis vajaks suuremat uurimist. Viimaseks, uuritakse Kolumbia politsei küberkuritegevuskeskuse (KKT) juhtumit, et näitlikustada, kuidas uuritud perspektiive saaks rakendada.

Töö tulemused soovitavad, et funktsionaalsed aspekte saaks parandada kui lisada juhtimise elemente uurimisprotsessi ettevalmistavasse järku. Ühtlasi saab hõlbustada kriminaalmenetluse uurimisel ka suhtlust sidusrühmadega ja teabe varustamisega. Veelgi enam, läbi haldusmenetlusprotsesside saab parandada nii usaldussuhteid kui teabe liikumise mustreid ja lõpuks suurendada organisatsioonide tõhusust võitluses küberkuritegevusega.

See lõputöö panustab teoreetilise baasi arendamisse, selgitab põhimõisted, mis tulenevad interdistsiplinaarnsest kontseptsioonide ja teooriate integratsioonist. Samuti esitleb lõputöö praktilisi vahendeid, mida saab kohaldada juhtimisorganisatsioonide koostoimemehhanismidele küberkuritegevuse uurimisel. Töös esitletakse vajaduste analüüsi tulemusi, parimate praktikate rakendamise suuniseid ning ettepanekut optimeeritud uurimismudeli ellurakendamiseks, mis lähtub organisatsiooni suhtluse vajadustest. Eelnimetatud moodustavad tööriistkasti praktilistest vahenditest, mida rakendada juhtimistehnikates, et suurendada tõhusust ja toetada otsuste tegemist võitluses küberkuritegevusega.

Võtmesõnad:

Küberkuritegevus, uurimine, institutsiooniline koostoime, koostöö, teabe jagamine, otsuste langetamine

CERCS: T175 REAALTEADUSED - Informaatika, süsteemiteooria

Table of Contents

1 Introduction

Concerns about the effectiveness of the fight against cybercrime have increased because of the rapidly evolving nature of cyber threats, procedural obstacles, and collaboration complexities associated with criminal investigation processes. As one of the major challenges for decision makers, this situation has forced organizations and specifically managers of Law Enforcement Agencies LEAs, to rethink cybercrime strategies. The urgent need to improve specialized reactions may require the interaction of different specialized stakeholders, well-trained cybercrime police units, and well-equipped teams with access to the latest technical and forensic tools.

This may also require the promotion of collaborative information sharing practices and strengthening of capacity building to overcome some of the most common problems affecting effective responses. Lack of administration management procedures; legal and procedural obstacles; privacy questions; trust issues; low interest from partners; technical barriers; and, delays in providing information, and mandatory report mechanisms have been identified as such. These deficiencies could be attributed to setbacks in the investigative process, lack of consensus on basic terminology and the very nature of cybercrime, lack of expertise, confidence and knowledge on how to cooperate and to which extent and distrust between those who must interact.

The general purpose of this work is to understand and explain organizational interaction in law enforcement decision making spheres, as a phenomenon that involves the concepts of collaboration, cooperation and information sharing, and the way that these affect cybercrime investigation processes.

To address the complexities of cybercrime investigations from the perspective of top management decisions, it emphasizes the relevance of computational social sciences research. Non-technical aspects may have a direct impact on the networks in all their layers and in cyber security where the narrow topic of decision-making process on cybercrime investigations is nested. This thesis proposes a conceptualization and theoretical advancements that could help minimize the problem of insufficient interdisciplinary theoretical developments of social sciences within technical fields. Specifically, on factors that guide managerial functions related to cybercrime investigations. Law Enforcement Agencies (LEAs) face increasing difficulties concerning processes, communication, and collaboration schemes derived from complex information sharing needs, and in particular, issues of timely delivery and mistrust. In accordance with the aforementioned scope, the following Research Questions RQ will be addressed:

RQ1. What are the impediments that may obstruct cybercrime investigation processes that could impact strategic decision-making?

RQ2. What are the necessary conditions to generate an optimal and collaborative sharing information environment for fighting against cybercrime?

The methodological approach selected included qualitative content analysis, surveys, a case study and the use of secondary data. They match the research tasks that follow, but details of their use will be explained in the corresponding section:

RT1 Definition and differentiation of concepts and key terms

RT2 Mapping the current state of the organizational interaction during cybercrime investigations.

RT3	Identification of the main obstacles and needs on the investigative process.
RT4	Comparative analysis of cybercrime investigation processes and existing models.
RT5	Proposing an optimized model of cybercrime investigations based on interaction needs.
RT6	Applicability of the optimized model using the information on needs
RT7	Study case of the Police Cybercrime Center (CCP)
RT8	Survey design and findings review applied to the diagnosis of the current state of organizational interaction at the CCP
RT9	Formulation of a set of guidelines to promote collaborative interaction on cybercrime investigations

RT1 is based on the literature review, documents analysis and revision of secondary data from various fields: law, criminology, and the social sciences. Terms and concepts of cybercrime and strategic decision-making are reviewed and interpreted, underlying that precision is achieved after differentiating the concepts. The review-concerned terminology associated with organizational interaction mechanisms such as collaboration, cooperation, and sharing information. RT2 is performed with the use of document analysis and secondary data that includes all information contained within the e-Crime Project EU 2015[1]. The mapping of the organizational interaction allocates stakeholders, key players, and the perpetration cycle within the cybercrime ecosystem produced by the aforementioned project. RT3 compiles collaboration, cooperation and information sharing needs of the LEAs collected from the conceptual analysis and drawing from the academic literature review, and from ENISA's[2] and HTCIA's[3] reports. RT4 compares five of the most representative models of investigation process from different perspectives, on each of their stages. RT5 formulates an optimized model of cybercrime investigations analysis based on the organizational interaction needs. RT6 applies the criteria recommended included in the model resulting from RT5, classifying and categorizing needs, to inform and report the stages of the process that would require greater intervention. RT7 studies the phenomena within Colombia at the Cybercrime Center. To proceed with this task, documentary analysis, official information and professional expertise were determining sources of insight. RT8 Was performed with an instrument distributed to a convenience sample of 40 officials belonging to CCP with experience in investigation processes. Finally, the RT9 applies the perspectives put forward by this work and concludes with a set of guidelines that may help to increase the effectiveness of the investigative process.

The present thesis is organized into five main parts: Methodology, explaining the research strategy and design. Theoretical background, determining the scope and definitions starting from documenting the relevance of the research problem, and defining cybercrime and related aspects of collaboration, cooperation and information sharing. Organizational Interaction within Cybercrime Investigations is divided in Conceptual Developments, and Contextualization of the Cybercrime Field Process Analysis. It is appropriating concepts via interpretation, and establishing an accurate mapping of the current situation within a cybercrime ecosystem from the stakeholders' point of view, determining their interaction mechanisms. Practical Applications, by modelling cybercrime investigation process,

[1] Available at http://ecrime-project.eu/about
[2] Available at https://www.enisa.europa.eu
[3] Available at https://www.htcia.org

proposing a new optimized model of cybercrime investigations analysis, identifying the needs that the investigative process reveals, a study case of the Police Cybercrime Center (CCP) of Colombia is reviewed, and surveys, illustrates how these perspectives may apply using proposed guidelines. Finally, concluding remarks with the limitations of this study and the avenues that are made available for further research.

The larger discussion furthered by this work suggest that by including management elements at the preparatory stage of the cybercrime investigation process, functional aspects (affected by the nature of these illicit conducts) could be improved, and the interaction between stakeholders can be facilitated. Furthermore, that via administrative procedures, trust relationships can be improved as well as information flow patterns. These effects have the potential to increase organizational efficiency in the fight against cybercrime.

The contributions of this thesis are, theoretical development, clarification of key terms resulting from the interdisciplinary integration of concepts and theories, and a practical instrument applicable to guide managerial organizational interaction mechanisms in cybercrime investigations. Other contributions of meaningful implications are the results of the analysis of needs, the guidelines for the implementation of best practices, and the proposal of implementation of an optimized model of investigation based on the need of organizational interaction. Those conform a toolbox of practical instruments for the implementation of managerial techniques to enhance effectiveness and support decision-making in combating cybercrime. The work is geared towards the managers in Law Enforcement Agencies LEA´s, or anyone interested in consulting collaborative investigation processes.

2 Methodology

The phenomena of organizational interaction in law enforcement decision making spheres under investigation, was considered to benefit most from a constructivist methodological approach that could help understand and explain the implications that affect cybercrime investigation processes. Therefore, the research problem is addressed using qualitative methods that prevailed for the data collection and the evaluation of the cybercrime investigative process. The processing of data collected is interpretative to achieve a valid exploratory document analysis on one hand and on the other, a mixed exploratory and confirmatory survey analysis that also included one open question, subject to qualitative analysis. Consequently, even if one of the collection methods is typically used in quantitative research, that is the survey, in this case, it had a limited reach and did not intend to support fundamental contributions. The additional open question on the survey administered as described below was analyzed as the rest of the documents by using, categorizations, classifications, conceptual modelling, visualization techniques, and charting.

The data regarding the theoretical contribution and the models was obtained from several academic articles and official documents, and secondary data taken from the e-crime project [4], as the main source of information, for establishing the current state on cybercrime and for making conceptualization and clarification of key terminology in the organizational interaction field, by the integration of different disciplines of law, criminology, and computational social sciences.

The data collected from surveys compile self-reported information about personal perception of real world cybercrime investigators, helping to understand the current situation of the Colombia Cybercrime Center. The analysis of this information is also qualitative and supplies empirical data that is used to determine the current status of the stakeholder's interaction and enriches the understanding of the phenomena discussed. Detailed report on the methods will be explained in the corresponding section below.

[4] Available at: http://ecrime-project.eu/about

3 Theoretical Background

This section lays the theoretical foundations, determines the scope and defines key concepts contained in this work. It starts from documenting the relevance of the research problem, and defining cybercrime and related aspects of collaboration, cooperation and information sharing. Then it introduces the new concept of organizational interaction as an encompassing phenomenon deserving of study, in particular in the context of law enforcement decision-making spheres where all these concerns have received little attention so far.

Gercke wrote that the changing nature of cybercrime is due in part to the increasing ubiquity of global connectivity, the complexity of global cyber criminal networks, and difficulties identifying links between the perpetrator and the crime [1]. Whereas Yar noted that the phenomenon of cybercrime is not new, or qualitatively different from ordinary crimes, but some novelty lies in new modalities and the use of virtual environments for their execution [2]. Crimes are evolving according to the expansion of the Internet, spreading rapidly and therefore, causing extensive damage. Criminals employ more sophisticated technology and seem to be ahead, more knowledgeable than cyber security professionals and LEAs [3]. Politically motivated cybercrime weaponry, and command and control systems have also moved into cyberspace to deploy and execute espionage and sabotage activities, according to Marshall and KPMG practitioners. [3], [4]

The complexity, barriers and obstacles that arise during cybercrime investigation have been discussed extensively in different spheres by authors such as Brown and institutions like ENISA [5], [6]. Also, the United Nations (UN) conducted an extensive study on cybercrime, stressing the importance of better information exchange, legal harmonization, implementation of best practices, technical assistance, and international cooperation. It mentioned the following key issues: The impact of fragmentation on international levels and diversity of national cybercrime laws on international cooperation; excessive reliance on traditional means of formal international cooperation in criminal matters, involving cybercrime and electronic evidence; location; regulatory harmonization; law enforcement and criminal justice capacity; and, cybercrime prevention activities [7]. The study mentioned preventive strategies that could help tackle cybercrime such as *"the promulgation of legislation, effective leadership, development of criminal justice, law enforcement capacity"* building, *"education and awareness"*, and international and private cooperation [7]. Bednar also emphasized on information sharing and collaboration trough the incorporation of interest groups, with contrasted worldviews, languages, and cultures into decision-making levels, to help overcome the negative implications of the poor quality of information presently prevailing in cybercrime investigations, and other investigative processes [8].

According to the report made by Police Executive Research Forum (PERF), the obstacles evidenced in police investigations, prosecution and forensic practices are frequently associated with lack of reporting, unclear models, and deficiencies on formal standards in this area. It coincide with authors such as Broadhurst, who claims the quickness which cybercrime crosses borders, legal differences between countries, and tricks used by criminals, could prevent attribution, prevent interrogation of suspects, and hinder the detention of offenders [9], [10]. Brown further argues that, the lack of capacity of investigators, prosecutors, judges, and jurors to understand the illicit use of technology could impact conviction rates [5]. In the context of collaboration, cooperation, and information sharing, ENISA highlighted difficulties related to "*lack of administrative*

management procedures, legal and procedural obstacles, privacy questions, trust issues, low interest from partners, technical barriers, intentional delays, and mandatory mechanisms" [11].

Cybercrime has become one of the biggest challenges for governments, organizations, and LEAs, creating the need for immediate action to reduce the existing risks and counteract the negative impact caused by impunity [1]. Actions' effectiveness is affected by time and speed, especially if they are performed by various instances, this has been recorded for example in the report made by the Dutch government on public private partnership, where Luiijf & Kernkamp stated "*The timely and speedy sharing of information between organizations is widely perceived as one of the most effective measures to address cybersecurity challenges in organizations"* [12]. Cerezo emphasizes on the need for international cooperation between countries and institutions properly backed by laws for the success in combating, investigation and prosecution of such crimes. The harmonization on international relations and the establishment of conventions and directives, could increase the competent fight against cybercrime [13].

The International community and cybersecurity practitioners concerned about the startling growth of cybercrime are making attempts to measure what has been considered an exponential growth in, costs, and impact on online users and enterprises. For example, Ponemon Institute discusses the evolution of cybercrime in terms of frequency and severity affectation to businesses. The study conducted in 252 companies from 7 representative countries, evidenced an average of $7.7 million USD annual costs documented in 1928 attacks, increasing by 1.9 percent per year [14]. The security report by Norton 2016 already show that more than 594 million of online consumers were affected by cybercrime; 348 million identities from trusted institutions were exposed, and losses rose to for more than 150 billion USD were reported only in 17 countries that were surveyed [15]. According to the UN 2013 report, cybercrime victimization rates are higher than conventional crime in online population. For example, conducts such as email hacking, phishing, identity theft, online credit card fraud, vary between 1 and 17 percent, instead burglary, robbery, and car theft; from 0 to 13 per cent. Also, European private sector report rates between 2 and 16 percent of data breaches, outside attacks, and data corruption [7]. The IC3 reported 269,422 complaints with more tan 800 million USD losses in the US only in 2014, revealing the growing impact of social media and the emergence of virtual currency transactions in cybercrime [16].

The Colombian case evidenced the typical exponential increase of the international scene. However, because since the Government is the committed to invest time efforts and resources to counteract cybercrime, the number of reports has increased markedly. For example, in 2014 3.871 crimes were reported, and 2015, 6.366. Most correspond to defacement cases: (34.4%, 15.5% to online scam, 8.9% to identity theft, 7% phishing, and 5.2% to smishing) [17].

Defining Cybercrime

Because of the confusion between the terms cybercrime and computer related crimes, the Tenth United Nations Congress on the prevention of crime and treatment of offenders, have differentiated these terms. "*In a narrow sense (computer crime) as: "Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them". And "Cybercrime in a broader sense" (computer-related crime) as: "Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network*"[18].

The Cybercrime Convention and its additional protocols describe cybercrime as "*criminal activities where computers and information systems are involved either as a primary tool or as a primary target"*. This work subscribes to it. The convention also contemplates a broad range of these activities such as: *"Offenses against the confidentiality, integrity and availability of computer systems and data (Illegal access, illegal interception, data interference, system interference and misuse of devices); Computer-related offenses (e.g. fraud, forgery); Content-related offenses (e.g. content violations, child pornography); and offenses related to infringements of copyright and related rights (e.g. copyright intellectual property)"* [19]

The Convention also defines: computer system, computer data, service provider and traffic data. However, it does not include standard typologies of crimes committed or facilitated using computer technologies such as money laundering, identity theft or storage of illegal contents as Alkaabi does. [20].

Collaboration

Collaboration is a term shared across multiple disciplines, but its interpretation depends on the theoretical perspective, and how it is assessed and studied. A universal definition of collaboration especially in the context of crime investigations is not available. Thomson argued that, precision becomes a challenge for scholars and practitioners in finding an approximate definition about the extent, parameters and evaluation of the term in theory and practice, [21]. And also, some difficulties of reaching agreement on definitions, due to a shortage of studies on measuring of collaboration [22].

The extensive study performed by Mattessich sheds some light on the matter, defining collaboration as "*mutually beneficial and well defined relationship entered into by two or more organizations to achieve common goals*". It also identifies some factors of influence classified in six groups: environment; membership; process structure; communication; purpose; and resource [23]. Another collection of works performed by Wood & Gray, defined as "*Collaboration occurs when a group of autonomous stakeholders of a problem domain engages in an interactive process, using shared rules, norms, and structures, to act or decide on issues related to that domain*" [24]

In addition, Thomson & Perry have conducted extensive studies incorporating those mentioned above, and included the evolution of collaboration, participation of stakeholders and of multidimensionality, interpreting collaboration as: "*The process in which autonomous or semi-autonomous actors interact through formal and informal negotiation, jointly creating rules and structures governing their relationships and ways to act or decide on the issues that brought them together; it is a process involving shared norms and mutually beneficial interactions*" [25]. This work will elaborate on the bases of this definition.

Cooperation

Mangal studies starts from the etymology of the word, which indicates two components. The term combines co and operation, meaning a work together, that is undertaken at the time [26]. Some definitions agree on the search of mutual benefit instead competing, including terms such as common effort [5], working together[6], or willingness to help someone in need [7]. An extensive study of the evolution of cooperation collects most of the

[5] Available at: http://www.merriam-webster.com/dictionary/cooperation
[6] Available at: http://www.oxforddictionaries.com/definition/english/cooperation
[7] Available at: http://dictionary.cambridge.org/dictionary/english/cooperation

terms related above, saying that "*Cooperation is the process of groups or organisms, working or acting together for common or mutual benefit, as opposed to working in competition for selfish benefit*" [27].

Mattessich also speaks of cooperation interpreted the term as the "*Informal relationship existing without commonly defined mission, structure or planning effort. Information is shared as needed, and authority is retained by each organization so there is virtually no risk"* [23]. In contrast, Thomson & Perry stated "*Collaboration connotes a durable and pervasive relationship, bringing separated organizations in a full commitment to a common mission, requiring well-defined communication channels, operation in many levels and contributing their own resources and reputation".* Therefore, when cooperation holds a common goal, it becomes collaboration; this also implies reciprocity and sharing of resources, but not necessarily in a symmetric way. Collaboration can advance individual goals, but some result should be shared [25]. This work will elaborate a differentiation and proper use of the term on the conceptual development section, appropriating the definitions related above

Information Sharing

According to Goodwin information is power. He states that "*receiving the right information at the right time can empower decision-makers to reduce risks, deter attackers, and enhance resilience*", and Cybersecurity information sharing describes "*the means of conveying information or experience from one trusted part to another*". An effective program also requires a detailed understanding of "*the actors involved; types of information exchanged; models and mechanisms of exchange; and, the scope and operational purpose*" [28]. According to Luiijf, the competencies of information sharing could cover strategic, tactical, operational and technical levels, and the properties expand throughout the phases of incidents response cycle. At the same time, the process is highly dynamic, crosses the boundary of the public and private domains, and sharing sensitive information can be very useful for some stakeholders, but potentially harmful to others [12].

ENISA developed some proposals to raise awareness of the practice of information sharing, defining it as "*the exchange of a variety of network and security related information such as risks, vulnerabilities, threats, internal security issues and good practices*" [6], [11], [29], [30]. It has also distinguished between disclosure, sharing, and exchange of information. The first implies a one-way communication, broadcasting to multiple recipients. Receivers are usually unknown, and there is no expectation of getting anything in return. In the second, the recipients are known or trusted, and there is an expectation of receiving something in return. And the last constitutes a bi-directional, one-to-one activity where the beneficiary delivers something in return [30]**.** This work will elaborate on the bases of the definitions related above, and the parameters proposed by ENISA on the conceptual development section,

Decision-Making

The expression is understood as the process of strategically choosing between alternatives. Given its importance to handle any human affair, decision-making has been widely theorized about and from different perspectives. The social sciences have described decision-making in various ways. The Institute of International Management Sciences as "*The process by which individuals select a course of action from among alternatives to produce a desired result*" [31]. Wang & Ruhe as "*To choose a preferred option or a course of actions from among a set of alternatives on the basis of given criteria or*

strategies" [32]. Al – Taraweneh as *"The process of choosing among alternative courses of action for the purpose of solving a problem or attaining a better situation regarding the opportunities that exist"* [33]; or, Babcock & Morse as *"The process of making a conscious choice between two or more rational alternatives in order to select the one that will produce the most desirable consequences (benefits) relative to unwanted consequences (costs)"* [34].

The scope and definition of decision-making will be determined in the section of conceptual developments, adopting some of the concepts studied on the theoretical background and advancing them.

All in all, the terminology studied reflects commonalities between the terms collaboration, cooperation and information sharing, and will be grouped under an encompassing umbrella term referred to in the following as Organizational Interaction. The expression will be studied as a phenomenon, without diminishing the importance of the separated entities in independent theoretical constructs.

4 Organizational Interaction within Cybercrime Investigations

This section progresses in the adaptation of concepts and terminology studied on the theoretical foundations and differentiates via interpretation. The first part is presenting the conceptual developments introducing into the context the concepts of cybercrime, collaboration, cooperation, information sharing, strategic decision-making, and organizational interaction mechanisms. The second refers to the contextualization of the cybercrime field process analysis, identifying connections between stakeholders, key players; the perpetration cycle; and, the cybercrime ecosystem based on the extensive study performed by the ecrime project [35]. Then, it is establishing an accurate mapping of the current situation within a cybercrime ecosystem from the stakeholders' point of view, and determines their interrelations between main components. With the integration of these concepts and theories within the different disciplines of law, criminology, and social sciences, it could get a better understanding of the phenomenon under study, and associate it into a single interpretation.

4.1 Conceptual Developments

Cybercrime in Context

The literature review evidenced that there is no consensus on the definition of cybercrime, and the term is being influenced by changes, evolution, differences in culture, and the legal system in place[36]. It is also open to a diversity of social, political, practical and scientific interpretations [37]. However, due to no boundaries exists, it is acknowledged by all that we must talk about it as a transnational phenomenon. The transnationality of cybercrime is the source of one of the most intense discussion at all levels, and the issue of jurisdiction and competencies that suffer has not been fully solved.

Due to the great variety of approaches in the search for a taxonomy of cybercrime, there are a variety of proposals for different authors, agencies and organizations. Most of the definitions come from social, political, practical and scientific context, and from the field of technology, criminology, and law. This study has considered the most universally accepted definition, adopting The Council of Europe Convention on Cybercrime 2001, widely known as the Budapest Convention [38]. Because this is the most accepted and recognized document by the international community on cybersecurity, and also the most used as a basis to refer to cooperation needs, legislation, and cybercrime investigations.

Accordingly, cybercrime could be interpreted henceforth as "*any criminal activities where computers and information systems are involved either as a primary tool or as a primary target"*. It comprises *"Offenses against the confidentiality, integrity and availability of computer systems and data (Illegal access, illegal interception, data interference, system interference and misuse of devices). Computer-related offenses (e.g. fraud, forgery). Content-related offenses (e.g. content violations, child pornography). And offenses related to infringements of copyright and related rights (e.g. copyright intellectual property)"*[19].

Collaboration on Cybercrime Investigations

The importance of analyzing collaboration of managers during cybercrime investigations is posed by the organizational interaction needs, which are imposed within the investigative process. The need for managers to interact with different stakeholders demands the implementation of efficient models, formal or informal mechanisms, and promotion relationships of trust. In this context, one could start by assuming that a typical cybercrime scene investigation can be viewed as a special case of collaborative decision-

making. The investigative process can potentially involve a variety of stakeholders from different types and nationalities, trying to combine efforts by the interaction of several actors from different disciplines, socio-cultural backgrounds and different legal frameworks. It might increase the complexity and the need for collaboration that supports the decision-making on cases of cybercrime [8]

Because of the nature and interdependence among stakeholders involved in cybercrime investigation processes, it is important to identify each of them and determine their capacity and scope of collaboration. The promotion of international cooperation and reduction of legal and procedural obstacles to effective collaboration could be achieved through improving information flows, supporting the implementation of coordinated bodies, exchange of experiences among communities, and adoption of safe protocols and security measures [29].

The literature review has indicated some confusion on the proper use of terms associated with collaboration. The significance of integrating theories into computational social sciences terminology is due in grand part to the widespread and interchangeable use of terms, and unawareness of differences in depth of interaction, integration, commitment, and complexity [25]. Therefore, it would be advisable to treat each one individually, making theoretical precision and properly delimitation of concepts.

For this work, it could be considered the definition stated by Thomson & Perry. They interpreted *"collaboration as the process in which autonomous or semi-autonomous actors interact through formal and informal negotiation, jointly creating rules and structures governing their relationships and ways to act or decide on the issues that brought them together"* The process involves shared norms and mutually beneficial interactions [25] Thomson's definition has adopted the studies mentioned in the literature reviewed; include the evolution of collaboration, the participation of stakeholders and multidimensionality; and five key dimensions of governance, administration, mutuality, norms, and organizational autonomy. They also remarked on the importance of collaboration costs and the significance of equilibrium between the variables described in Table 1.

Table 1 Collaboration Dimensions adapted from Thomson & Perry [22]

DIMENSION	DESCRIPTION	HOW TO ACHIEVE
Governance	Making joint decisions about rules to govern the collaborative effort.	*"Creating structures that allow to make choices about how to solve the collective action problems they face by developing sets of working rules about who is eligible to make them"*
Administration	"*Getting things done through an effective operating system that supports clarity of roles and effective communication channels*".	Implementing and managing administrative structures for agreeing goals and coordinating activities to achieve a goal.
Organizational Autonomy	*"Addressing the implicit tension exhibited in collaborations between organizational self-interests and the collective interests of the group"*	*"Achieving individual organizational missions and maintaining an identity distinct from the collaborative, and a collective interests".* Maintaining accountability to collaborative partners and their stakeholders.
Mutuality	Working through difference to arrive at mutually beneficial relationships	Keeping interdependence, obtaining mutual benefits interpedently, based either on differing interests or on shared interests.
Norms	Developing trust and modes of reciprocity	Promoting reciprocal benefits and obligations. Besides the ''I-will-if-you-will', partners m will equalize the distribution of costs and benefits over time out of a sense of duty.

The above table summarizes the collaboration dimension´s, proposed by Thomson & Perry [21]. The five categories of the multidimensional perspective are listed on the first column; second describes the main features and the expected results; and third exemplifies possible ways to achieve collaboration. This compilation only suggests the importance of these properties on the implementation of collaborative mechanisms. However, it would be necessary to make measurements in practice and enclosed within a community or a circle of stakeholders, to make an empirical interpretation of collaboration on cybercrime investigations.

Cooperation to Fight Cybercrime

The found literature refers to terms associated with collaboration and cooperation as synonyms or supplements. This could be because there is not sufficient awareness of the proper use of these terms and the differences have not yet been fully clarified. However, it is important to recognize that there is a standard relative level of awareness on the need of incorporate efficient models and methods, but each of these terms represents diverse forms of contribution to a group and each comes with its own dynamics and power structures.

The definitions studied in the literature review suggest that cooperation has a lower level of action than collaboration. On the one hand, collaboration refers to the sum of individuals who come together to reach to an end, and on the other, cooperation is the need to interact with individuals to come to an end [25]. For the purposes of this work, it is important to perform a wide differentiation in the use of these terms, interpreting the concept of cooperation as the arrangement or process with the aim of uniting a group, in which different stakeholders come together voluntarily to meet their individual interests, with independent goals in combating cybercrime.

Diferent scholars and practicioners have discussed extensively on the importance of implementing high levels of cooperation among stakeholders in the fight against Cybercrime. For example, Brown states that responses for private sector assistance are generally slow creating difficulties to cybercrime investigations, prosecution, and interrogations. The acceptance of mandatory cooperation could affect the efficacy of police investigations, and jurisdiction goes beyond international borders, delaying the work of investigators in bringing offenders to justice [5]. The Police Executive Research Forum PERF says that investigators are frequently confronted with legal constraints on criminal justice process, they require more streamlined cooperation with Internet Service Providers ISP, private corporations and other local, state and federal agencies when investigations crosses multiple jurisdictions [9]. ENISA works also emphasize on the promotion of informal discussions and face-to-face meetings with regular intervals, moderated or facilitated by regulatory authorities, to help in the establishment of trusted platforms and improve information flows between stakeholders [6].

The importance of cooperation is also highlighted on the Budapest Convention, which is the most accepted guideline for domestic legislation, and used as a framework for international cooperation. It emphasizes the need of enhancing cooperation through the effective application of its standards, and supporting others bilateral, regional and international agreements on cooperation. It is evidenced in Articles 23 to 35 in relation to international cooperation, extradition and mutual assistance, including legislative adjustments and improved procedures police-to-police and judicial cooperation. Moreover, Articles 29 and 31, stated on international preservation requests and the commitment made

by participants in compliance with the principles and guidelines given by the convention and the Cybercrime Convention Committee.[38].

A wide range of cooperation requirements has been discussed through various initiatives and mechanisms of participation at international, regional and local levels. They agree on the importance of incorporating cooperation factors on cybercrime strategies. For instance, United Nations (UN) provides assistance to countries to develop cybercrime strategies, especially in legal and procedural support, and regional and international instruments for cooperation [7]. The International Telecommunication Union has highlighted the importance of cooperation with governments and the private sector, specially on international spheres [36]. Current models of cooperation are not satisfactory effective, they are based on analogous or traditional investigations patterns or demands in the real world, but cybercrime is transnational in nature, which means that is not restricted to a single crime scene [39]. Consequently, it appears that decision-makers should take into account for the implementation of strategies against cybercrime, the inclusion of such cooperative efforts to meet the needs of LEAs on conducting international cases, joint investigations and coordinated responses.

Some of the existent initiatives to support the work of LEA's are focusing efforts on implementing strategies assisting complex collaborative decision-making. Police forces and investigation agencies at local, regional, and international levels are more aware of working under collaboration and cooperation schemes. For example, the European Cybercrime Centre EC3[8] was established to strengthen law enforcement response to cybercrime in the European Union (EU). They concentrate their efforts in helping to protect European citizens, businesses, and governments, providing a variety of strategic analysis products supporting decision-making. The Global Cybercrime Expert Group 2014 INTERPOL[9] was created with the aim to advice on policy formulation, the implementation of cyber programs and operations. They promote the exchange of information and best practices, and assistance in developing long-term cybersecurity strategies in the world. The AMERIPOL Cybercrime Center [10] is an emerging interagency collaboration initiative between INTERPOL and EUROPOL, created in response to the need for preparation of cyber police in the development and specialization of criminals and terrorists. PERF also mentioned the role of LEA's in preventing and investigating cybercrime, and the need for developing comprehensive strategies to overcome different obstacles [9]. They also remarked on underreporting of crimes by individuals and corporations, inadequate awareness of this issue by public officials and the public, and difficulties in handling crimes that stretch across multiple jurisdictions. The FBI National Cyber Investigative Joint Task Force NCIJTF[11], supports information sharing, incident response, joint enforcement and intelligence actions among national and local communities. The UK National Cybercrime Unit NCCU[12] helping the fight cybercrime by providing experience and response to cyber threats. The Bundeskriminalamt BKA[13] has established support mechanisms by the "Service Center for Information and

[8] Available: https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837
[9] Available:http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
[10]Available:http://www.ameripol.org/portalAmeripol/appmanager/portal/desk?_nfpb=true&_pageLabel=portals_portal_page_m2p1p2&content_id=66089&folderNode1=66002
[11]Available: https://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1
[12] Available: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit
[13]Available:http://www.bka.de/nn_194550/EN/SubjectsAZ/InternetCrime/internetCrime__node.html?__nnn=true

Communications" and the "High Tech and Computer Crime".

The adherence and participation on the presented initiatives could be considered as very useful and profitable tool for managers for supporting decision-making. This brief compilation of actions shows that given the growing threats on cybercrime, there is a concern and awareness of the benefits of establishing or joining mechanisms of cooperation and mutual help. However, this does not preclude the obligation of countries to act independently, adjusting to their particular needs and prioritizing internal resources to fight crimes. This could also indicate that stakeholders could prefer to concentrate their efforts in requiring more cooperation, rather than offer or provide it.

Cybercrime Information Sharing

In the context of cybersecurity, there is a more or less general agreement that collaboration and sharing of information help reduce risks, but also, there are some confusion and controversy surrounding their implementation. Information sharing has become a common term within the cybersecurity community, but there is no certainty of what and when exactly should be shared, how much ought to be shared, and what can be done with the information shared [28]. The importance of the acceptance and implementation of common information patterns sharing in cooperation models could be considered useful to improve the quality of the information collected for decision-making. This could allow others to reduce risks, defend, detect and improve responsiveness to the cybercrime in a harmonized way.

For the purposes of this work, it might be advisable to appropriate the concepts and differentiation of terms suggested by ENISA works. In this regard, information sharing could be interpreted as the good practice for the exchange of a cybercrime related information between one trusted part to another. It could be a variety of data related to risks, vulnerabilities, threats, security issues and provision of information to support the criminal investigation process. The organizational interaction among stakeholders could be accessible by disclosure, broadcast, sharing, and exchange of information [30].

ENISA's efforts are also focused on information sharing needs between CSIRTs and LEAs, with the aim to enhance cooperation between members' states on the European Union (EU) when combating cybercrime. They found that some of the main obstacles in the exchange of information are prevalent in the current lack of standardization and misunderstanding on how to perform the exchange, limiting the amount of information that can be shared, and the possibilities of automation of these processes. Their proposals depart from the construction of new mechanisms based on a common taxonomy, and following a roadmap for this implementation [40] Some of these arguments coincide with the High Technology Crime Investigation Association HTCIA [41][42]. They have claimed the need for promoting ideas for training, education and information sharing between law enforcement and corporate cybercrime investigators, based on the promotion of voluntary exchange of information, experiences, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies in the field of cybercrime.[41] Their reports conclude on the need of improvement of information sharing and collaboration between law enforcement and corporate cybercrime investigators, and the establishment of cyber crime reporting, strategies, and policies [41], [43], [44]. The results of these studies demonstrate the emerging need to share information among stakeholders and emphasize the need to increase levels of awareness, promoting the construction of a policy, legislation and mechanisms of participation. In addition, they note the disadvantages of not having this form of collaboration, and weaknesses in relation to the growth and professionalization of criminal activity on cyberspace.

In contrast, the implementations of such solutions are not entirely accepted by some actors. Sometimes they are reluctant to share information because fear of liability if shared information turns out to be wrong or causes unintended damage. Also the tendency to avoid loses of prestige; face legal conflicts on freedom of information, and worries that shared information might be used against the company by regulators. Effective information sharing requires the government to share fully and in a timely manner with the private sector through a public-private partnership established for this purpose [45]. Experts have criticized the expected efficacy of information sharing and the provisions for clarifying ambiguities, agreeing on the convenience but also concerned about privacy issues. When the legislation goes from theory to practice, the exchange of information is positive with benefits for companies under attack, but the rules of procedure will delay the process. They acknowledge that criminals are well organized and can act rapidly and undeterred by the laws and procedures, while institutional action is slow, paced and constrained by the law [46]

In summary, understanding the practice of sharing information as a form of collaboration, it can be seen that today the need for the implementation of this practice as support for cybercrime investigations is increasingly accepted. The implementation of these models at organizational levels is currently promoting, and the greatest needs are in the supply of information by private sector and other investigation agencies. However, there is also a resistance level of participation of this practice that should be recognized and treated in depth by decision-makers, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing. In addition, most of the arguments studied agree on the importance of voluntary exchange of information, but also on the possible disadvantages and risks involved. Mandatory mechanisms might not be suitable in all cases because these do not constitute genuine cooperation and could be coercive. However, voluntary agreements could drive organizations with privacy issues that just avoid the exchange of information, as they can keep getting useful information from the government and different stakeholders, causing setbacks or lack of trust in the practice of sharing information.

Strategic Decision-Making On Cybercrime Investigations

According to the Institute of International Management Sciences, the practice of decision-making could be a difficult exercise. It is the product of deliberation, evaluation, and thoughts that managers follow in a sequential set of steps into a process [31]. Models of these processes have been presented by several researchers in the literature [33]. However, the one proposed by Baker seems standard and also is widely accepted in the literature. It starts from *"the identification of actors, reducing the possible disagreement about problem definition, requirements, goals, and criteria"*. Then, it is conducted by defining the problem, determining the requirements that the solution to the problem must meet, establish goals that solving the problems should accomplish, and identify options and other alternatives. Finally, by developing evaluation criteria based on the aims, selecting a decision-making tool, applying it to select a chosen alternative, and verifying the solution found to make sure it solves the problem [47].

For this work, it could be appropriate adapt the interpretation of decision-making concept as the process of selecting a course of action among several alternatives achieving a predetermined goal, choosing the one that will produce the most desirable benefits and the less unwanted consequences. This definition seems to be consistent with most of the concepts studied in the literature review and contains most elements needed to bring it within the context of this work. However, it also is important to follow the Baker`s model,

which involves the identification of the decision maker and stakeholder, reducing possible disagreements about problem definition, requirements, goals and criteria. [47]

The efforts of this theoretical precision are concentrated on strategic management of LEAs when dealing with cybercrime. In this context, heads of these agencies are expected to play many roles in a case investigation; they must be better qualified to guide its collaborators and help to achieve their goals. However, it could not happen only following a series of steps; it might also be developing a set of attributes of leadership and human, conceptual, technical and personal skills, which allow managers to obtain the desired level of maturity and experience as an advantage in a high capacity for decision-making.

In this regard, a generic crime scene could be viewed as a particular case of collaborative decision-making. Once the agency responsible for conducting the investigation is aware of the occurrence of cybercrime, they should express their interest and need to deal with it. The lead investigator might face the requirement to convoke a group of experts from different profiles that help to contribute to their knowledge and experience to understand and make traceability of the criminal activity presented. Then, leaders will face a scenario of decision-making, which implies the involvement of a vast number of individuals and groups that need to communicate with each other, by sharing information and taking decisions through many levels and limits. Also, according to the conditions and unique features of the nature of cybercrime treated in this study, decision-making have to deal with several variables such as management procedures, legal and procedural obstacles, privacy questions, trust issues, interest from partners, technical barriers, delays, or mandatory mechanisms, among others issues.

Managers of LEA have to face the responsibility of failure or success in a cybercrime investigative case. The outcome will depend on the quality of the decisions taken, and how obstacles are overcome [31]. They must make smart and sound decisions while performing managerial functions such as planning, organizing, staffing, leading, and controlling [33]. Sometimes they have to act under limited availability of time or resources, think under pressure, with low quality of information or using only their experience or intuition [34] [35]. The heads of LEA have to deal regularly with complex collaborative decision-making in cybercrime cases, in determining what investigation practices or expertise has to be used to address the complexity of supporting teams. They have to evaluate the origin of the data and evidence, deciding how it could be assembled and correctly used in criminal investigations. Also, they have to determine who are responsible for establishing the scope and boundaries of the investigation, how to build a common language among forensic investigators to facilitate collaboration with each other and with other actors, and how to deal with logistics and negotiations [8].

Organizational Interaction Mechanisms Combating Cybercrime

Since the literature review evidenced the need of LEAs to implement mechanisms of collaboration, cooperation or information sharing in the fight against cybercrime, there is not sufficient clarity about the appropriate use of this terminology, and in some cases, it could overlap and confuse stakeholders when attempting to establish any collaborative mechanism. For this reason, it is important to make clarity of the meaning and scope of each of these concepts, to avoid indiscriminate use, employing appropriately terminology in what kind of mechanism is required and helping on the implementation of a common language for cybercrime investigations.

In this regard, adopting the concept given in social sciences by Berger & Luckmann, the interaction could be interpreted as *"The process by which people act and react in relation*

to others. Partners agree on their goals, negotiate behaviour, distribute resources, and include activities such as exchange, competition, cooperation, conflict and coercion"[48]. The term organizational interaction could be appropriated on the delimitation of these three types of mechanisms, referring to any action that occurs among stakeholders, having an effect upon one another, and specifically for referring to the relationship of LEAs with stakeholders in which the object of this study is concentrated

In this regard, the main interest of establishing organizational interaction mechanisms between stakeholders and LEAs is to achieve mutual benefits toward the investigative process. Managers could refer in applying to any of these mechanisms in specific requirements, depending on the context, purpose, and scope of each need of interaction. Collaboration applies when working alongside to achieve something. It is practicable when there is a jointly defined mission, shared goals, using shared resources and sharing mutual interests. By contrast, cooperation is achievable when interaction enables greater ability to perform activities, usually by providing information or resources that are limited in the investigative process. At the contrary of collaboration, there is not necessarily typically defined mission, goals are independent, and stakeholders use their resources pursuing private interests. Moreover, collaboration requires clear communication channels, longer commitment and involves cooperation to achieve its aims. Instead cooperation, it could be informal, limited in time, and it does not require collaboration in practice. Finally, authority and autonomy are retained by each organization in cooperation, so there is virtually no risk. Instead in collaboration, it is coordinated, and therefore, it has a higher risk.

Information sharing was described as the good practice for the exchange of a cybercrime related information between trusted parts. The practice of doing it could be obtainable by sending and receiving tacit information to support the criminal investigation process. It could be accessible by disclosure, broadcast, sharing, and exchange of information, and the organizational interaction among stakeholders might occur in both collaboration and cooperation mechanisms.

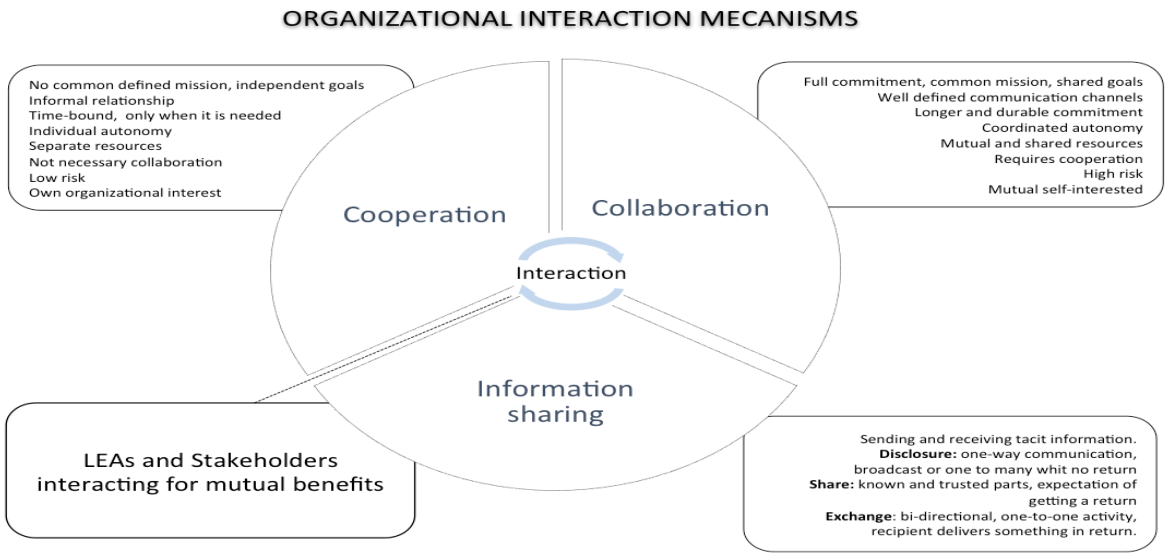

Figure 1. Organizational Interaction Mechanisms on Cybercrime Investigations

The above figure summarizes the main features and differences in terminology related to the phenomenon under study. At the center, the three mechanisms explored in this section are located to denote to organizational interaction between LEAs and stakeholders for mutual benefits. The squares in front of each term refer to the description and differences

in the terminology studied. The differentiation and proper use of this terminology could allow stakeholders to apply precisely in establishing any of these mechanisms, avoiding confusion and delays in the provision of information or other resources. Moreover, by understanding the purpose and scope of each requirement, managers could get more benefits in improving information flows to help the cybercrime investigative process.

4.2 Contextualization of the Cybercrime Field Process Analysis

Identifying Cybercrime Stakeholders

According to ENISA, investigators must act quickly and efficiently in the exchange of information, interacting with a broad range of stakeholders, promoting free flows of information and overcoming many legal, regulatory and operational obstacles [29]. But, as Brenner stated, in most cases cybercrime investigation competencies are exclusively reserved for law enforcement officers [39]. Therefore, the success of the investigation process on cybercrime investigations could be improved having clearly identified who are the most important players and what kind of information they can exchange.

According to the Dutch experience, an upright stakeholder administration keeps track of the information needs and promotes relationships of trust among community members. This could be achieved with the establishment of clear rules, understanding interests from partners, and maintaining feedback trough reliable communication channels [12]. The Microsoft cybersecurity framework states that the evaluation of stakeholders requires the analysis of interests and needs of each actor, because they may have a variety of backgrounds, capabilities, skills and motivations, and the articulation of the unique needs is a fundamental part of building trust [28]. Martin & Rice have identified a broad range of stakeholders involved in various aspects of cybersecurity matters, including government, private critical infrastructure, business enterprises, IT companies, IT security firms and security researchers, among others. [28] To have a detailed view of the stakeholders in cybercrime investigations, this stakeholder analysis, could guide this work. The analysis also considered a broad range of actors including an extensive list of interested parties that could serve as a basis for understanding and manage organizational interaction needs regarding the phenomenon under study.

Table 2 Cybercrime Investigation Stakeholders, adapted form Martin & Rice [49]

CYBERCRIME STAKEHOLDERS	
Governmental organizations	Ministries and state governments agencies. National Emergency response Team CERT Domestic Law Enforcement Agencies (Police cybercrime unit) International law enforcement agencies Prosecution or judicial authorities Federal legal and financial regulation agencies Federal and State Privacy Commissioners Military and National security organizations. National Intelligence agencies, community. Federal technology policy and regulation agencies International government organization Government business enterprise
No Governmental organizations	Information and technology special interest groups Financial industry special interest groups Not-for-profit businesses Tertiary level research centers (covering technology and law) Educational institutions/academy
Public and private companies	National Critical Infrastructures CI. Telecommunications and Internet service providers ISP Banking and Financial companies. Sectorial emergency response Teams CERT-s, CSIRT, SOC. Security software businesses enterprises Consulting businesses enterprises
Individuals	Individuals participating on Internet domain. Independent researchers. Citizens Victims/ witnesses

The above table compiles most of the stakeholders involved in cybercrime investigation processes. The first column titles the four broad categories, and the second list all of the interested parts involved in organizational interaction. This categorization is based on the mentioned study of Martin & Rice and complemented with other actors such as citizens, victims, witnesses, other cybercrime units and CERTs, considered relevant for LEAs [49]. Although all of the stakeholders related can be considered important for organizational interaction, this work only refers to the four main categories.

Cybercrime Key Players Analysis

For a complete overview on the current state of cybercrime and its perpetrators, it is important to identify who are the key players from the criminal perspective, determine their roles and how might they affect the stages of the investigative process. In this regard, considering the relevance of the analysis of attackers made by the ecrime project [35], it could be appropriate to integrate these elements in the study of the organizational interaction in cybercrime investigations. The study confirmed that crimes are usually perpetrated by hackers, former employees, organized criminal groups, current employees, customers, competitors, political and protest groups and terrorists. Cyber criminals have been analyzed, described and classified into four general types of players: International criminal organizations, foreign intelligence or states, legitimate organizations, and individuals or small groups. The outcomes of the investigation and its categorization could be visualized in the table 3.

Table 3. Cybercrime Key Players, based on ecrime project [35].

PERPETRATORS	DESCRIPTION	
International criminal organizations	Organized Crime	Highly qualified individuals specialized in the use of IT. Create or join to organized international crime. Generate incomes from illegal activities, or affect governments.
	Virtual criminal networks	Specialized members (hacking, spamming, denial of service, etc.). Working separately and coordinated by a core member. Operating under a secret structure and strict rules. Using nicknames, forums, and not personal meetings.
	International hacker groups	International crime with temporary affiliation. Promoting free flows of information, uncensored communications. Claiming invalidity of copyright, patenting and Internet surveillance.
Foreign intelligence agencies, states	Use of state intelligence agencies to perpetrate attacks against foreign governments. Targeting on intellectual property, awarding contracts, industrial or military espionage. It can be confused with cyberwarefare when criminal cyber hack ends and where some type of state or state-sponsored event begins.	
Legitimate organisations	Institutions, organizations or private companies committing crimes such as IP theft, industrial espionage, etc., for increasing competitive advantages.	
Individuals and small criminal groups	Perpetrators generally motivated for financial gain, paedophile, recreational or hacktivism purposes. Attacks may be planned or opportunistic. Sophistication depends on the resources.	

This summary of the key players is based on the ecrime project but adapted to this work according to the original analysis [35]. The very first column lists the categories of perpetrators. International criminal organizations are divided on three subcategories, and the last column describes behaviours, motivations and some examples of modus operandi of perpetrators. This categorization suggests that besides these categories, the actors not only act individually, and they can interact with each other. There is also a marked hierarchy according to their capacity of resources. While worldwide criminal organizations and states have greater resources, capacity to support and coordinate activities, they can control small criminal groups and individual hackers committing crimes. Also, each actor might have multiple affiliations to different criminal organizations and can play multiple roles simultaneously. Theses cases could indicate the

complexity of the investigation process in a large-scale criminal activity that could involve the efforts of many players at the same time.

Cybercrime Ecosystem Analysis

A full description of an entire ecosystem of cybercrime is a clue but a hard task, because of the complexity of actors, constant changes, and rapid evolution. However, the ecrime project has proposed a general guide identifying the key roles in cybercrime networks that could be used as a general guide for better understanding cybercrime spheres. The main factors affecting the ecosystem and criminal roles could be summarized as follows:

Table 4. Criminal Roles on Cybercrime Ecosystem, based on ecrime project [35]

FACTOR/PLAYER	DESCRIPTION	EXAMPLES
Criminal Zero	Individual or group that directly interfaces with victims. Primary beneficiary of the crime.	Criminals, organized crime.
Organized Crime and Black Market	Criminals exchange products, goods, services, illegal content, tools, and traffic information. Generally by forums or encrypted and private messaging.	Silk Road, Blackhole Exploit Kit, carder.su, etc.
Criminal Service Providers	Providers of illegal services, used by other criminals as proxies.	Outsourced malware, DoS attacks.
Developers	Facilitators of specific and customized IT development services for perpetrating cybercrime.	Tools, exploits, malware, botnets.
Infrastructure Providers.	IT providers, independent of conventional, facilitating and enabling cybercrime.	Bulletproof hosting
Monetization Service Providers	Irregular service providers facilitating the delivery of goods and services traded by illegal activities.	Extortion payments, mules.
Victim	Person or entity affected by cybercrime	Individuals, organizations, Internet users.
	Intermediate victim: used to attack the end victim.	
	End victim: final target, ultimate goal of criminal 0.	
Corruption	Occasional factor facilitating the perpetration or affecting efficiency of the investigation.	Immorality, bribery, sabotages

This summary table is based on the ecrime project study but adapted to this work according to the original analysis [35]. The first column lists the identified players or factors affecting the ecosystem; the second describes the structure, modus operandi, and the role of each player; and third, exemplifies cases and conducts to perform cybercrime. It is important to recognize that because of the complexity and constant changes of the ecosystem, the scenario may evolve, not all cases are identical, and not all factors could intervene in every case. This representation might be used as a general bases analysis, and not for any particular behaviour or a specific criminal. To achieve a deeper and detailed analysis, of organizational interaction, the factors should be adjusted to a concrete case or criminal network features, and recognizing what stage of the investigative process has affectation or would require intervention

Cybercrime Cycle Analysis

The purpose of describing cybercrime in an overall visual representation is to understand the sequence of operations that are performed to commit a crime. Through visualizing the cycle from the criminal side, the heads of LEAs could identify with precision what stage of the process may require intervention or resources by the stakeholders, understanding the whole structure and concentrating efforts on solving specific problems in the investigative process. According to the ecrime project, the resources required and the decisions taken in committing a crime could determine the modus operandi of cybercrime. The study of cybercrime cycle represents most of the cyber criminal behaviours from the perspective of the criminal side. The outcome of the study is a high-level journey map showing a broad spectrum of cybercrime acts that could be used as a basis for more detailed analysis in different typologies of crimes [35].

The study has divided the cybercrime cycle in three main phases: The first, preparation includes pre-attack actions, initial decision, evaluating reconnaissance of target, value of attack, choosing a victim and attack methods. Criminals may use their own abilities, outsourcing services or buying solutions. The second, execution comprises the creation and implementation of a plan, interfacing with the target system and conducting criminal activities. And the third, monetization involves the payment, different modus operandi, and the way to get profit or personal gain. Although the report also mentioned the motivation factors affecting the cycle before the preparation, it was not considered by the project or this work, because it does not change the steps required to complete a crime.

Table 5 Cybercrime Cycle, based on ecrime project [35]

CYBERCRIME CYCLE DESCRIPTION			
Preparation	Market research, taking the decision, evaluating opportunity, weighing costs and benefits. Choosing a victim, the method and deciding to execute	Using own means or abilities	Botnet, malware or exploit
		Acquiring from another criminal.	Seller, broker, deal-breaker, developer or programmer
		Crime as a service: hiring a outsourcing service	By specific forums, markets and online stores.
Execution	Conducting the attack plan	Gaining access to victim resources	By using malware, drive-by downloads, user actions, etc.
		Mapping the compromised network	Deploying additional malware
		Interacting with the target system and taking actions	Hacked PC: taking over for illegal activities
Monetization	Materialization of payments in four ways	Victim pays to Criminal Zero directly	Extortion, ransomware, or DDoS extortion schemes
		Victim resources are turned to tangible assets	Trade, sale or purchase of assets.
		Criminal Zero pays for ordered services or goods to another criminal	Real money, crypto currency, re-sellable, money equivalents (i.e. gaming assets).
			Goods and services (real or virtual, legal or illegal).
			Buying and/or bartering other goods and services
			Using laundering services, mules.
		Criminal Zero access to victim resources	Personal gain

This summary table is based on the ecrime project study and adapted to this work according to original analysis [35]. The very first column lists the three main phases of the cycle; the second describes the activities performed by criminals to conduct each phase; the third includes the description of how criminals obtain the expected results; and fourth includes examples to illustrate the materialization of the crime. Although the original purpose of this study is to analyze the economic impact of non-Information and Telecommunications Technology (non-ICT) sector, this can be considered an important tool to visualize how it affects the entire ecosystem. It also could help to understand the nature of needs and the current state of organizational interaction during cybercrime investigations.

Current State of the Organizational Interaction During Cybercrime Investigations

Due to the complex structure of the cybercrime development, the ecrime project has focussed efforts on an exhaustive and detailed analysis of several aspects, structures and stages of cybercrime from different angles. The study describes the economic effects of cybercrime in the non-ICT sector, identifying taxonomy and inventories, evaluating counter-measures and mapping cybercrime journeys, to develop measures and methods to deter criminals and limit their actions [35]. Given that this project has collected valuable sources of information from the literature, and has developed a recognized great contribution in building information to combat cybercrime, it is appropriate to take it as a

reference for the phenomenon under analysis and for the purposes of this work.

To represent a general idea of the cybercrime ecosystem interrelations and understand its current state, this study has compiled most of the elements considered throughout this work, with the intention to present a reliable current state of organizational interaction during cyber-crime investigations. With graphical representations of key cyber players, stakeholders, cybercrime cycle, and understanding the cybercrime ecosystem; it can be obtained necessary elements for future analysis and evaluation of any problem related to cybercrime. Moreover, by mapping these elements, managers of LEAs, or anyone interested in making improvements to the investigative process, could get a holistic view of the phenomenon and propose solutions to strengthen weaknesses where more attention is required.

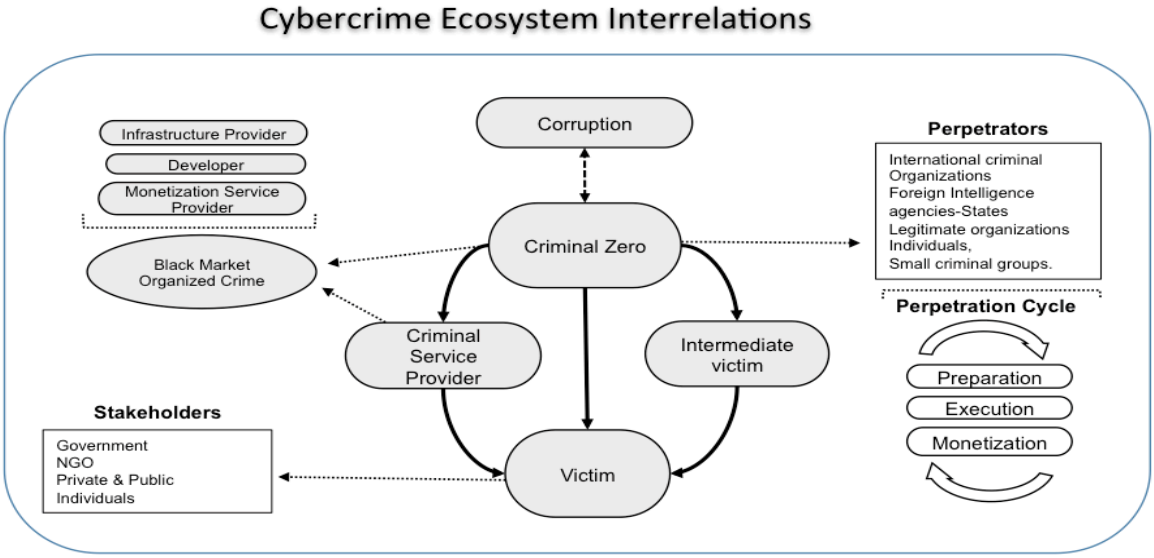

Figure 2. Cybercrime Ecosystem Interrelations, adapted from ecrime project [35].

The above figure is based on the extensive work of the ecrime project and the analysis of organizational interaction studied in this work [35]. This represents an advance for understanding the current state of organizational interaction ad the interrelations on the cybercrime ecosystem. In this regard, cybercrime comprehends diverse criminal activities where computers and information systems are involved and undertake many factors and elements described as follows. The figure includes the four principal groups of elements: Stakeholders, perpetrators, the cybercrime ecosystem, and the cybercrime cycle. On the left side are the stakeholders, represented in this figure as the victims, which were explained and described in this section in table 2. On the right side are the perpetrators, which also were studied on in this section and summarized in table 3. The factors and players affecting the cybercrime ecosystem were explained in Table 4, they are located at the center of the figure, and represent the criminal interactions to attack a victim and commit a crime. Finally, the perpetrator conducts activities to commit a crime through a perpetration cycle compound by the phases of preparation, execution, and monetization explained of table 5. The graphical representation summarizes the most critical components and the interrelation of these elements within the cycle and the ecosystem. It also provides valuable components for facilitating the analysis, contextualization, classification and categorization of the phenomenon under study. This material could be considered as a guide to help to understand the problems associated with the investigation process and its stages, obtaining a broader view for solving specific problems, and in particular, for identifying challenges and needs faced by decision makers of LEAs.

5 Practical Applications

This section describes the analytical sequence that leads to the weaknesses and intervention needs' identification in five stages. Five of the most representative types of investigation processes that depart from diverse perspectives will be compared first. Then, an optimized investigation analysis model, based on needs of organizational interaction, will be proposed. Next, the work will present a compilation of the collaboration, cooperation and information sharing needs of LEAs. Besides, the Colombian case study on organizational interaction will be introduced. Finally, how the perspectives studied in this work may apply is illustrated with a set of guidelines and best practices for the enhancement of the investigative process.

5.1 Modelling of Cybercrime Investigation Process

Acording to Roger & Achille, no clearly defined or standardized process for cybercrime investigations exist, or consensus on the definition of tasks to be developed for investigators at each stage of the processes [50]. It is also evident that among the procedures some proactive and reactive activities must be carried out to obtain evidence before to bringing a case before the court and to support prosecution. Despite multiple attempts to adopt an existing model, no instance seemed applicable to the objectives of this work. Models vary depending on specific contextual factors such as technical and regulatory scenarios. At the same time, there are enough similarities (not to mention principles and doctrines of universal observance such as the rule of law) to warrant an attempt to conceptualize a more general scheme.

By comparing different models of the detection of successful investigation requirements is facilitated. The identification of the steps that necessitate the most efforts on issues related to organizational interactions helps in turn the task of underlining possible intervention spots because weaknesses affecting decision making converge there. Without discarding the merits of other methodologies, formulated according to the needs and peculiarities of each investigation process, commonalities are picked from the following five consolidated types: Casey proposes an exhaustive model applied for managing digital forensic analysis on mobile and computer networks, dividing the process into 12 steps but emphasizing on the stages of acquisition, analysis and reporting [51]. Meanwhile, Lee does not discuss rather the full investigative process but marks four steps of the crime scene management: recognition, identification, individualization, and reconstruction [52] The first Digital Forensics Research Workshop (DFRW) proposes a 7 steps linear model for digital forensic analysis, developed for military, civilian, and law enforcement purposes, which is well known and used widely as a standard framework [53]. Mandia & Prosise, propose a model of incident response investigation procedures, focusing on management and quick containment of security incidents, business processes, and recovery, also consisting of seven steps [54]. A summary of the comparative exercise is summarized in table 6.

Table 6. Comparison of Cybercrime Investigation Models

	Roger	Casey	DFRW	Lee	Mandia
	Proactive, active and reactive activities analysis.	Digital forensic analysis management	Forensic Linear process analysis.	Physical crime scene	Incident response model
PRE	Alert	Accusation or Incident Alert			Pre incident preparation.
					Detection of incidents
		Assessment of Worth (prioritization)			Initial response
					Formulate response strategy
ANALYSIS	Identification	Incident/Crime Scene Protocols (Activities on scene)	Identification	Recognition	Data collection
	Collection	Identification or Seizure (recognition)	Preservation	Documentation,	Search for and identify evidence
	Preservation.	Preservation (integrity)	Collection	Collection	Collection of evidence
	Analysis	Recovery (hidden, deleted)		Preservation	Transport of evidence
		Harvesting (data)	Examination	Identification classification and comparison	Storage of evidence
		Reduction (Filter, eliminate)			
		Organization and Search (focus) Analysis (scrutinize)	Analysis	Individualization, link analysis, evaluation and interpretation	Data analysis
POST	Documentation	Reporting (detailed record)	Presentation	Reconstruction, leading reporting and presentation	Reporting
		Persuasion and Testimony (explanation)			

The compilation was drafted by compiling the five representative models of the investigative process marked on the first row by the name of the proponent. The column to the left shows the 3 classifications of the stages. According to the moment where the procedure takes place these are the preparatory, analytical, and posterior stages. The row below the perspective's name designates the nature and objectives of each model type.

From the text analysis of the terminology contained in the documents describing the models it can be can be seen that, although each model type meets specific requirements, was developed based on different methodologies and pertains a variety of activities, the categories of steps (pre, analysis, and post) could be applied. In addition, for assessment purposes, this way of systematization is simple and yet very useful to organize the sequences and patterns involved. All models at least imply preparatory activities (including the prearranged) that take place before the crime is noticed or alerted. Lead investigators perform planning activities when allocating resources and tools for the investigation, and the identification of potential sources of evidence. Next, investigators acquire and collect sources of evidence, preserving and preventing changes. Then, the evidence is analyzed, interpreted and traced, by using protocols, methodologies, and techniques and data interpretation tools. A final report communicates the results of the analysis and a decision. Later, after the forensic process has reached an end, continuous improvement and monitoring and control activities begin to happen. Blank spaces in the table show the steps that are missing from some of the model types.

The model proposed by Roger includes most of the components, incorporating a multidimensional-perspective. It summarizes the process in six stages of investigation considering the reactive, active and proactive phases and a set of activities on each stage. However, this model does not include the managerial elements that could be contained in the preparatory stage before the crime is noticed, nor after the delivery of the final report. For the purposes of this work, it will be necessary to explore the incorporation of these

new elements that could be essential to the analysis of needs of organizational interaction on cybercrime investigation levels.

5.2 Optimized Cybercrime Investigation Model

The aim of this model is not to discuss the effectiveness and appropriateness of existing models but to propose a sample or model of cybercrime investigation based on the needs of interaction with stakeholders and not merely on the procedural steps that are established by procedural laws, regulations and practices. This model expands the considerations towards strategic management domains where organizational interaction elements play an important role. Hence, aspects related to schemes of organizational interaction will be added, allowing more uses, for instance, the prioritization of efforts in the process stages that require intervention, and the enhancement of flows of information between certain stakeholders. The resulting stages, descriptions and activities developed in each stage are indicated in Table 7.

Table 7. Optimized Model of Cybercrime Investigation, based on Roger's [50]

	STAGE	DESCRIPTION	ACTIVITIES
1	Preparation	Strategic activities for planning, management and control the investigation process.	Founding clear objectives, specific, measurable, verifiable and achievable, according to the available resources.
			Identification of legal and procedural framework, barriers and obstacles.
			Training planning on forensic investigation techniques, legal procedures, use of ICT, acquiring knowledge and skills.
			Recognizing and evaluation available resources of cooperation.
			Establishing policies, plans and procedures to support collaboration and cooperation schemes to facilitate the exchange of information on the investigative process.
			Provision plan of resources and technical tools.
2	Alert	The process is activated with a complaint, alert, detection or notification. A management plan is developed according to risk and internal policies	Identify case regulations.
			Determine the assessment of worth.
			Incident confirmation.
			Obtain an authorization.
			Obtain a search warrant.
			Determine a containment strategy.
			Formulate an investigation plan.
			Coordinate the resources.
			Accelerate the investigation.
			Notification of the investigation.
3	Identification	Identification of possible sources of evidence, data and clues are prioritized and evaluated.	Identify data in the order of volatility
			Prioritization according to specific requirements
			Hostile and outstanding behaviours are also selected and catalogued.
			Identify all the electronic equipment used by the suspect.
			Identify and protect fragile evidence from plugging of the power cable.
			Obtain the maximum information from people present in the scene.
			Prevent form violating the jurisdictional laws and corporate policies.
			Classifying victims, suspects, bystanders, witnesses, etc.
4	Collection	Evidence acquisition or live collection of identified data and unusual behaviours, in a form which can be preserved and analysed	Choosing collection equipment or automated tools.
			Imaging storage devices, hard disks or seizure of entire computers.
			Collection of volatile evidence.
			Evaluating according to a specific situation.
			Capturing, recording, analysing network audit trails, discovering the source of security breaches or other information assurance problems
5	Preservation	Evidence collected is preserved and located in a safe place, ensuring of tempering, integrity, authentication, transportation, storage, documentation.	Applying hashing methods and tools to preserve evidence.
			Electronic devices must be photographed with all of the accessories
			What is appearing on the screen should also be documented
			A record of all visible data must be created.
			Establish "police line" to protect evidence of damaged cybercrime scene.
6	Analysis	Evaluating if evidence constitutes sufficient information for the reconstruction of the incident or it is in line with hypothesis.	Automated tools and forensic technics to analyse data (data mining)
			Revisit the investigation plan.
			Brief reconstruction of the case.
			Review the relevance of tools and expertise available.
			Develop the hypothesis.
			Analyze the evidence.
			Test the hypothesis.
			Make a finding.
			Validate the results of analysis.
			Documenting and securing activities
			Document the case
7	Report	Documentation and detailed report of findings.	Presentation of findings and probable cause to court or authorities.
			Reveal the root-cause
8	Post-Investigation	Monitoring and control of activities post processing	Translation and explanation
			Legal assistance on post crime process procedure
			Control and supervision by third parts
			Successfully prosecute a perpetrator
			Retraining and feedback
			Continuous improvement

The proposed optimization is based on Roger's multidimensional perspective six step model but unlike his, the investigative process distribution consists of eight phases that are numbered and listed in the first two columns to the left of the table [50]. The third column describes the phases functionally, and the fourth operationally, listing the activities that each phase comprises. To reduce the complexities associated with the different instances and operations required to complete the investigation process, organizational interaction or the schemes of collaboration; cooperation; and sharing information have to be implemented, involving all stakeholders identified in section 4.2, and grouped in Table 2.

Figure 3 proposes a visualized description of the need for organizational interaction during cybercrime investigation arises and should take place.

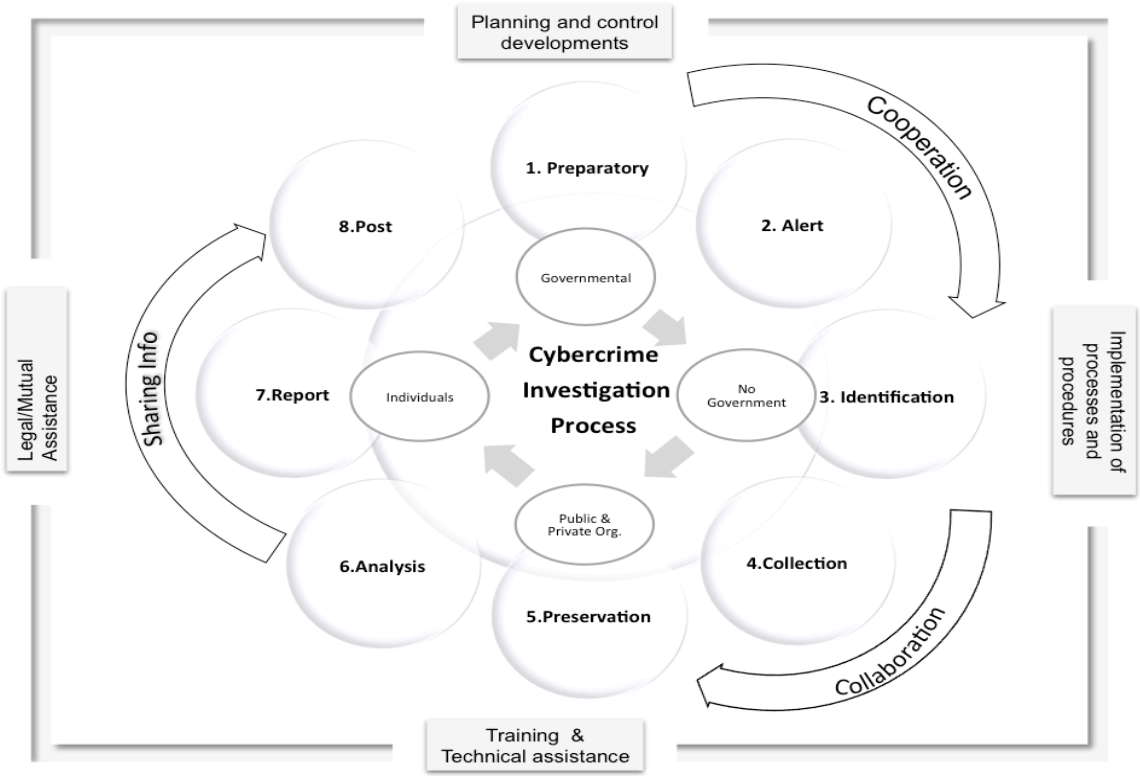

Figure 3. Organizational Interaction needs during Cybercrime Investigation Processes

The investigation process is at the center of the figure, surrounded by the stakeholders that in turn participate and interact during the eight stages located and listed in the circles. Placed the outer square are the needs grouped in the categories that are explained in section 5.3. The arrows show the mechanisms that correspond to the phenomenon of organizational interaction. All the components that appear in the figure are fundamental parts of the whole, not isolation, if to think of strategic decision-making and other managerial responsibilities such as planning and monitoring, within cybercrime investigations.

To assess the effectiveness of the optimized model is not a task of this thesis and falls beyond its scope. In fact the models that are available in the literature do not get statistical validation but are acceptable or not based on how sound the assumptions they put forward are and when they become accepted by practitioners and institutionalized in time. However, measurements on performance can be obtained under a different research design when enough information on its application can be collected. A construct for quantitative analysis based on empirical data is a promising option to support improvements in investigative processes, and would complement the model in the longer run.

5.3 Analysis of Needs During Cybercrime Investigation Processes

The general purpose of this section is the application of the optimized model for the analysis of needs of managers or LEAS during cybercrime investigation processes. In particular those concerned with collaboration, cooperation and information sharing. An extensive list of +100 needs collected and compiled from the academic literature, reports from ENISA and HTCIA was grouped according to their similarity on one hand and in an original categorization on the other. The resulting list contains 41 needs within four categories as presented in Table 8.

The application of the model seeks first, to identify the most pressing needs, meaning the most urgent. Second, the most recurrent, recognizing the frequency in which the needs arise. All of the above performed within the context of higher-level spheres. Additionally, the application of the model will allow managers to spot the stages of the process where organizational interaction is the most required or/and problematic and may require intervention. The work is also concerned on how to categorize the type of needs required, and how it fits according to the terminology adopted in this study.

The results of an analysis of needs based on this optimized model should persuasively indicate the importance of considering a model of cybercrime investigation based on the needs of interaction with stakeholders. It allowed the proposal of two stages that are ordinarily disregarded where the impact of prioritizing efforts would be the most beneficial. The establishment of the necessary conditions to facilitate the implementation and practice of the mechanisms of organizational interaction: collaboration, cooperation and sharing information among stakeholders cannot guarantee the success of an investigative process

Table 8 shows the summary of needs and the analysis made based on the proposed model. It includes the categorized needs, the stages of the investigative process and the organizational interactions interrelations. The sources of information were taken from the literature review, mainly from ENISA works 2010-2013, 2015 [6], [11], [29], [30], [40]; HTCIA 2010, 2011 [41] [43]; Gercke 2011, 2012 Brown [5]; [1] [36]; ITU [7]; PERF [9]; Broadhurst [10]; and Berdnar 2008 [8].

Table 8 Categorization of the needs of interaction on cybercrime investigations processes

STAGES	LAW ENFORCEMENT AGENCIES LEA's NEEDS	PRE	ALERT	IDENT	COLLECT	PRESERV	ANALYSIS	REPORT	POST	Σ Stages	COLLAB	COOPE	INF SHARE	Σ Mechanism
MANAGERIAL	1. Administration of management procedures, models or standards for collaboration success.	1	1	1	1	1	1	1	1	8	1	1	1	3
	2. Improving trust relationships, reducing difficulties getting a return from stakeholders.	0	1	1	1	1	1	1	1	7	1	1	1	3
	3. Avoid and prevent communication breakdown between strategic, technical and operational levels.	1	1	1	1	1	1	1	0	7	1	0	0	1
	4. Avoid and prevent conflict of interests.	1	0	1	0	0	0	0	1	3	1	1	1	3
	5. Avoid resistance due to the imposition of mandatory reporting.	1	1	0	0	0	0	0	0	2	0	0	1	1
	6. Promotion regular face to face meetings for exchange experiences, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies in the field of cybercrime	1	0	0	0	0	0	0	1	2	0	0	1	1
	7. Clarify information sharing policies, common benefits and goals among stakeholders community.	1	0	0	0	0	0	0	0	1	1	1	1	3
	8. Avoid and prevent excessive workload.	1	0	0	0	0	0	0	0	1	1	1	1	3
	9. Recognition and support from international community and counterparts.	1	0	0	0	0	0	0	0	1	1	1	0	2
	10. Promoting voluntary mechanisms instead mandatory, preventing wastage of efforts in formal agreements.	1	0	0	0	0	0	0	0	1	0	1	1	2
	11. Cooperation agreements with specific stakeholders (GOs, NGOs, courts, abuse teams, ISPs, security service providers, independent researchers, malware repositories, hosting providers, network operators, among others)	1	0	0	0	0	0	0	0	1	0	1	0	1
	12. Benefits of getting memberships to associations and organizations in the field.	1	0	0	0	0	0	0	0	1	0	1	0	1
	13. Promotion of cross-border law enforcement cooperation and Public–Private Partnership (PPP).	1	0	0	0	0	0	0	0	1	0	1	0	1
PROCEDURAL	14. Simplification of procedures and bureaucratic requirements in prosecutions, and digital forensics interrogations.	1	1	1	1	1	1	1	1	8	1	1	1	3
	15. Prevent and avoid providing erroneous information to divert or intentionally misleads the course of the investigation	1	1	1	0	0	0	0	1	4	1	1	1	3
	16. Provision of related information with responsibilities and ownership for IT Resources (IP addresses and URLs)	1	0	1	0	0	0	1	0	3	1	1	1	3
	17. Standardization on terminology reducing language barriers.	1	1	1	0	0	0	0	0	3	0	1	1	2
	18. Access to privileged information (Intelligence sources, according to domestic and international legal settlements	0	0	1	1	0	0	0	0	2	1	1	1	3
	19. Reduction of loss of quality of information or CIA proprieties of the data collected.	0	0	0	1	1	0	0	0	2	1	1	1	3
	20. Inclusion of control and supervision from communications regulatory authorities or collectively by industry.	1	0	0	0	0	0	0	1	2	1	1	1	3
	21. Open access to IoC Indicators of Compromise from specialized stakeholders	1	0	1	0	0	0	0	0	2	0	1	1	2
	22. Provision of automatic mechanisms for exchange of data.	1	0	1	0	0	0	0	0	2	0	0	1	1
	23. Regularity of flows of information with stakeholders.	1	0	1	0	0	0	0	0	2	0	0	1	1
	24. Provision of secure platform of communication channels.	1	0	1	0	0	0	0	0	2	0	0	1	1
	25. Prevention and reduction of exposure to loss of reputation due to sharing sensitive information.	1	1	0	0	0	0	0	0	2	0	0	1	1
	26. Avoid legal pitfalls on data exchange	1	0	1	0	0	0	0	0	2	0	0	1	1
	27. Protection of disruption or contamination of evidence in the chain of custody	0	0	0	0	1	0	0	0	1	1	1	1	3
	28. Access to mandatory reporting in accordance with current and local regulations.	0	0	1	0	0	0	0	0	1	1	1	1	3
	29. Timely processing requests for mutual legal assistance and supply of information	0	0	1	0	0	0	0	0	1	1	1	1	3
EDU /TECHNICAL	30. Optimized and up to date tools to support investigations and reports.	0	1	1	1	1	1	1	0	6	1	0	0	1
	31. Provision of technical tools: web portal or incident repositories, avoiding proliferation of communication channels.	1	0	0	0	0	0	1	0	2	0	0	1	1
	32. Assistance in process of information gathering and preparation of cases in court.	1	0	0	0	0	0	1	0	2	0	1	0	1
	33. Assistance on criminal investigations, providing expert testimony, collection or exchange evidentiary data.	0	0	1	1	0	0	0	0	2	0	1	1	2
	34. Assistance on conducting international cases, joint investigations, and coordinated responses.	0	0	1	0	0	0	1	0	2	1	1	1	3
	35. Assistance on post-processing crimes procedures	0	0	0	0	0	0	0	1	1	1	1	0	2
	36. Education, training in forensic investigation techniques, legal procedures, use of ICT, knowledge and skills.	1	0	0	0	0	0	0	0	1	1	1	0	2
LEGAL	37. Reduction of legal obstacles on delivery of information and privacy issues, harmonization on data protection law.	1	1	1	1	1	1	1	0	7	1	1	1	3
	38. Reduction of restrictions in a formal legal mandate for reporting crimes.	1	1	0	0	0	0	0	0	2	0	0	1	1
	39. Legal assistance on complaints or questions for sharing sensitive information, data protection and privacy issues.	0	0	1	0	0	0	0	1	2	0	0	1	1
	40. Legal assistance on jurisdictional issues associated to cross border gathering evidence and cloud computing.	0	0	1	0	0	0	0	0	1	1	1	1	3
	41. Legal framework that establishes commitments and obligations for private sector parties to cooperate with LEA's.	1	0	0	0	0	0	0	0	1	0	1	1	2
	TOTAL	**29**	**11**	**22**	**9**	**8**	**6**	**10**	**9**		**22**	**29**	**27**	

The first row designates the name of the columns where the first title is on the categorization of needs; the second on the concrete needs; from the third to the tenth the title indicates the stages of the model; the eleventh shows the total of times that a need repeats across the modelled process (recurrence); titles twelve to fourteen refers to the organizational interaction type (collaboration, cooperation or information sharing); and, the fifteen show the total of interaction types that each given need would require. In the rows below from the second to the forty-first are the categories of needs that are called: managerial, procedural, technical and educational, and legal, according to their salient commonalities. On the following column the summarized list of needs that were reduced from +100 to 41 that the next eight columns will recognize as appearing or not on each of the stages of the modelled process. These slots on stages are valued with "1" when organizational interaction needs are detected, or "0" when otherwise. Some of the needs might have impact in various stages simultaneously. The total of results is shown in the column that follows immediately ("∑Stages"). The three columns that are next refer to the type of mechanisms that are the most needed or typify the interaction, and the last show the total of these that can be also coincide in the case of some needs ("∑Mechanisms").

To restate, from the completion of this analysis, each necessity is assessed and classified within the established concepts of collaboration, cooperation and sharing information that should correspond to certain mechanisms of action (they are not specified on this section). Then, it is determined at which stage of the modelled investigative process the need compromises most or impacts management functions and responsibilities. It is observable on the table that a need could be perceived and therefore has impact on one or more stages of the process, depending on how pressing the need for interaction with stakeholders may be. Most of the requirements that investigators and managers are facing come from the preliminary and identification stages (having obtained 29 and 22 implications respectively, as shown in the row of totals at the bottom of the table), which are two added to the list by Roger [50], and these correspond to cooperation and sharing information needs, with a lower impact on the rest of the stages. The findings support the advantages of this model and the practical value of its formulation, because the most pressing and recurrent needs, and the stages where intervention is warranted become visible and can be acted upon.

Totals, however, do not necessarily mean that some needs may be of greater or lesser importance in a specific stage, the relevance of such categorization indicates that all identified needs are a fundamental part of the organizational interaction phenomenon, but most of these correspond to activities for strategic planning, management and monitoring the investigative process.

The analysis illustrated on the table evidenced that most of the organizational interactions gaps and weaknesses correspond to strategic activities for planning, management and monitoring the investigation process. This also indicates that if decision-makers acted on this information, they could handle these deficiencies early in the processes, namely, from the preparatory stage. Improved organizational interaction mechanisms could encourage the establishment of necessary conditions to facilitate the investigation of cybercrime. The following ideas are sample corrective tactics that should be applied to the intervention of the preparation stage, the most affected according to the analysis and where the managerial actions can have greater impact, in the shortest period of time:

1. The need number 1 could be resolved by developing management procedures, models or standards for organizational interaction since early stages of the investigative process. The strategies should intend to simplify procedures and bureaucratic requirements to cyber crime investigations, prosecutions, and digital forensics interrogations, reducing legal obstacles on the delivery of information, harmonizing data protection law, and privacy issues;
2. The need number 2 could be contented by promoting and establishing reliability in the investigative process. Trusted relationships among stakeholder community might avoid legal pitfalls on data exchange and decrease difficulties to getting a better return.
3. The need number 3 could be prevented by including secure platforms of communication channels that allow the provision of automatic mechanisms for exchange data, prevent and reduce loss the of reputation risks due to sharing sensitive information. The provision of technical tools (web portal or incident repositories, avoiding proliferation of communication channels), and the standardization of terminology, could reduce obstacles and language barriers on organizational interaction mechanisms;
4. The need number 4 could be overcome by clarifying organizational interaction mechanisms. However, improving trust relationships could require long-term strategies to increase reliability in processes and reduce conflicts of interest in stakeholders;
5. For needs 5 and 10, it would be necessary to evaluate the convenience of voluntary reporting instead mandatory, reducing restrictions in a formal legal mandate rather than mandatory, and preventing waste of efforts in establishing formal agreements with specific stakeholders;
6. The need number 6 could be meet by the promotion of regular face to face meetings, exchange of experiences, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies in the field of cybercrime;
7. The need number 7 by the clarification of information sharing policies, emphasizing on shared benefits of shared goals among stakeholders community, it could improve flows of information on cybercrime investigations.
8. The need number 8 by developing strategies for proper management of human resources, prioritizing cases and avoiding excessive workload of investigators.
9. For needs 9 and 12, the development of a positioning strategy to obtain recognition and support from international community and counterparts could be considered, accentuating on benefits of getting memberships to associations and organizations in the field of cybercrime.
10. The need number 11, requires cooperation agreements with Governmental and no Governmental Organizations, public and private companies, individuals, in regional, local or international organizations and specialized agencies. (Courts, abuse teams, ISPs, security service providers, independent researchers, malware repositories, hosting providers, network operators, among others).
11. The need number 13 by the Promotion of cross-border law enforcement cooperation and Public–Private Partnership (PPP). It may include control and supervision procedures from communications regulatory authorities or collectively by industry.

5.4 Organizational Interaction within the Colombia Cybercrime Centre CCP

The "Centro Cibernetico Policial de la Policia Nacional de Colombia", also known as DIJIN CCP, is the Colombian Cybercrime Center Unit. It is one of two investigative institutions established to conduct investigations and therefore an intended audience for the work henceforth contained. The unit belongs to the National Police, a greater structure where the CCP is ascribed. The legal framework on cyber security in place includes legal texts and public policy documents. The most important for the purposes of this section can be said to be. The National Cyber Security Strategy (NCSS) called "Lineamientos Para la Politica de Ciberseguridad y Ciberdefensa CONPES" which correspond to the National Planning Policy Guidelines on Cybersecurity and Cyberdefense" CONPES 3701/2011. In April of the present year, a new set of guidelines is to be issued and into place receiving the name "Politica Nacional de Seguridad Nacional" CONPES 3854/2016.[14] These documents are developed to meet the global challenges on cybersecurity while attending to the needs and requirements of the country. In the NCSS of Colombia issues cooperation are pointed out through the incorporation of priorities for implementing the appropriate institutions, providing training and strengthening legislation and international cooperation. National guidelines have represented the most advanced lean towards collaboration and cooperation at the initiative of the government. These clarify of roles and assign the responsibilities of the main stakeholders, and include essential managerial mechanisms of interaction as the ones discussed in this work, to support the fight against cybercrime. The objectives and guidelines of the NCSS of Colombia regarding linked to the phenomenon of organizational interaction mechanisms to facilitate the work of investigation and prosecution of cybercrimes can be summarized as follows. (The original document is in Spanish) [55].

1. The section IV, in pg. 20-23 and paragraphs A and B, are relevant to managers because it refers to the identification and recognition of the existing local and international regulations. The document adopts terminology and the establishment of bodies for effective and efficient prevention, investigation and prosecution of cybercrime;
2. The section A, in pg. 10-14, refers to the national existing initiatives regarding cooperation and collaboration between the government and all levels of the private sector. Paragraph 9 marks ways to deter cybercrime, recommending the implementation and development of legal frameworks related to cybersecurity that are consistent with international standards. It gives recommendations for the development of response systems, including monitoring and analysis and proposes guidelines for the implementation of a national culture of cybersecurity to improve levels of protection of information of the Critical National Infrastructure;
3. The section 3, in pg. 17, recognizes high levels of vulnerability and awareness with the increase of Internet users, critical infrastructure interdependencies, national electronic media, proliferation of incidents and crimes risks, threats and the persistence of impunity for handling such crimes. Managers should be responsive to the current situation to justify the need for organizational interaction;

[14] During the last weeks of the completion of this work, the new public policy document was released and became available on 11.04.2016 https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

4. In section d in pg. 25-27, the Police Cyber Center – CCP, is given a mandate with responsibilities in combating cybercrime within the national territory. It must for example offer information, support and protection against cybercrime by preventing, investigating and prosecuting computer crimes in the country, attending national guidelines and working in coordination with ColCERT and the Cybernetics Joint Command CCoC (Military);
5. The section 3 in pg. 19 paragraphs 3 recognizes regulatory weaknesses about data protection. Although there are legal and regulatory instruments, there are shortcomings that impede timely response to incidents and cybercrime;
6. The section B pg. 14 identifies the need of strengthening the legal framework to advance international cooperation and the accession of Colombia to various international instruments such as the Convention of the Council of Europe on Cybercrime (Budapest Convention). Managers could obtain benefits for judicial cooperation and extradition, adding to 24/7 point of contact, access to storage, and supply of logs by ISPs to facilitate investigations;
7. The establishment of the need to design and implement training plans regarding cybersecurity, investigation and prosecution of computer crimes to judicial police, judges and prosecutors and final users that page 18 contains under guideline 2 b concerns managerial activities;
8. Weaknesses on ISPs, regulations were recognized and discussed. For example in section 3 and page 19, describes the lack of policies to share information to authorities. Although these companies were obliged to implement security models to improve the security of their access networks, managers face difficulties for clear policies, storage and supply of information and logs in the fight against cybercrime;
9. If Colombia faces the challenge of positioning itself as a regional leader in the area of cybersecurity through sharing of best practices, knowledge, and experiences, with particular attention to the promotion of national expertise in the development process of the policy of cyber security and defense, cooperation, collaboration and sharing of information may be configured. In page 28 section 3 the text says that leaders and experts will participate in lectures, workshops, and specialized meetings;

Despite progress to achieve the objectives of this initiative, the period of validity have ended in 2014 and only at this time the national government is advancing efforts to develop a new strategy. However, given the complexity and evolution of cybercrime, other recent initiatives have been presented for incorporating mechanisms of interaction. For example, the creation of a high-level committee led by the Ministers of Defense; Justice; and Information Technology and Communications, to strengthen the existing policies and adapt to the challenges posed by technological advances and threats in cyberspace. The current cooperation mechanisms were activated convoking national government, internal cybersecurity agencies, Organization of American States OAS, World Economic Forum WEF [15], the Organization for Economic Cooperation and Development OECD, and the Council of Europe and Interpol [56].

Online Survey

[15] Accesible on: https://www.weforum.org/global-challenges/projects/cybercrime/

This work sought to find support from experts in considerations regarding the relevance and importance of organizational interaction mechanisms. Collecting information on these respects supports both research questions and the assumptions developed in the conceptual section of the thesis, it relates in particular to the research task 8. An online survey was distributed to obtain empirical data that could reaffirm the findings illustrated in Table 8 on the analysis of needs applied to the optimized modelling proposal explained in Table 7 and illustrated in Figure 3. The main finding to corroborate was the prevalence of certain organizational interaction weaknesses due to their urgency and recurrence and whether the expert group consulted coincided with the results. .

A survey was conducted including a questionnaire of 9 closed and one open question that asked about level of criticality (urgency and recurrence) of the organizational interaction needs that the Colombia National Police faces during cybercrime investigations. The questions referred to the most representative needs from the four categories taking into account the number of stages where they appear and the amount of mechanisms involved from the corresponding totals on Table 8.

The survey was administered in Spanish, the official language of the country, and then translated for this report into English. A convenience group was requested to participate based on expertise, occupation and ease of reach. The invitation was sent online to 90 officials from the National Police Cybercrime Unit DIJIN-CCP from Colombia, which forms its entire staff at the headquarters in Bogota. The group is in charge of administrative, operational, investigative and decision-making roles and responsibilities within the process of investigation of cybercrime in the country. The officials belong to different investigative groups according to the internal structure of the cybercrime center. The responsibilities and tasks of the investigative process are distributed in the groups of combating child pornography, financial crimes, cyber terrorism, critical infrastructure protection, forensic laboratory, citizen services (CAI Virtual), management and support.

The instrument was emailed to the corporate accounts of each of the officials directly. All potential participants were informed on the aim and nature of the survey and were asked about their perception of what are the major impediments, obstacles and requirements that criminal investigation process face regarding collaboration and efficient delivery and timely information by third parties in the investigation of cybercrime at the Colombia National Police. The answers to the questions posed were evaluated by respondents on a scale from 1 to 5, where 1 is the lowest value and 5 the maximum. One additional open question was formulated in order to obtain detailed information of the requirements that could not be contained in the questionnaire. The data collected and summary of results remains accessible online[16], a report is also attached to the appendix section.

Results description: 40 officials from the group of 90 responded the questionnaire. It represents a significant sample of 44% of the total base, sufficiently distributed among the different responsibilities represented, allowing significant collection of information. 75% of respondents execute operative and investigative roles; 15% perform administrative tasks such as management of resources and training, and 10% develop planning and control activities for decision-making. The summary of results and analysis for questions 1 to 9 can be visualized in the following figure 4.

[16] Accesible on : https://docs.google.com/forms/d/1-Vg8QXexWHBIoycIVRuKs7KVSanR5yTD48CBmy-OiyA/edit?usp=drive_web

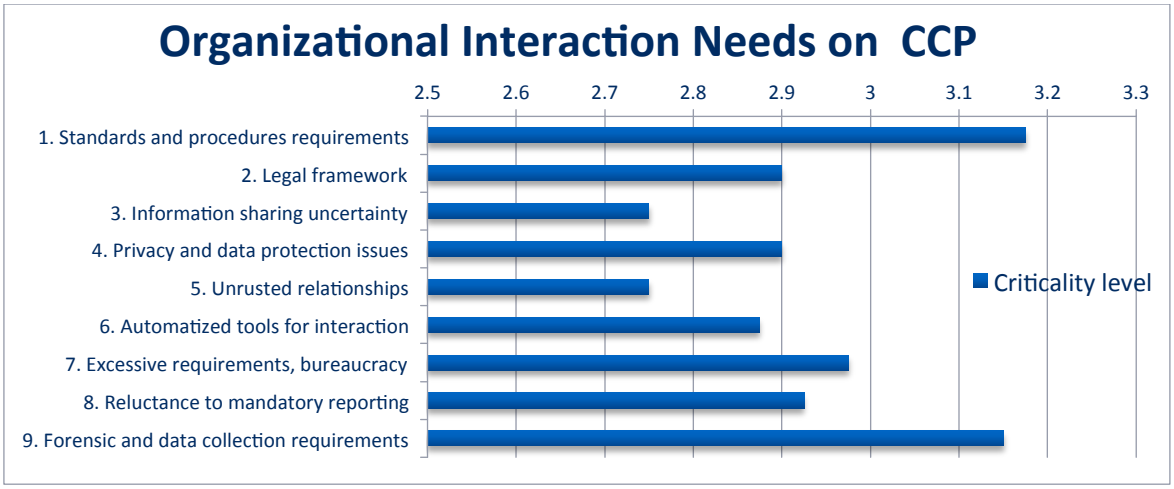

Figure 4 Summary of results indicating level of criticality.

Figure 4 summarizes the results of organizational interaction needs criticality evaluated by the respondents, and should be interpreted as follows: the list on left side represents the issues of importance that were reflected in questions formulated and listed from 1 to 9 (each corresponding to the nine most representative needs of the 41 that were categorized in table 8), while on the horizontal axis at the top the level of criticality of each matter is shown, as scored by the participants. The evaluation scale ranged from 1 to 5, but the figure zooms into the responses area and represents the original scale from 2.5 to 3.3. The blue bars evidenced greater urgency and recurrence in respect to aspects one 1 and 9.

On standard procedures and requirements: Most of the respondents found deficiencies in the mechanisms, standards and common procedures for promoting the flow and exchange of information with other organizations on cybercrime investigations (e.g. International or local agencies as the General Attorney Office, Telecommunications Service Providers, private sector organizations, etc.) This could indicate that although there are some mechanisms for interaction, these may not be entirely effective and do not meet the needs of the investigative process.

On the legal framework: The respondents recognized some deficiencies in the legal system regarding mandatory preservation of the evidence and timely delivery of information to the authorities on a medium-high level of prioritization. These could be attributed to weaknesses in the regulatory framework that do not take into account the particularities of digital evidence and its impact on the preservation and delivery of information during investigations.

On information sharing and certainty: The respondents evaluated at a midpoint the need to clarify and reduce uncertainty on legal procedures for sharing information related to cybercrime by third parties. Ranking with lowest score along with the fifth issue on trust. This could indicate that although flows of information between some stakeholders exist, interruptions or delays may occur because of ambiguities on internal regulations.

On privacy and data protection issues: The respondents are not outstandingly aware of the importance of digital rights but considered of a high level of prioritization the need to increase awareness and knowledge on privacy and data protection when information needs to be distributed. This could indicate that stakeholders might fear interaction with the authorities, because of the potential liabilities that may result from mishandling sensitive information. Reservations like these may cause setbacks during the investigative process.

On relationships and trust: Medium to high was the respondent's averaged response on the criticality and recurrence of the need to improve trust relationships for increasing interactions. Some resistance may remain among the stakeholders on the supply of information to authorities or mistrust in the existing practices and processes.

On Automation in interaction: Respondents considered between mediums high the importance of implementation of automatic tools that facilitate the timely exchange of information (e.g. Web Portal, data repositories, encrypted information, secure channels). This could indicate that investigators are not familiar with the use of such tools to facilitate the exchange of information, and they would prefer to obtain information directly from third parties without technical limitations.

On requirements and bureaucracy: To reduce bureaucratic obstacles and excessive procedural requirements in response to requests for assistance or information provided by third parties (e.g. authorities, telecommunications and infrastructure service providers, banking or private sector) ranked a high priority. This has often been considered complications in investigative process, but is also a guarantee of rational action by the state organs. Generally, the transaction costs are attributed and may really be associated to lack of clear policies and ambiguous or inadequate procedures for investigations.

On reluctance to mandatory reporting: Respondents considered that the issue of low reporting rates about incidents or offenses by cybercrime victims to authorities ranked medium high. This is a light dismissal of one of the major impediments in the fight against cybercrime because no investigation starts without an alert or criminal report; the fact that there is no mandatory reporting may cause lack of information and impunity.

On forensic and data collection requirements: Respondents ranked this issue the highest priority of the nine, together with the first. This responds to realizations on that even though investigators are given some tools and follow predetermined processes to preserve the effectiveness of forensic investigations, the evolution of criminal techniques requires specialized training and the most advanced technologies and standards during investigative processes.

The respondents were also asked an open question about their personal opinions on the criticality of organizational interaction needs linked to cybercrime investigations, and how to improve the investigative process. Only 24 out of 40 respondents elaborated in the answer on the issue, corresponding to 60% of the total. Nevertheless these answers can be associated coincide with claims and aspects discussed in this work. These texts were translated into English and grouped into categories on the basis of frequency.

Figure 5 Organizational Interaction Open Question Chart

Figure 5 charts repeated reactions by respondents, listed in order of frequency. The seven most representative reactions resulted from re-grouping the 24 initial responses in 13 based on similarity and then sorting recurrent terms. In the first place, the need for improving organizational interaction is manifested and was expressed in terms of cooperation with specific stakeholders (in coincidence with the stakeholders identification made in section 4.2 Table2). Timely information flows between the investigation units and others was the extent of the cooperation mentioned by respondents R3, R13, R15, R18, and R19. And examples of stakeholders were: social networks administrators, hosting providers and digital messaging services. In the remaining, respondents claim for harmonization of domestic laws and regulations, specifically R1, R8, R10, and R25; on reducing legal barriers and procedural boundaries such as excessive requirement or lengthy procedures commented R9, R14, R21, and R27; R33 and R35 stated mandatory reporting mechanisms would overcome issues of an underdeveloped security culture; training and expertise support; sensitization and training to prosecutors were an issue to consider by R18 and R34 only; and, appealing to international support seemed important to R30 and R2. Also, they emphasized the need for workforce (R39), budgetary allocations (R35), more training (R35), logistic support (R35) and assistance on specific cases such as ransomware (R30).

The surveys can be said to have become a rank of criticality on specific needs that was evaluated by an expert group of law enforcement agents, representative for Colombia, from a unit that only handles cybercrime investigations. The results reaffirm the importance of the inclusion of elements in planning and control in the previous stages of the investigative process to facilitate the successful investigation of cybercrime. This was explained when the optimized model presented in this work reformulated Rogers' six stages process (section 5.2 Table 7). Moreover, a regulatory framework that supports criminal investigation activities already exists, but seems not to adjust to the needs of the provision of information by third parties. A situation like this may cause in turn barriers and obstacles for providing information or the flow of resources to help the process. R1 wrote "some legal procedures end up benefiting cybercriminals only…". Setbacks are also common in the process of organizational interaction within stakeholders when they exist.

Some of the limitations faced on the development of this survey were evidenced on the recurrence of values of criticality at mid points. It could be attributed to most of the respondents being responsible for investigative and administrative activities while the questionnaire was more oriented to strategic decision makers and officials working in managerial positions. Therefore, responses ranked high scores on issues related to standards and procedures, and forensic and data collection requirements. Understandable, these are the most critical activities that their tasks in the investigative process impose. In future studies, surveys and questionnaires should address specific domains of the investigative process, differentiated groups and expand on other fields of interest, for contrast and balance

Summary of weaknesses and capabilities

The Colombian government established the DIJIN-CCP, in 2011 responding to expectations consigned on the National Strategy CONPES 3701 [55]. The scope of operations of the unit is extends to the territory of the country but activities are coordinated from the Capital District Bogota. The CCP is specialized on cybercrime events and investigations and tasked with the protection of the interests of citizens and Government in the cyberspace[17]. For this work, since one of the promised research tasks

[17] Available at: http://www.ccp.gov.co/#servicios

was to perform an analysis of the current state on organizational interaction at the CCP (RT8), an examination in terms of structure and capabilities will follow. Accordingly, to complete this task, the existing regulatory framework, memberships to organizations and alliances, strategic alliances, mechanisms of collaboration, cooperation and sharing information studied on the conceptual developments on section 4.1, must be identified and recollected. Information is also retrieved from the categorization of needs studied on section 5.3 Table 8. The conclusions on this summary could show managers what are the organizational interaction strengths/capabilities and weaknesses in terms of decision-making in the fight against cybercrime. The compilation of information is presented in Table 9.

Table 9. Current Status of Organizational Interaction on CCP

NAME	MECHANISM	DESCRIPTION
Manpower development	CNP has 180000 members across the country. DIJIN CPP 250 members (roles and responsibilities on cybercrime investigations). 90 members working in capital city district, 210 in the rest of the country.	
Education, Professional training.	20% professional certifications 30% have technical certifications in in forensic technics and tools. 50% not formal certifications, but informal training and certified experience.	
Criminal legislation	Statutory Law 1273/ 2009	The Criminal Code, information and data protection
Regulation and compliance	Statutory Law 1266 /2008	Habeas data, personal data
	Statutory Law 1581 /2012	Privacy and data protection law
	Decree 1377 of 2013	Regulation on data protection law
	External Circular 052 /2010 and 042 /2012 Financial Superintendence	Data protection regulations and responsibilities in financial operations (Financial crimes)
	Statutory Law 1621	Intelligence and counterintelligence law
Child online protection	Statutory Law 1336 /2009	Child pornography
	Law 1273/ 2009 (Article 218, 219A) Law No. 679	Child online protection
	UN Convention and Protocols	Articles 16, 17(e) and 34(c); and Articles 2 and 3
National Strategy, governance guidelines	The Model of information security for government online strategy and COPES 3701	National Planning Policy guidelines for cyber security and defense, Renovation currently in development
National/ local cooperation with accredited CSIRT/CERT	CSIRT-Ponal; ColCERT; CSIRT-CCIT; CSIRT-ETB; DigiCSIRT; CSIRT OLYMPIA; SOC TEAM Claro; SOC-CCOC.	Eight accredited teams at national level, sharing information and regular meetings.
National cooperation Private sector, NGO, GO.	ASOBANCARIA, SAINET Ingenieria, RedPAPAZ, PuntoCO Internet, ICBF, Gobierno en Linea	Public and private partners, for online child protection, financial security matters and online transactions.
Agency certifications/ standards/ best practices	ISO 27001 Information Security Management System ISMS	Criminal Investigation, judicial investigation, forensic, and criminological; Administration of Criminal Information, Technology and Document Management processes
Intra-state cooperation	ColCERT and CSIRT Ponal	Sharing of cybersecurity assets across borders
Int. cooperation	APWG and FIRST	Active member since 2012
Institutional support	The Police Cybernetic Centre	Reports and support on cybercrime and child online protection.
Reporting mechanism	The Police Cybernetic Centre and National Prosecutor Office	Victims can report both organizations, currently complaints and crimes can be online reported http://www.ccp.gov.co/contenido/cai-virtual-0
International conventions	Budapest Convention	Submitted application in 2013, currently candidate
Law Enforcement Cooperation	AMERIPOL	Active member since 2007
	INTERPOL I 24/7	Active member since 1954, liaison officer
	EUROPOL EC3	Liaison officer, Cooperation in malware analysis.
	UNITED STATES FBI, DEA, ATA	Supported by malware analysis laboratory
	OAS Inter-American Committee against Terrorism (CICTE)	Cooperation to combat and eliminate terrorism
	Latin American Working Group of technological crimes GTDLT	Active member of this community and currently holds the presidency
	Korea International Cooperation KOICA	Support and training on security matters
	National Crime Agency NCA UK	Combating organized crime

First and second rows describe the structure of the agency in terms of workforce and training. Starting form third row, the first column indicates the types of asset, mechanism, or statutes that the entity have, the second presents the denomination, and third describes the current status and nature of each. The information is an overview of the advances, capabilities, developments, and implementations of the entity in terms of organizational interaction. The data has been collected from internal and public sources of information, mainly from ITU "Cybersecurity & Cyberwellness Profiles Index, the Police Cybernetic Centre CCP and from the National Strategy documentation [55], [57], [58]

From the data collected it can be observed serious deficiencies in the workforce and training that might require further attention. The quantity and quality of investigations and reports might be affected due to lack of workforce, inadequate training or excessive workload. Moreover, there are some advances in the regulatory frame in terms of criminal legislation, compliance and online child protection. However, as it was evidenced on the survey, this seems that it need to be adjusted in terms of regulated provision of information by third parties. The existing regulation do not contemplates strict parameters on aspects such as mandatory report on crimes, storage directives, provision of logs, and timely provision of information by service providers regarding to responsibilities and ownership for IT Resources (e.g. IP addresses, URLs, mail and social networks accounts, cloud services). In addition, it can be observed some advances on the establishment of organizational interaction at national and international levels. However, due to the survey evidenced greater level of criticality on cooperation with specific stakeholders, the agreements could not cover all the expected needs of the investigative process. As special limitations it can be observed that Colombia has not still achieved the accession to Budapest the Convention, and there are not sufficient organizational interaction at regional levels. However, there are some strengthens on organizational interaction in international spheres, especially with Europol, Interpol, and GTDLT.

5.5 Guidelines to Promote Collaborative Interaction

Despite the existence and practice of existing models of collaboration, cooperation, and exchange of information between LEAs and stakeholders, it is important to consider the evaluation and the incorporation of renewed guidelines for the improvement of the organizational interactions during cybercrime investigative process. The implementation of such practices could help to reduce constraints, and overcome obstacles and barriers when decision-makers are facing complex investigative challenges. This part condenses some of the most important setbacks discussed throughout this study and states a the minimum conditions that could help promote collaboration, cooperation and information sharing schemes, at the strategic level for cybercrime investigations success organizational interaction for cybercrime investigations success. The guidelines drawn from the weaknesses (needs) that were detected during preparatory stages according to the optimized cybercrime investigation model presented and discussed on table 7. These guidelines could be considered a valuable instrument especially for managers of LEAs for the analysis and practice of organizational interaction components affecting cybercrime investigations. These considerations are linked to the analysis of needs during cybercrime investigations performed on section 5.3 and presented on the analysis of table 8.

1. Development of management procedures, models and standards to contribute to organizational interaction success. Maintaining consistency, completeness, and accuracy in the investigative process could impact the process and the results. The initiatives should simplify procedures and bureaucratic requirements to investigations, prosecution, and digital forensics responsibilities, reducing legal obstacles on the delivery of information, harmonizing data protection law, and reducing privacy concerns. (Connected to managerial need No1).
2. The clarification of legal framework on data protection could help to reduce the risk of uncertainty and improve information flows, especially when privacy concerns and data protection issues are presented. (Connected to managerial need No 2).

3. The promotion of relationships of trust in the stakeholder's community could help to increase the benefits of organizational interaction. This could be achieved by the clarification of policies, emphasizing on shared benefits and common goals, establishing reliability in the investigative process, and encouraging long-term relationships. However, improving trust relationships could also require long-term strategies to increase trustworthiness in processes and reduce conflicts of interest. The promotion of regular face-to-face meetings, exchange of experiences, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies in the field of cybercrime, are expamples of the possibilities. (Connected to managerial need No 3);
4. Managers could consider branding strategies for positioning the status of LEAs to obtain recognition and prevent reputational risk. This could generate brand recordation, and therefore, better support from international community and counterparts. LEAs, also could obtain better benefits on organizational interaction accessing to memberships, associations and organizations in the field of cybercrime (Connected to managerial need No 4);
5. The inclusion of secure platforms, protected communication channels, and automatic mechanisms for data exchange, could safeguard information flows during investigative processes. The implementation of such instruments (web portal, incident repositories, cyphered communications, etc.), could reduce proliferation of communication channels, in favour of standardization of terminology, reducing obstacles and language barriers on organizational interaction (Connected to managerial need No 5);
6. In some cases, mandatory mechanisms for organizational interaction could indeed be counterproductive. This could generate resistance or scepticism in the stakeholder community, affecting the expected results for the investigative process. Each particular case should be considered separately, reducing legal restrictions and preventing waste of efforts in establishing formal agreements with specific partners (Connected to managerial need No 6);
7. The development of strategies for proper management of human resources could impact organizational interaction. Cybercrime investigation may face excessive workload in day-to-day operations, affecting productivity as in any other type of work. The managers should consider by prioritizing efforts, improving the quality of reports, and impacting positively in post-processing data. It includes delegation and associating other agencies to advising on cases and provide or receiving technical assistance. (Connected to managerial need No 7);
8. Promoting the establishment of organizational interaction agreements with specific stakeholders for supporting special cases. The investigative process may faces weaknesses and gaps the stages identified earlier with the help of the optimized investigation model. In some cases, it would be desirable to concentrate efforts in creating agreements with key stakeholders (Courts, abuse teams, ISPs, security service providers, independent researchers, malware repositories, hosting providers, and network operators, among others) to be able to intervene the stages of the process more affected. Moreover, with the Promotion of such agreements, it would be advisable to evaluate the possibility to invite third parties or monitorinf instances transparency and control (Connected to managerial need No 8).

6 Concluding Remarks

The activities perfumed on RT1 demonstrated the importance of differentiating concepts and terminology associated with organizational interaction mechanisms such as collaboration, cooperation, and sharing information. This theoretical precision is a key factor in the establishment of a common language among the stakeholder community. The integration of different concepts and theories of law, criminology, computational, and social sciences was successful in filling some knowledge gaps and helped to advance on issues of strategic management research applied to cybercrime. Also, with the exploration of organizational interaction during cybercrime investigations performed on RT2, the analysis of requirements of LEAs made on RT3, and; the comparison of existing models of the investigative process, stages, components performed en RT4, the categorization and classification into an optimized model proposed on RT5 was possible. This can be said to be a first step in resolving one of the most significant impediments that may obstruct decision-making in the process of cybercrime investigations.

The analysis of organizational interaction in law enforcement decision-making spheres was useful to respond to RQ1. It indicates that the cybercrime investigative process could be adversely affected by the lack of reporting, deficiencies in models or formal standards or deficits on collaborative mechanisms. It also indicates that due to the lack of management procedures; legal and procedural obstacles; privacy questions; trust issues; low interest from partners; technical barriers; delays in providing information, and mandatory reporting mechanisms; are among others the main obstacles to achieving the success of investigations. This has been found to apply to cybercrime as much as it does traditional criminal investigations, or even more considering their transnational implications.

RQ2 was evidenced on the importance of addressing the necessary conditions to generate an ideal environment, identifying and overcoming barriers when facing the effective exchange of information, becoming a challenge and a task for managers and policy makers. The applicability of the optimized was demonstrated on RT6. The results evidenced that with the inclusion of management elements, particularly in the preparatory stage of the process, could facilitate interaction with stakeholders and the provision of information to support the investigative process. Furthermore, with the implementation of administration procedures, it could maintain the relationship of trust with stakeholders, increasing the information flows, and improving interaction and efficiency in the investigative process. Law enforcement alone cannot effectively combat cybercrime. It requires the establishment of organizational interaction mechanisms that reduce barriers and help to meet the challenges that decision and policy makers have to face and overcome.

The need to increase awareness especially on strategic levels for the implementation of improvement mechanisms, guidelines, and best practices for supporting complex cybercrime investigations remains challenging. However, since the purpose of RQ1 was to identify what are the main obstacles concerning interaction with stakeholders during the investigative process, to obtain an actual measurement or an objective evaluation of the results in the implementation of these proposals was beyond the scope of this work. For this reason, assuming that the needs analysis provide valuable evidence to detect what part of the process requires greater focus, this thesis proposes according to RT9, a set of improvement actions, that may increase the practice of interaction and optimize the results of the investigative process. For a factual verification, it would be necessary to make a

measurable implementation over a period, and case studies or periodical observations that may open an avenue for future research.

This thesis contributes to theoretical development, clarification of key terms resulting from the interdisciplinary integration of concepts and theories, and practical instruments applicable to guide managerial organizational interaction mechanisms in cybercrime investigations. Other contributions of meaningful implications are the results of the analysis of needs, the guidelines for the implementation of best practices, and the proposal of implementation of an optimized model of investigation based on the need of organizational interaction. Those conform a toolbox of practical instruments for the implementation of managerial techniques to enhance effectiveness and support decision-making in combating cybercrime. The work is geared towards the managers in Law Enforcement Agencies LEAs, or anyone interested in consulting organizational interaction on the cybercrime investigative process.

The needs analysis and the original model proposed helps to identify gaps and when to intervene and compensate for the weakness that may appear at certain stages during the investigative process. Moreover, The Guidelines for the implementation of best practices are a practical instrument for the communication of policies and the implementation of management procedures. These establish interaction mechanisms that reduce language barriers across stakeholders´ groups. The applied surveys on RT7, and the case study presented on RT8, were performed based on the Colombian National Police and its organizational interaction capabilities. This is a valuable empirical contribution that supports the understanding of the phenomenon of interaction in practice. Policy and decision makers of LEAs, and in particular at the Cybercrime Center CCP, get tools for evaluation and consultation that can be a basis for implementing policies, guidelines, management, allocation of resources, raise awareness, and the inclusion of improved interaction mechanisms. All in all, new models optimize traditional ones, while preserving their best features.

The limitations of this study were in part due to the difficulties obtaining official sources of information in preparation for the diagnosis on the organizational interaction capabilities between the Colombian Cybercrime Center and other stakeholders. And in part to the time constraints for a more detailed application in the determination of the properties of information flows in cases of organizational interaction. Moreover, while the needs analysis was conducted according to up to date information, relying on current typologies, the changing nature of cybercrime may require continuous revision. Needs evolve and cannot be predicted or treated within the scope of one single work. Consequently, is important to update the analysis of needs according to the emergence and evolution of new requirements, making constant adjustments in the improvement of the cybercrime investigation processes.

The thesis deals with only a few of the available aspects of organizational interaction with stakeholders in cybercrime investigations; so opportunities to explore and consolidate this work abound. Two ways are, for example, to test the effectiveness of the model and evaluate results on the incorporation of managerial elements of planning and control in the pre and post-processing stages of the investigation. Besides, the use of the model in practice, if monitored and kept in records, could be addressed with the use of quantitative methods. For this purpose, performance indicators and measuring scales must be devised to assess the effectiveness and degree of which improvements increased process efficiency. This highlights that the management of operations and organizational

interaction is an ongoing process that could benefit from further studies and other research methods in the long perspective.

7 References

[1] M. Gercke, "Understanding Cybercrime: Phenomena, Challenges and Legal Response.," *Underst. Cybercrimes Int. Telecommun. Union.*, 2012.

[2] M. Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *Eur. J. Criminol.*, vol. 2, no. 4, pp. 407–427, 2005.

[3] KPMG International, "Cyber Crime – A Growing Challenge for Governments," *Issues Monit. Cybercrime*, no. July, 2011.

[4] J. B. Marshall and M. Adbullahi, "Cyber-Atacks: The Legal Response," *Int. J. Int. Law ISSN 2394-2622 (Volume 1 Issue 2)*, vol. 1, no. 2, pp. 1–18, 2015.

[5] C. Brown, "Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice," *Int. J. Cyber Criminol. IJCC*, vol. 9, no. 1, pp. 55–119, 2015.

[6] ENISA, "Incentives and Challenges for Information Sharing in the Context of Network and InformationSecurity", Heraklion, Greece," vol. 10, p. 52, 2010.

[7] United Nations, "Comprehensive Study on Cybercrime," 2013.

[8] P. M. Bednar, V. Katos, and C. Hennell, "Cyber-crime investigations: Complex collaborative decision making," in *Proceedings - 3rd International Annual Workshop on Digital Forensics and Incidents Analysis, WDFIA 2008*, 2008, pp. 3–11.

[9] Police Executive Research Forum PERF, "The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime," *Crit. Issues Polic. Ser.*, pp. I, 1–50, 2014.

[10] R. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Polic. An Int. J. Police Strateg. Manag.*, vol. 29, no. 3, pp. 408–433, 2006.

[11] ENISA, "Detect, Share, Protect: Solutions for Improving Threat Data Exchange among CERTs, Heraklion, Greece," 2013.

[12] Eric Luiijf; and A. Kernkamp, "Sharing Cyber Security Information, Good Practice Stemming from the Dutch Public-Private-Participation Approach, The Hague, Netherlands.," 2015.

[13] A. I. Cerezo, J. Lopez, and A. Patel, "International Cooperation to Fight Transnational Cybercrime," in *2nd International Annual Workshop on Digital Forensics and Incident Analysis WDFIA*, 2007, no. Wdfia, pp. 13–27.

[14] (PonemonInstitute), "2015 Cost of Cyber Crime Study: Global," *Hewlett Packard Enterp.*, no. October, 2015.

[15] S. Corp., "Norton Cybersecurity Insights Report," pp. 1–13, 2016.

[16] Internet Crime Complaint Center IC3 US, "2014 Internet Crime Report," 2015.

[17] Departamento Nacional de Planeacion, MinTIC, MDN, and DNI, *Consejo Colombiano de la Politica Ecnomica y Social- Politica Nacional de Seguridad Digital CONPES 3584*. 2016.

[18] United Nations, "Resolutions and decisions of the economic and social council

1996," 1997.

[19] European Commission, "Joint Communication to the European Parliament, the council and the European Economic and Social Committee and The Committee of the Regions," 2013.

[20] A. Alkaabi, G. Mohay, A. Mccullagh, and N. Chantler, "Dealing with the problem of cybercrime.," in *Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime.*, 2010, no. October, pp. 8–9.

[21] A. M. Thomson, J. L. Perry, and T. K. Miller, "Conceptualizing and measuring collaboration," *J. Public Adm. Res. Theory*, vol. 19, no. 1, pp. 23–56, 2009.

[22] A. M. Thomson, J. L. Perry, and T. K. Miller, "Linking collaboration processes and outcomes: Foundations for Advancing Empirical Theory," in *Collaborative Public Management*, 2008, pp. 97–120.

[23] P. Mattessich, M. Murray-Close, and B. Monsey, *Collaboration: What Makes It Work, 2nd Edition: A Review of Research Literature on Factors Influencing Successful Collaboration*. 1992.

[24] B. Wood, D. J. Gray, "Toward a Comprehensive Theory of Collaboration," *J. Appl. Behav. Sci.*, vol. 27, no. 2, pp. 139–162, 1991.

[25] A. M. Thomson and J. L. Perry, "Collaboration Processes: Inside the Black Box," *Public Adm. Rev.*, no. December, 2006.

[26] S. K. Mangal, *Emotional Intelligence: Managing Emotions to Win in Life*. 2015.

[27] R. Axelrod and W. D. Hamilton, "The Evolution of Cooperation," *Sci. New Ser.*, vol. 211, no. 4489, pp. 1390–1396, 1981.

[28] C. Goodwin, J. P. Nicholas, J. Bryant, K. Ciglic, A. Kleiner, C. Kutterer, A. Massagli, A. Mckay, P. Mckitrick, J. Neutze, T. Storch, and K. Sullivan, "A framework for cybersecurity information sharing and risk reduction," 2015.

[29] ENISA, "Give and Take, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime", Heraklion, Greece," 2011.

[30] ENISA, "Improving Information Security Through Collaboration, Heraklion, Greece," 2012.

[31] P G Aquinas, "Principles and practices of management," New Delhi: Excel Books Privated Limited, 2011, p. 79.

[32] Y. Wang and G. Ruhe, "The Cognitive Process of Decision Making," *Int. J. Cogn. Informatics Nat. Intell.*, vol. 1, no. 2, pp. 73–85, 2007.

[33] H. A. Al-Tarawneh, "The Main Factors beyond Decision Making," *J. Manag. Res.*, vol. 4, no. 1, pp. 1–23, 2011.

[34] L. C. Babcock, D. L., & Morse, "Decision Making," in *Managing engineering and technology: an introduction to management for engineers.*, 2010, pp. 74–96.

[35] T. Sõmer, R. Ottis, T. Lepik, M. Lagazio, B. Hallaq, D. Simms, T. Mitchener-Nissen, and M. Riek, "E-crime 'The economic impacts of cyber crime' D2.3 Detailed appendixes on cyber crime inventory and networks in non-ICT sectors," 2015.

[36] M. Gercke, "Understanding Cybercrime: A Guide for Developing Countries," 2011.

[37] D. Simms and S. Ghernaouti, “E-CRIME ‘The economic impacts of cyber crime’ D2 1 A Report on taxonomy and evaluation of existing inventories,” 2014.

[38] Council of Europe, “Convention on Cybercrime.,” Budapest, 2001.

[39] S. W. Brenner, “Private-public sector cooperation in combating cybercrime: In search of a model,” *J. Int. Commer. Law Technol.*, vol. 2, no. 2, pp. 58–67, 2007.

[40] ENISA, “Information sharing and common taxonomies between CSIRTs and Law Enforcement, Heraklion, Greece,” 2015.

[41] T. G. Shipley, C. Hutchings, T. G. Shipley, and A. Bowker, “Report on Cyber Crime Investigation 2010,” 2010.

[42] HTCIA, “High Technology Crime Investigation Association,” *2016*. [Online]. Available: https://www.htcia.org/. [Accessed: 09-Mar-2016].

[43] C. Hutchings and J. Garcia, “2011 Report on Cyber Crime Investigation Treasurer,” 2011.

[44] M. Snyder, P. Morin, C. Hutchings, and E. Hutchings, “Cybercrime Survey 2013 HTCIA,” 2013.

[45] S. Bucci, P. Rosenzweig, and D. Inserra, “A Congressional Guide: Seven Steps to US Security, Prosperity, and Freedom in Cyberspace,” *Backgrounder*, vol. 20002, no. 2785, 2013.

[46] Forbes, “The Problems Experts And Privacy Advocates Have With The Senate’s Cybersecurity Bill - Forbes,” *29,oct 2015*, 2015.

[47] D. Baker, D. Bridges, R. Hunter, G. Johnson, J. Krupa, J. Murphy, and K. Sorenson, “Guidebook to decision-making methods. Developed for the Department of Energy USA.,” no. January, Washington DC., 2001.

[48] P. Berger and T. Luckmann, “Social Interaction in Everyday Life,” in *Communication Theory*, 2007.

[49] N. Martin and J. Rice, “Cybercrime: Understanding and addressing the concerns of stakeholders,” *Comput. Secur.*, vol. 30, no. 8, pp. 803–814, 2011.

[50] A. E. Roger and M. M. Achille, “Multi-Perspective Cybercrime Investigation Process Modeling,” *Int. J. Appl. Inf. Syst.*, vol. 2, no. 2, 2012.

[51] E. Casey, *Digital Evidence and Computer Crime, forensic science, computers, and the Internet*, 2nd ed. ELSEVIER Academic Press, 2004.

[52] H. C. Lee, T. Palmbach, and M. T. Miller, *Crime Scene Handbook*. 2001.

[53] G. Palmer, “A Road Map for Digital Forensic Research,” *Proc. 2001 Digit. Forensics Res. Work. (DFRWS 2004)*, pp. 1–42, 2001.

[54] K. Mandia and C. Prosise, *Incident Respnse & Computer Forensics*. McGraw-Hill, 2003.

[55] Departamento Nacional de Planeacion DNP, MDN, and MINTIC, *Consejo Colombiano de la Politica Ecnomica y Social- Lineamientos de Politica Para la Ciberseguridad y ciberdefensa. CONPES 3701*. Bogota, 2011, pp. 9–43.

[56] Organization of American States AS, “Cybersecurity Technical Assistance Mission,” Bogota, 2014.

[57] International Telecommunication Union ITU, “Global Cybersecurity Index & Cyberwellness Profiles,” 2015.

[58] P. N. de Colombia, “Cai Virtual Centro Cibernético Policial,” *2016*, 2016. [Online]. Available: http://www.ccp.gov.co/contenido/cai-virtual-0. [Accessed: 11-Apr-2016].

Appendix

I. Survey

Questions addressed to conduct the analysis of the current state of priorities on collaboration mechanisms on cybercrime investigations at the Cybercrime Center, Colombia National Police.

Please rate from 1 to 5, where 1 is the lowest value and 5 the maximum, about your perception of what are the major impediments, obstacles and requirements that criminal investigation process faces regarding collaboration and / or efficient delivery and timely information by third parties in the investigation of cybercrime.

1. Deficiencies in mechanisms, common standards and procedures that promote the flow and exchange of information with other organizations in cyber crimes investigations (e.g. International or local agencies as Attorney, Telecommunications Service Providers, private sector, etc.)

2. Deficiencies in legal system concerning mandatory preservation of evidence and timely delivery of information to the authorities.
3. Lack of clarity and uncertainty of the legal procedure for sharing information related to cybercrime by third parties.

4. Lack of knowledge by those who provide information on matters related to privacy and protection of personal data.

5. Lack of trust and deficiencies in personal relationships with third parties.

6. Lack of automation tools that facilitate the timely exchange of information (e.g.: web portal, data repositories, encrypted information, secure channels).

7. Bureaucratic impediments, obstacles and excessive procedural requirements in response to requests for assistance or information provided by other authorities, service providers or telecommunications infrastructure, banks or private sector.

8. Lack of reporting to authorities on behaviours, incidents or offenses by victims of cybercrime.

9. Deficiencies in the process of collection digital evidence and forensics.

Additional open question

10. Where do you think it should be prioritized intervention efforts to improve collaboration on cybercrime investigations?

II. List of Abbreviations

AMERIPOL	The Police Community of the Americas
APWG	Anti-Phishing Working Group
BKA	*BundesKriminAlamt German Police*
CAI	*Centro de Atencion Inmediata Colombia*
CCoC	*Comando Conjunto Cibernetico Colombia*
CCP	*Centro Cibernetico Policial Colombia*
CI	Critical Infrastructure
CICTE	*Comité Interamericano contra el Terrorismo*
Col CERT	Colombia Computer Emergency Response Team
CONPES	*Consejo Nacional de Politica Economica y Social*
CSIRT	Computer Security Incident Response Team
DFRW	Digital Forensics Research Workshop
DIJIN	*Direccion de Investigacion Criminal Colombia*
ENISA	European Network and Information Security Agency
EU	European Union
EUROPOL	European Law Enforcement Organization
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
GO	Governmental Organizations
HTCIA	High Technology Crime Investigation Association
ICT	Information and Communication Technology
INTERPOL	International Criminal Police Organization
ISO	International Standard Organization
ISP	Internet Service Provider
IT	Information Technologies
ITU	International Telecommunication Union
KPMG	Klynveld Peat Marwick Goerdeler consulting services
LEAs	Law Enforcement Agencies
NCSS	National Cyber Security Strategy
NCA	National Crime Agency UK
NCCU	National Cyber Crime Unit UK
NCIJTF	FBI National Cyber Investigative Joint Task Force
NGO	No Governmental Organizations
OAS	Organization of American States
PERF	Police Executive Research Forum
PPP	Public-Private- Partnerships
RQ	Research Question
RT	Research Task
SOC	Security Operation Center
UNODC	United Nations Office On Drugs and Crime

III. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Alex Duran**,

(*author's name*)

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

Organizational Interaction Mechanisms Affecting Strategic Decision-Making During Cybercrime Investigations ,

(title of thesis)

supervised by Maria Claudia Solarte and Raimundas Matulevicius

(supervisor's name)

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, **25.05.2016**