future internet

MDPI

Article

Analysis of Dynamic Complexity of the Cyber Security Ecosystem of Colombia

Angélica Flórez [1,*], Lenin Serrano [1], Urbano Gómez [1], Luis Suárez [2], Alejandro Villarraga [3] and Hugo Rodríguez [4]

[1] IT Engineering Faculty, Universidad Pontificia Bolivariana, Bucaramanga 680006, Colombia; lenin.serrano@upb.edu.co (L.S.); urbano.gomez@upb.edu.co (U.G.)

[2] Industrial Engineering Faculty, Universidad Pontificia Bolivariana, Bucaramanga 680006, Colombia; luis.suarez@upb.edu.co

[3] Strategic Business School, Universidad Pontificia Bolivariana, Bucaramanga 680006, Colombia; alejandro.villarraga@upb.edu.co

[4] Law Faculty, Universidad Pontificia Bolivariana, Bucaramanga 680006, Colombia; hugo.rodriguezv@upb.edu.co

* Correspondence: angelica.florez@upb.edu.co; Tel.: +57-7-679-6220

Academic Editor: Luis Javier Garcia Villalba
Received: 12 February 2016; Accepted: 28 June 2016; Published: 19 July 2016

Abstract: This paper presents two proposals for the analysis of the complexity of the Cyber security Ecosystem of Colombia (CEC). This analysis shows the available knowledge about entities engaged in cyber security in Colombia and the relationships between them, which allow an understanding of the synergy between the different existing components. The complexity of the CEC is detailed from the view of the Influence Diagram of System Dynamics and the Domain Diagram of Software Engineering. The resulting model makes cyber security evident as a strategic component of national security.

Keywords: Cyber security; cyberspace; ecosystem; influence diagram; domain model; system dynamics; software engineering

1. Introduction

Technological advances, in particular the widespread use of Internet by people and companies, have created an open space for the exchange of data and information. Different actors participate in this virtual and technological platform: users, who use it to carry out their daily personal or work related activities but also "intruders", who use the web for their own benefit by taking advantage of the diverse existing vulnerabilities and the high amount of users with little knowledge about the risks and threats to which they are exposed in this communication channel. This has created an important challenge in the protection of the information and infrastructure that are found on the Internet.

Cyberspace, as a result of the Internet and defined as the virtual environment that concentrates the diverse infrastructures, technological devices, and people who connect to the network, has brought about an evolution of the concept of Information security into cyberspace security. Aforementioned infrastructures, devices, and connected people range from small networks at home to state networks, large industries, communication service providers, as well as others.

Consequently, there exists a panorama filled with challenges to take up and gaps to close, in order to face the risks and threats present in cyberspace, which potentially expose actors to cyber-attacks, cyber-espionage, cyber-terrorism, cyber-bullying, hacktivism, amongst others. Physical borders are diluted when exposed to different sectors of society in cyberspace.

Lately, the Colombian government has shown interest in Information Security, as well as in the current reality of exposure of diverse sectors of society to cybernetic threats. There is legislation regarding this subject since 1999, ranging from the Law of Electronic Commerce to the Statutory Law 1571 of 2012 regarding the protection of personal data. Additionally, the National Economic and Social Policy Council CONPES 3701 document, active from 2011 to 2015, defines the guidelines to be followed by the State regarding cyber security and cyber defence for Colombia, with the purpose of improving the capabilities of the state for dealing with possible threats in cyberspace.

In 2014, the Mission of Technical Assistance on Cybernetic Security sent by the Organization of American States (OAS) published a document with conclusions and recommendations that give consideration to, amongst other things, the need of action in Colombia so that efforts can be made to work in cyber security due to a lack of a clear strategic vision [1].

Based on these considerations, this research paper proposes a definition of the Cyber security Ecosystem of Colombia, which establishes its components, the strategic vision of cyber security in government institutions and the analysis of the complexity of the ecosystem using the Influences Model of System Dynamics and the Domain Model of Software Engineering. As defined by [2], both models were created as a way of representing relevant aspects of the system, and they help to comprehend it adequately.

The rest of this paper is structured as follows: Section 2 describes the concepts to be taken into account to define the ecosystem. Section 3 details the Cyber security Ecosystem of Colombia. Section 4 describes the complexity of the cyber security ecosystem through an Influence Diagram of System Dynamics and the Domain Model of Software Engineering. Lastly, conclusions can be found in Section 5.

2. Conceptualization

This section describes the concepts that lead to the definition and establishment of the Cyber security Ecosystem of Colombia, and also those necessary for the analysis of the dynamic complexity of the ecosystem through the knowledge of System Dynamics, Software Engineering and the diagrams that allow its representation.

2.1. Ecosystem

The concept of ecosystems was initially developed by ecology studies departing from the relationship between living organisms and their environment. Nevertheless, this concept has been adopted and used by social, economic and technological sciences since then. In regards to this, several authors have carried out research studies that promoted a multidisciplinary approach. This very approach has prompted the emergence of a combination between ecology and economics to identify eco-systemic services and their conservation [3]. The technology-based approach has caused States and companies to generate huge amounts of information, whose storage and spread requires high technological power, strategic perspectives and process-oriented knowledge management systems. This approach needs to be supported by methods that timely inform decision-making as an essential step of any process.

Under this approach, the technology ecosystem consists of a compound of software components interrelated by means of information flows through physical media. These media work as the main support for the aforementioned information flow.

There is a close similarity between the classical concept of the natural ecosystem and that of the technology ecosystem; especially because the components that perform the role of the living organisms and their relationship with their counterparts around them, can be identified in the technology ecosystem, in its conditioning to the physical medium and its relationship with the software components.

Therefore, when comparing and relating the natural ecosystem and the technological ecosystem's schemes, the three basic principles of ecological ethics can be clearly identified [4]:

- In a natural ecosystem, every living organism is inter-dependent and need one another. Likewise, in a technology ecosystem every component is inter-dependent on one another. If one component is entirely independent, then; it is not part of the ecosystem.

- Diversity in ecosystems is the main constituent of stability. The more diverse an ecosystem, the more likely it is to offer possibilities and opportunities under the premises of harmony, unity, security, and coherence.
- The growth of a system is expected to occur in a controlled manner as raw materials are limited. That is why, the technology ecosystem must evolve under the guidance of a clear and specific objective. Otherwise, it would become unsustainable and therefore the objective for which it was created might not be achieved.

2.2. The Influence Language of System Dynamics

System Dynamics (SD) is a method that allows different systems to be represented and modelled in such a way that it is possible to understand their complexity so that its behavior can be studied under certain conditions in order to obtain conclusions that can be useful in decision making [5]. According to Gomez, Andrade & Vasquez [6], SD contributes to the construction of a consensus between researchers that can be used in the construction of computational models that constitute support tools to research so that it's possible to represent the complexity of the model.

SD uses different representative languages of the mental models constructed after the study of phenomena. One of them is the influence diagram that sets a scheme for the integration of variables and the relationships amongst them in a determined system. The influence diagram is used in this proposal as a way to represent the complexity of the ecosystem by means of the representation of the feedback cycles. The latter describe the growth and its relationship with the reinforcement of its elements or the tendency to reach stability, or even the pursue of the goal in the system [6].

2.3. Domain Model from Software Engineering

Abstraction is a fundamental element of Software Engineering (SE). It is supported by a combination of paradigms, models, meta models, diagrams, languages, semantics and syntax in order to formalize complex systems or elements of physical and conceptual reality to ease the development of applications. Additionally, these elements allow the arrangement of the complexity of the system into finite elements.

The conceptual representation of the real world serves as the basis for the Domain Model. This shows objects, associations and attributes that do not describe neither compromises nor components of software [7]. When Class Diagram in the Unified Modelling Language is adopted, entities such as an object or an idea, in the Domain Model, can be modelled. It helps to determine the elements of the system and the analysis cycle of it.

2.4. Cyber Security

The International Organization for Standardization (ISO) issued the ISO/IEC 27032:2012 norm to define cyber security as the "preservation of confidentiality, integrity, and availability of information in cyberspace". Cyberspace refers to a virtual environment, resulting from the Internet, comprising organizations, people, users, and technological devices that are connected to this network. Therefore, security in this cyberspace or virtual world is what leads to the concept of cyber security [8].

In Colombia, cyber security has been defined by the CONPES 3701 document as the "capability of the State to minimize the level or risk to which citizens are exposed to threats or incidents of cybernetic nature" [9].

3. Cyber Security Ecosystem of Colombia

3.1. Legislation and Political Guidelines of Cyber Security in Colombia

In the last few years, Colombia has become conscious of the importance of legislating and regulating in the area of information security. This is why the government has created a series of laws, notices, and resolutions that significantly strengthen the State's capabilities to face threats that are generated in cyberspace, such as: Law 527 of 1999—electronic commerce; Law 599 of 2000—illicit violation of communications; Notice 052 of 2007—minimum security and quality requirements in the management of information through distribution channels for clients and users of the Financial Superintendence of Colombia; Law 1273 of 2009—the protection of information and data; Law 1341 of 2009—in which concepts and principles regarding information societies and the organization of Information and Communication Technologies are defined; The resolution of the Commission of Regulation of Communications 2258 of 2009—security of network services and network providers of telecommunications Statutory; Law 1581 of 2012 for the protection of personal data.

Additionally, in 2011 the CONPES 3701 document defined the guidelines of policies regarding cyber security and cyber defence in Colombia which seek to improve the capabilities of the government to face cybernetic threats [9].

The general objective of CONPES 3701 document is to "strengthen the capabilities of the State to confront the threats that act against its security and defence in cybernetic realms, creating the adequate conditions to provide security in cyberspace" [9].

CONPES 3701 document expired in 2015. Because of this a new version of this document is being developed, which sets out, amongst other things, the strengthening of entities to support cyber security, the generation of a Cyber security ecosystem that defines the diverse entities that are considered key factors for the development of cyber security in Colombia, the development of a national strategy of Cyber security and cyber defence to close the gaps that were identified in the CONPES 3701 document. This new version was approved in April of 2016.

3.2. Definition of the Components of the Cyber Security Ecosystem of Colombia

Five components of the cyber security ecosystem are defined (Figure 1):

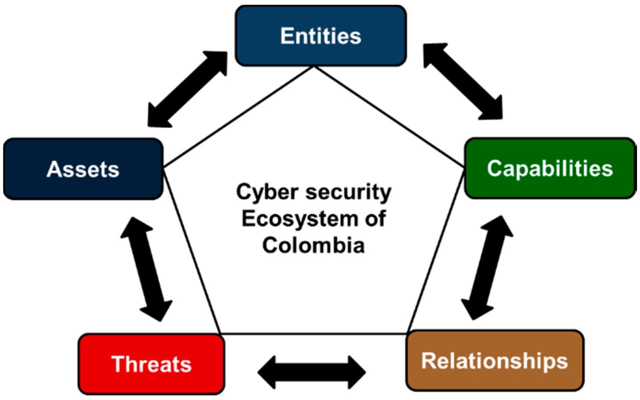


Figure 1. Components of the Cyber security Ecosystem of Colombia.

Entities: natural or juridical person considered to be an active or passive agent in the ecosystem.

Assets: tangible or intangible assets that belong to the entities of the ecosystem.

Threats: risks to which the assets, as defined in the ecosystem, are exposed to.

Capabilities: resources that are needed for the proper management of the threats that the assets are exposed to in the ecosystem.

Relationships: interaction between the different components in the ecosystem.

3.3. Entities of the Cyber Security Ecosystem of Colombia

Based on the CONPES 3701 document [9] and the research carried out by the authors, six types of entities have been identified in the Cyber security Ecosystem of Colombia, such as (Figure 2):

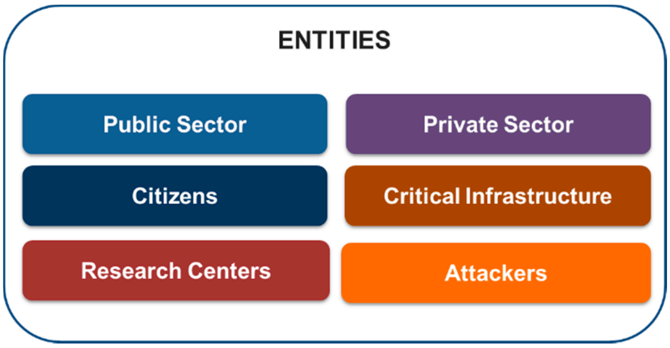


Figure 2. Entities in the Cyber security Ecosystem of Colombia.

Public Sector: Public entities and institutions belonging to the Colombian government and state, which have as part of their objectives functions related to the strengthening of Cyber security and cyber defence.

Private Sector: group of small, medium, and large businesses that make part of the productive industry axis and every other non-public businesses that participate in the ecosystem.

Citizens: group of people that reside in the Colombian territory.

Critical Infrastructure: entities that provide essential services, which are considered strategic in Colombia, such as energy, water, and financial service providers, amongst others.

Research Centers: institutions that carry out research and innovation in subjects related to cyber security, such as universities, tech centers, excellence centers, think tanks, etc.

Attackers: people or businesses that attempt to access, intercept, or damage an information system affecting the integrity, confidentiality, and availability of data and systems.

Taking in to account the aforementioned information, the description of entities in the public sector that are considered fundamental inside the ecosystem is presented (Figure 3):

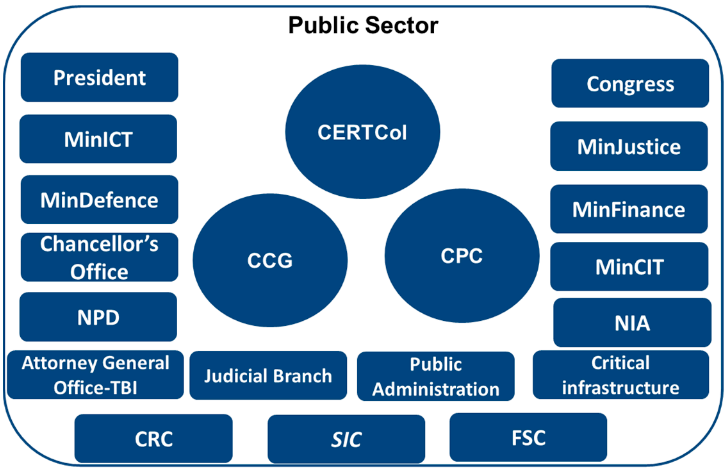


Figure 3. Public sector entities in the Cyber security Ecosystem of Colombia.

President: head of State, head of government and supreme administrative authority [10].

Congress of the Republic of Colombia: comprises the senate and chamber of representatives. It is the congress' duty to "reform the constitution, make laws and exert political control over the government and the administration" [10].

Ministry of Information and Communication Technologies (MinICT): develops its objective through the regulation of existing norms, adoption of public policies, financing of projects and other activities related with information and communication technologies, including those that correspond to the area of cyber security through the Direction of Standards and Information Technologies Architecture [11].

Ministry of National Defence (MinDefence): directed by the Minister of Defence, who works in collaboration with the general commanders of the military forces and the national police. CERTCol, the CCG, and the CPC belong to this ministry [12].

Cybernetic Emergencies Response Team of Colombia (CERTCol): Working group which takes part in the public security and infrastructure management in the Vice ministry for Public and Foreign Affairs of the Ministry of Defence. Created in 2012, it's in charge of the coordination on a national scale of all matters of cyber security and cyber defence, as well as answering to all cybernetic incidents that take place in the territory, coordinating with CSIRT (response teams of information incidents) in the country, and the coordination of international organisms in matters related to cyber security [9,13,14].

Cybernetic Command Group (CCG): dependence attached to the general command of the armed forces, which have the purpose of preventing and counteracting threats and cybernetic attacks that affect national interests and values. Created in October 2012, its role is the implementation of protocols of cyber defence and defence to critical infrastructure [9].

Cybernetic Police Centre (CPC): part of the organizational structure of the National Police of Colombia. It's in charge of managing cyber security in national territory, supporting investigative labor and judicialization by the commission of cybernetic punishable acts, receiving information and reporting cybernetic crimes. It was originally a unit of cybernetic offenses but from CONPES 3701 document it changed its name to CPC [9].

Chancellor's Office—Ministry of Foreign Affairs: entity in charge of the Administrative Sector of International Relations. This office has two divisions: Crime Prevention Coordination and Multilateral Political Affairs Direction, where all the different subjects related to cyber security are discussed [15].

National Planning Department (NPD): through the Sub direction of Security and Defence, it is in charge of the coordination, planning, determining of available budget and tracking defined actions in the CONPES 3701 document referring to cyber security, the generation of information that can be useful in the decision making that the State makes regarding the present subject [16].

Ministry of Justice (MinJustice): one of this entity's functions is the formulation and direction of national public justice policies, the coordination of matters related to penitentiaries and prisons, the promotion of legality in the local culture and other functions established by law. The subjects related to Cyber security are coordinated through the Direction of Criminal Policies [17].

Ministry of Finance and Public Credit (MinFinance): in charge of the definition, formulation, and execution of the economic policy in the country; prepare its laws, decrees and the pertinent regulation in fiscal, financial and customs sectors. It defines as a regulatory entity in anything related to information security the Financial Superintendence of Colombia [18].

Ministry of Commerce, Industry, and Tourism (MinCIT): its functions are related to the socioeconomic development of the productive sector of the national industry, the strengthening of small, medium and large businesses, promoting investments, etc. It defines as a regulatory entity the Superintendence of Industry and Commerce in aspects related to the protection of data [19].

National Intelligence Agency (NIA): entity that is in charge of producing strategic intelligence and counterintelligence of state on a national and international scale.

Attorney General Office: this entity is part of the judicial branch of public order, it is autonomous from an administrative perspective and constitutionally as well as financially it is designed to be the accusing organism of the State, in this sense it is the one in charge of enforcing penal action [10]. The Technical Body of Investigation attached to the Coordination of Cybernetic Crimes, is the division in charge of all aspects of electronic offenses.

Technical Body of Investigation (TBI): it has as objective the investigation and the search of actors and participants of a felony, including cybernetic ones. It works along with the judicial branch in aspects of judicialization of cybercrimes.

Public Administration: public entities and institutions belonging to the Colombian State, such as State owned businesses, city halls and other forms of governments.

Critical Infrastructure: public entities that provide essential services which are considered strategic in Colombia, such as financial, energy, and aqueduct service providers.

Communications Regulatory Commission (CRC): this special administrative unit is part of MinICT. It has as its objective the regulation of the communication services and network sectors [11].

Financial Superintendence of Colombia (FSC): its objectives are the preservation of stability, security and trust in the financial system of Colombia, development of the stock market and protection of investors, savings and, creditors [20]. In 2007, it emitted an External Notice 052, which establishes the minimum requirements of security and quality in the management of information through means and distribution channels of products and services for clients and users of the financial system [21].

Superintendence of Industry and Commerce (SIC): a technical organism, part of MinCIT. Its main goal is strengthening the development of markets by taking into account consumerism, competition, and its organization. Additionally, through the delegation for the protection of personal data, the entity is in charge of protecting the fundamental right of Habeas Data, establishing the policies to follow on behalf of the ones responsible and in charge of treating and handling personal data [22].

3.4. Cyber Security as a Strategic Component of National Security

CONPES 3701 document emphasizes that there is no national strategy to confront threats and the weaknesses of the state regarding cyber security [9].

Due to this, an investigation process was carried out for identifying the approaches of several States in regards to this subject. The strategy of national security of Spain was taken as a reference point, given that this country was one of the most advanced in terms of security as it handled national security in an integrated way, taking into account both global relationships and daily life aspects of its population.

In Spain's National Security Strategy it is obvious that cyber threats, make part of possible risks and threats to national security, which leads to the definition of guidelines of cyber security strategies and protection of critical infrastructures [23].

It is concluded that cyber security is defined as a strategic component of national security in a country, since it looks into the strengthening of the capabilities of a nation to prevent, detect, and respond to cybernetic attacks.

4. Complexity of the Cyber Security Ecosystem of Colombia Visualized from an Influence Diagram of System Dynamics and the Domain Model of Software Engineering

The analysis of the complexity of the Cyber security Ecosystem of Colombia directed its efforts to the elaboration of two concept models (Influence Diagram and Domain Model) using System Dynamics (SD) and Software Engineering (SE), which are two disciplines within Computing and Software Engineering that provide tools to understand the structure and behavior of a specific problem that is formally described by the models.

The term model refers to the representation of a system using graphs and texts [24] to reveal the complexity of a situation, which can then be used to explain or further understand the situation [6].

The models proposed will be validated with the results of the research Project that permits this article: "Feasibility study for the creation of a National Cyber security Observatory in Colombia". In order to design Influence Diagrams, we used the software "*Evolution*", a free-use type of software used in academic contexts for the construction of models under the SD methodology [6].

4.1. Influence Diagrams in the Cyber Security Ecosystem of Colombia

To represent the Cyber security Ecosystem of Colombia, the influence language of SD will be used: a diagram in which the variables and the relationships of each one of these to the system are integrated.

Relationships are shown through arrows that go from one variable to another, demonstrating the direction of influence in one way. With the Influence Diagram language, it's easier to explain the complexity through the identification of feedback cycles, which show that the system is dynamic.

Based on the components of the Cyber security Ecosystem of Colombia (Figure 1), an initial approximation of the relationships between the elements is carried out, which suggest existing relations between them (in the description of each diagram the words that correspond to elements within the diagram will be written in bold).

Figure 4 shows the general influences diagram of the Cyber security Ecosystem of Colombia, which illustrates how the **Entities** have **Assets** that are susceptible to **Threats** which can then be taken advantage of to affect the **Entities**; In turn, the **Entities** count with **Capabilities** that allow them to be protected from **Threats**. Additionally, it is made evident that the arrows in the diagram represent the interactions that take place between the different components in the ecosystem; they were called Relationships in Section 3.2.

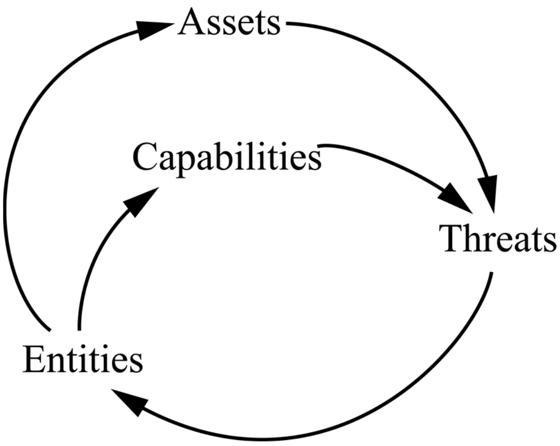


Figure 4. General influence diagram of the basic structure of the Cyber Security Ecosystem of Colombia.

The diagrams that are found in Figures 5–11 establish the relationships within the ecosystem and some of the feedback loops. To simplify the complexity of the influence diagram, all of the entities have been grouped into one element (taking into account that the ecosystem defines certain entities, just as it is described in Section 3.3, Figure 2), and extra elements have been added to represent the dynamic complexity in the ecosystem.

In Figure 5, it is shown how **Entities** develop **Investigation and Development** (**InvDev**) to acquire **Capabilities** that will allow them to manage **Risks** to alleviate **Threats**, which could lead to the perpetration of **Cybercrimes** that affect the **Entities** if they were to occur.

Figure 6 shows that **Resources** are used to acquire **Capabilities** that allow the management of **Risks** to alleviate **Threats**, which could lead to the perpetration of **Cybercrimes**; an increase in these would generate **Strategies** to promote the **Regulations** that will generate **Sanctions (through the application of Laws)** whose implementation would allow new **Resources** for the **Entities**, especially those related to the public sector. Lastly, the **Resources** should be used to carry out **InvDev** that allow for the purchasing of **Capabilities**.

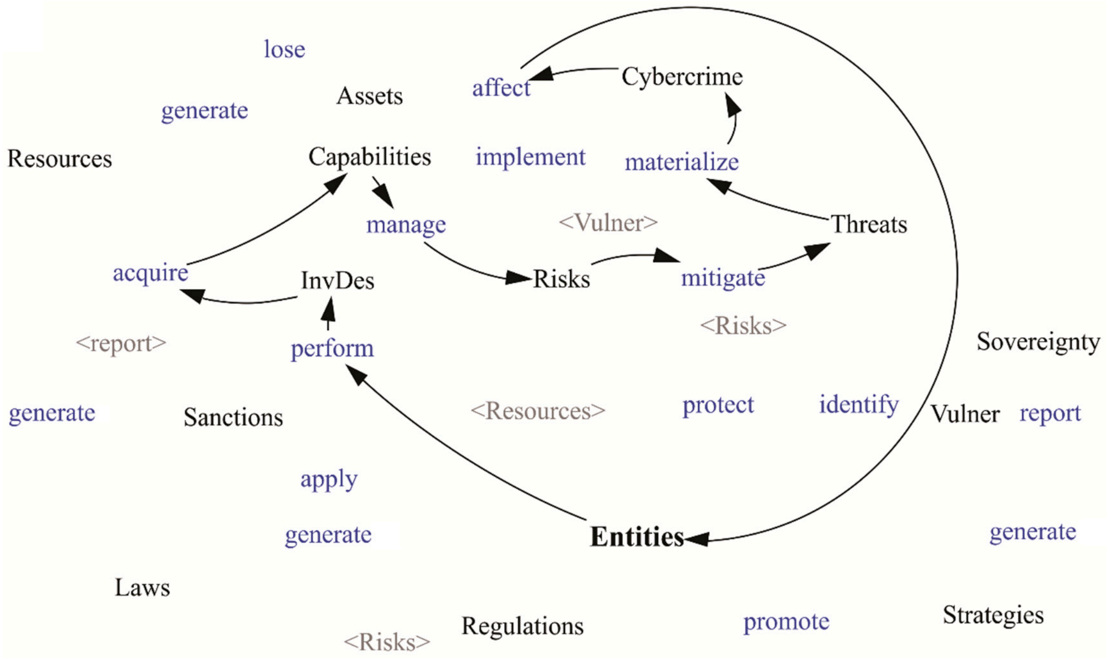


Figure 5. Risk management cycle.

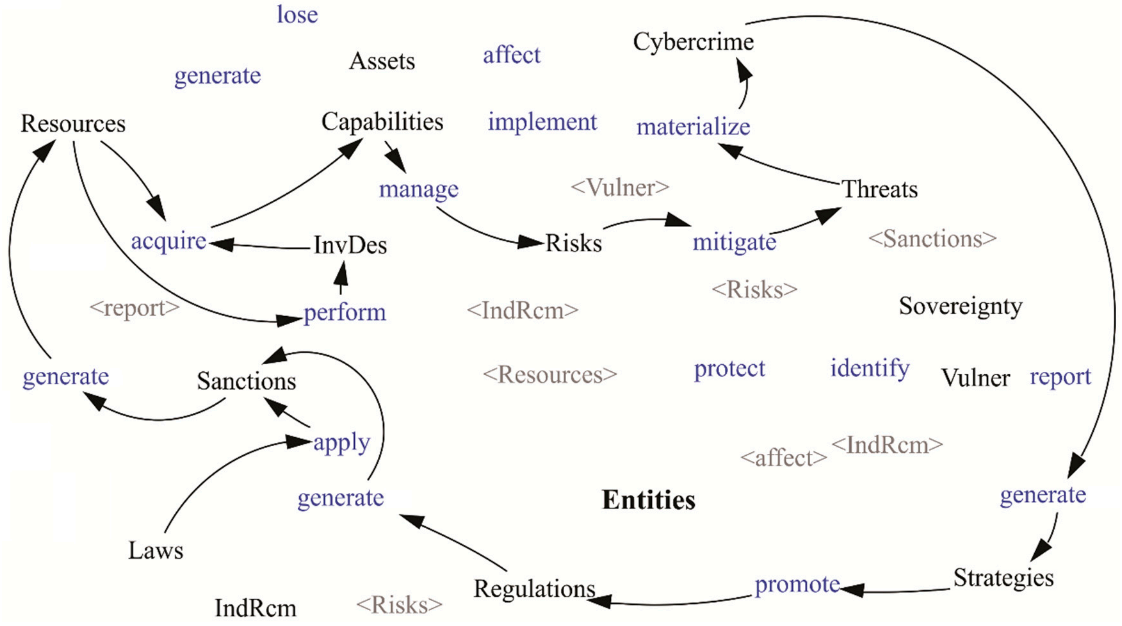


Figure 6. Cycle of crime by capabilities and laws.

Figure 7 illustrates how **Sanctions** (which include fines and punishable sentences to negligent or attacking entities) alleviate the **Threats** that if they were to occur could lead to the perpetration of a **Cybercrime**, which must be reported by and to the **Entities**, so that the appropriate **Sanctions** can be applied in order to reduce **Threats**. In addition to this, managing the **Risks** will also reduce **Threats** and allow the **Entities** the creation of **Indicators and Recommendations** (**IndRcm**) that allow further management of **Risks** and identifying **Vulnerabilities (Vulner)** which can be taken advantage by crime offenders to commit **Cybercrimes.**

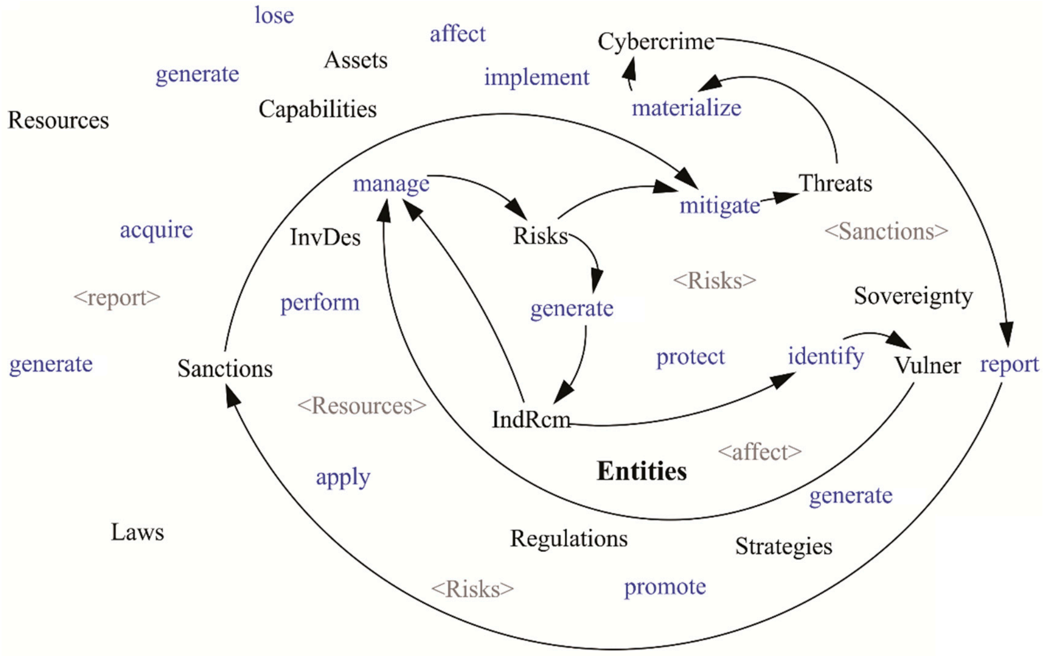


Figure 7. Cycle of crimes by sanctions and vulnerabilities.

In Figure 8, it can be seen how **Resources** are used to acquire **Capabilities** that allow the management of **Risks** to reduce **Threats** that can be materialized for the commission of **Cybercrimes**; an increase in these must generate **Strategies** to promote **Regulation** that will generate **Laws**, whose application will allow to generate new **Resources** for the strengthening of **Capabilities**.

Additionally, **Entities** apply **Sanctions** that will generate **Resources** that allow the purchase of **Assets** to generate more **Resources**, and these lead to the acquirement of **Capabilities** that can be used by illegal **Entities** to commit cybercrimes. **Cybercrimes** generate **Strategies** to promote **Regulations** that transform into **IndRcm** that justify the **Laws** to apply **Sanctions** that generate **Resources**. It is also taken into account that **Cybercrimes** generated losses of **Resources**.

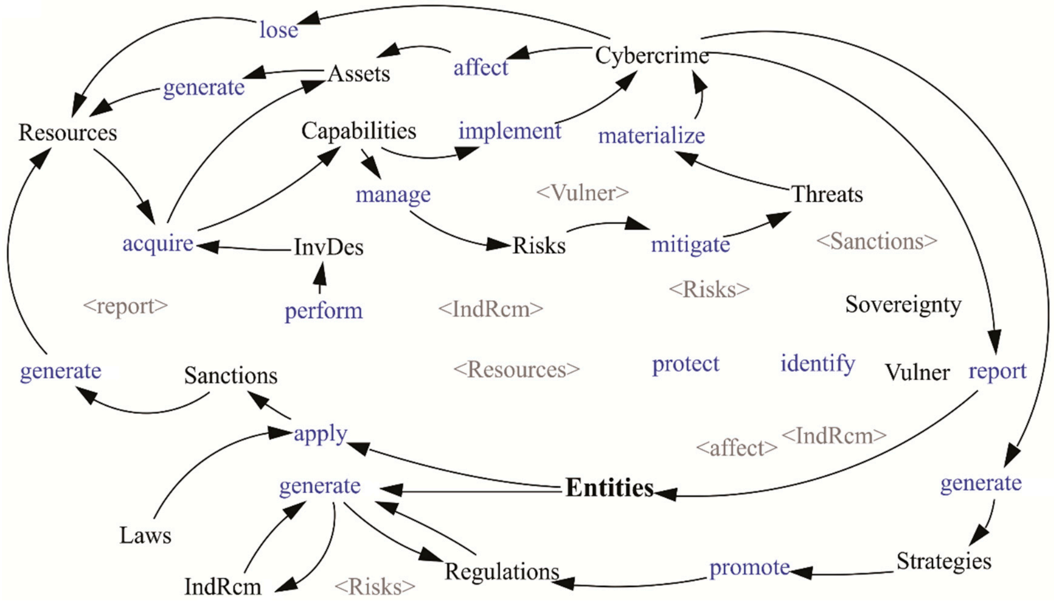


Figure 8. Cycle of crimes by strategies, laws, and sanctions with the participation of assets.

In Figure 9, the relationships of the Entities with other elements are shown, in other words, the actions that are taken by the entities: Report **Cybercrimes**; Generate **Strategies**; Promote **Regulation**; Generate **Regulation, IndRcm, and Laws**; Acquire **Capabilities**; Carry out **InvDev**; Reduce **Threats**; Identify **Vulnerabilities**; Acquire **Assets**.

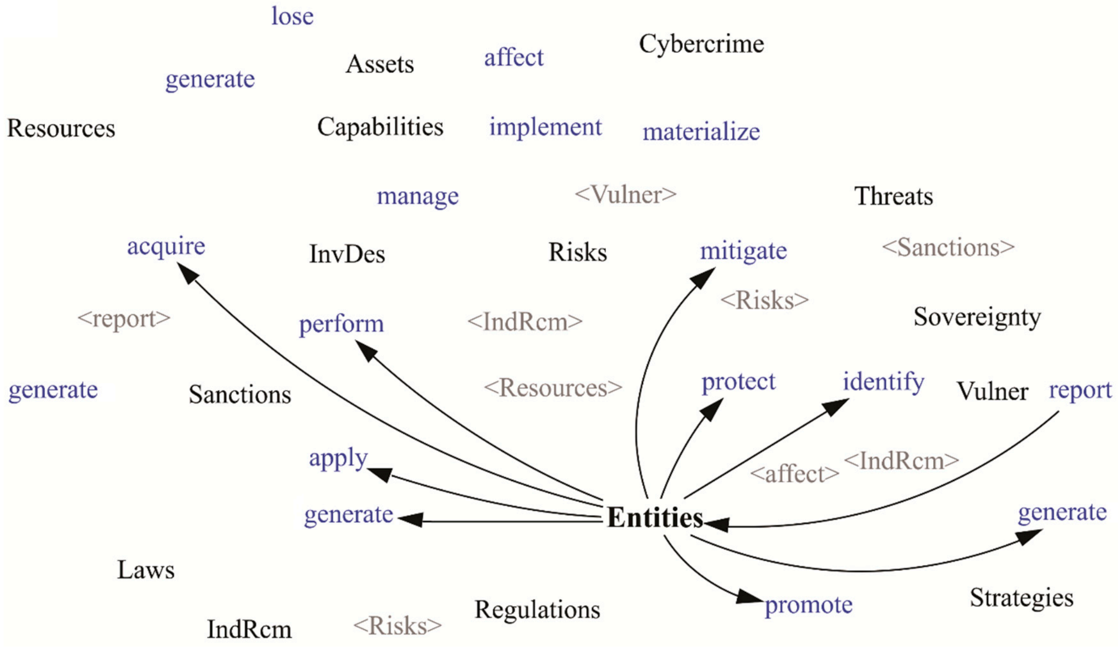


Figure 9. Actions carried out by the entities.

In Figure 10, copies of variables were used (gray elements surrounded with angle brackets that correspond to clones of other elements to avoid crossed lines), and only the relationships between these and other elements were included:

Sanctions require to be reported and enable the reduction of **Threats**.

Resources allow **InvDev** to be carried out.

IndRcm allow the management of **Capabilities** and the identification of **Vulnerabilities**.

Attackers take advantage of **Vulnerabilities** to commit **Cybercrimes,** and the knowledge of them leads to management of **Risks**; the aforementioned management of risk allows the protection of the **Sovereignty** and the generation of **IndRcm**.

In Figure 11, the ecosystem's hypothesis can be seen, which sows some relationships not mentioned before: **Entities** are responsible of generating **IndRcm** that will allow the management of **Risks** so that **Threats** are reduced in case these are carried out and lead to **Cybercrime** offences that are detrimental to other **Entities**. Furthermore, it is shown that the **Capabilities** that are developed may be used to commit **Cybercrimes**.

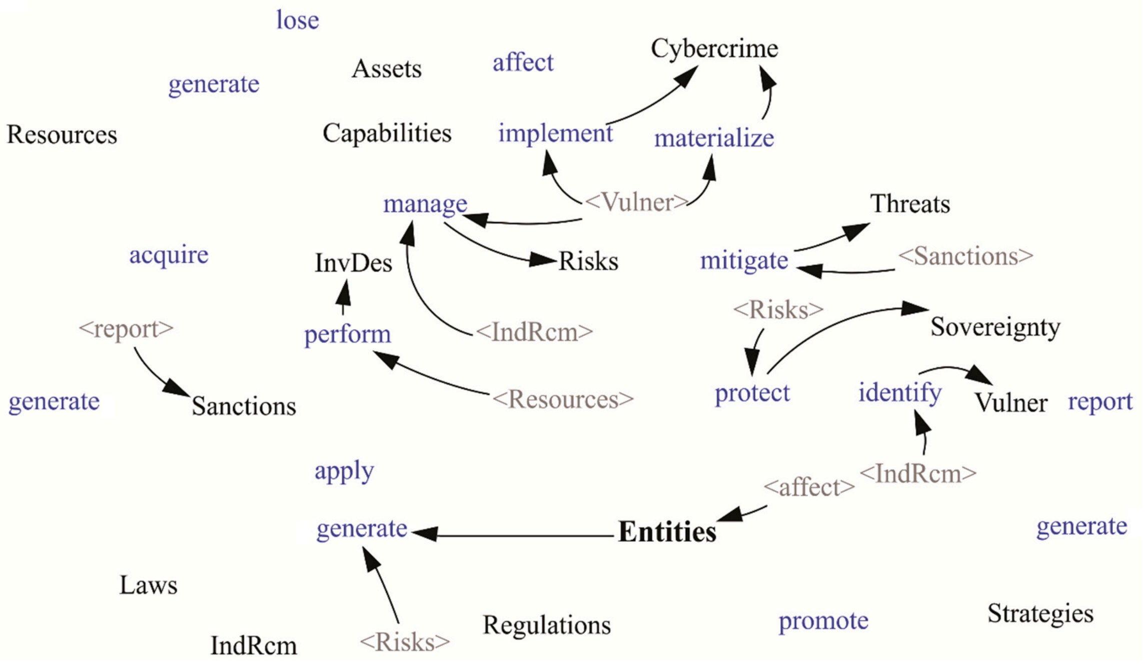


Figure 10. Use of clones to facilitate reading.

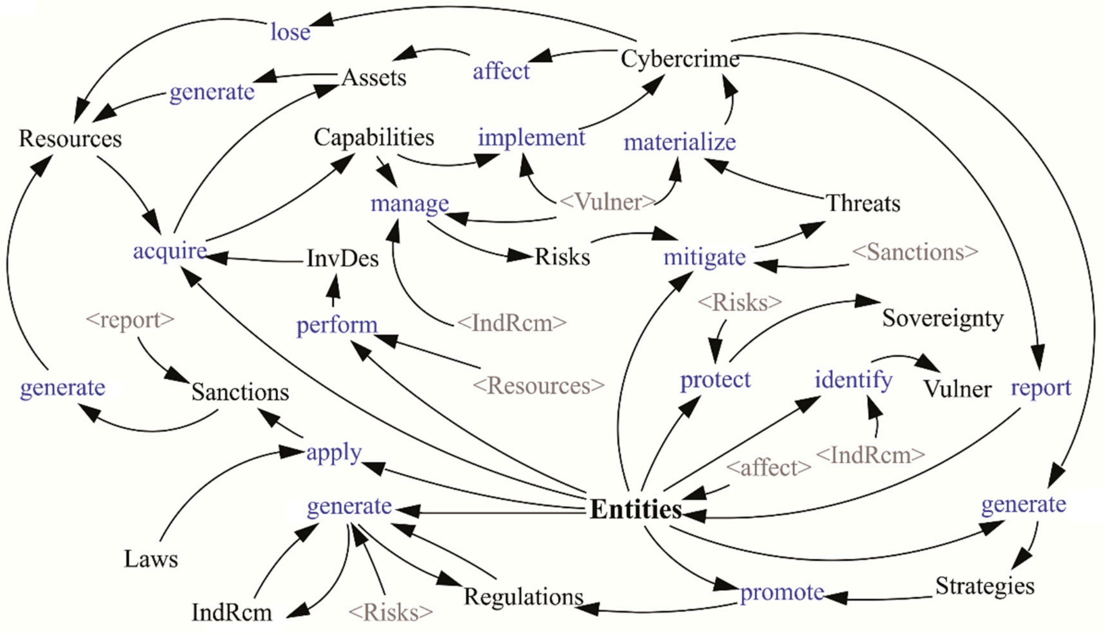


Figure 11. Ecosystem general hypothesis.

4.2. Domain Model of the Cyber Security Ecosystem of Colombia from Software Engineering

This section reveals the behaviour that each of these groups of entities have in regards to cyber security, modelled in four interfaces or contracts that in some cases are common for a specific implementation. These actions are conclusions of the feedback cycles presented in the influence diagrams: for example the method: **Apply sanctions** (**Laws**): **Resources**, obeys the pattern: **Entity –> apply –> Sanctions** (**–> Laws**) **–> Resources**; see Figure 12. This means that entities can give sanctions based on these laws and this will generate new resources.

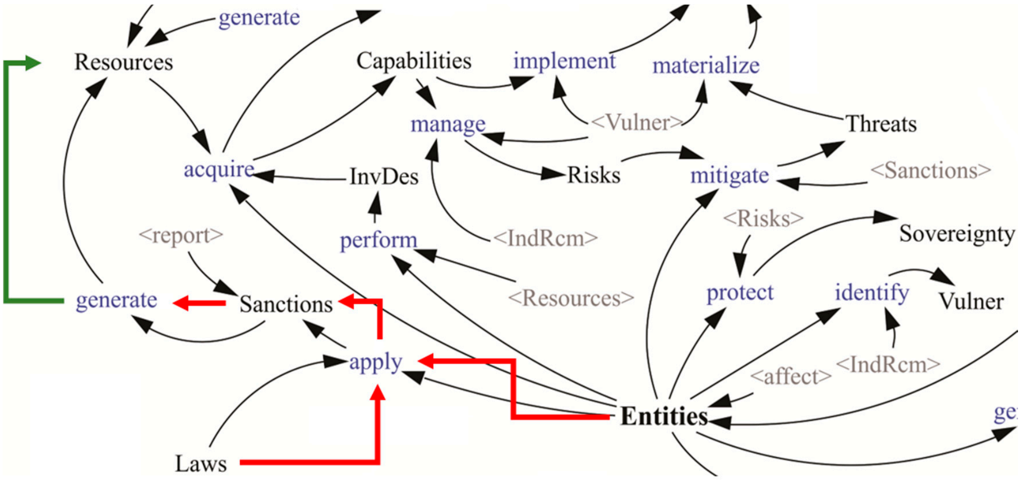


Figure 12. Design pattern.

Once the complexity of the system has been analyzed, the Cyber security Ecosystem of Colombia can be modeled through Software Engineering in a Domain Model, which is developed based on a class diagram to present the relationships and actions taken by entities in Colombia.

The Domain Model requires a detailed specification of the entities, which are shown in the Influences Diagram as a single general variable. Because of that, it's necessary to create a meta model that lists the stereotypes and eases the making of the model.

Meta Model: entities and objects of the domain are specified by the meta model, which is a common representation of the characterization of the different mechanisms involved. Therefore, the ecosystem model is governed by the meta model "Meta Model of the Cyber security Ecosystem of Colombia" that represents the formalities of the entities defined in Section 3.3 (Figure 13) and that describes the following entities:

<<Meta>>Public Sector.
<<Meta>>Private Sector.
<<Meta>>Citizen.
<<Meta>>Research Center.
<<Meta>>Attacker.
<<Meta>>Critical Infrastructure.

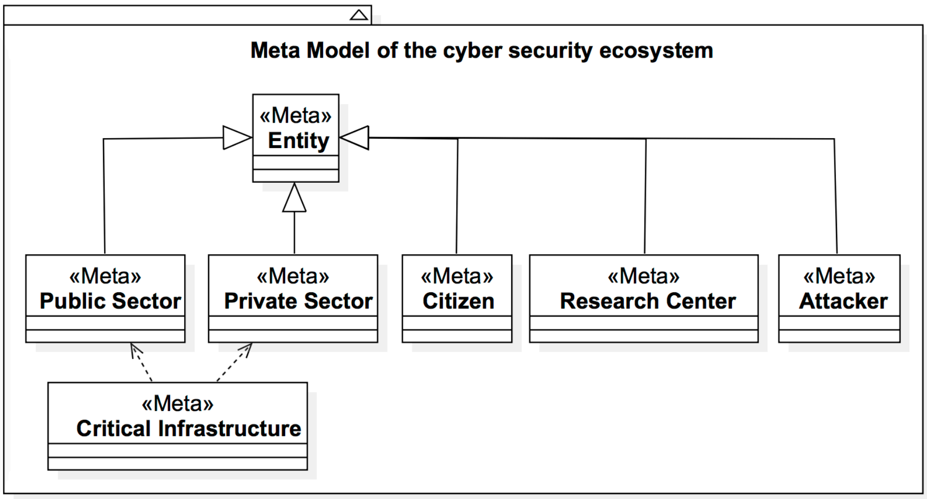
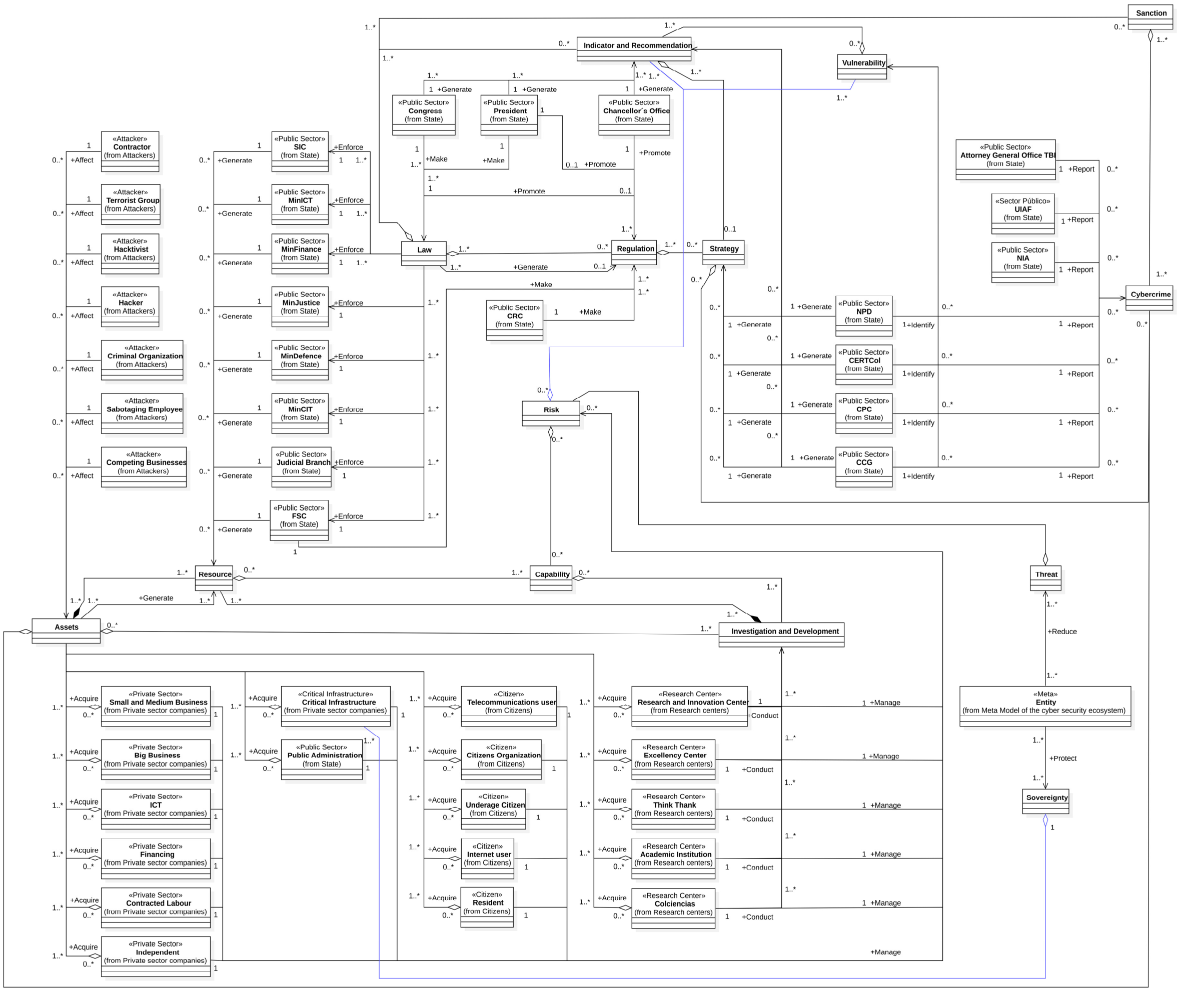


Figure 13. Meta Model of the Cyber security Ecosystem of Colombia.

It is important to point out that the intention is to emphasize Entities as a succinct definition of the basic elements found in the Cyber security Ecosystem of Colombia. In Figure 12, the stereotypes of the public and private sectors, research centers, attackers, and critical infrastructure are important graphical elements in the analysis of the objects that belong to the ecosystem and may be used on their own to represent any of the entities; the Critical Infrastructure entity depends on the public and private sectors due to the fact that they can belong to these two. Although this will not represent a major hierarchy in the meta model, the relationship suggests that the existence (or instance) of a <<Critical Infrastructure >> object will always mantain at least one tie to one of these sectors.

Domain Model: in software development, a domain model is used during the requirements phase as a first step for identifying and formulating objects (entities) and methods (actions) surrounding the problem. The resulting class diagram contains a qualitative description of the problem, in other words, it models the current system. The domain model is not expected to generate a transformation to code in a particular programming language, but it's used to describe the present state of the system using, for example, the Unified Modelling Language (UML); in other words, it's a codified image in UML of the present state of the system.

A model can be read in several ways, such as by taking one of the Entities and following the relationships. For example, in Figure 14:



Sanction
Indicator and Recommendation
Vulnerability
«Public Sector» Congress (from State)
«Public Sector» President (from State)
«Public Sector» Chancellor´s Office (from State)
«Public Sector» Attorney General Office TBI (from State)
«Sector Público» UIAF (from State)
«Public Sector» NIA (from State)
Cybercrime
«Attacker» Contractor (from Attackers)
«Attacker» Terrorist Group (from Attackers)
«Attacker» Hacktivist (from Attackers)
«Attacker» Hacker (from Attackers)
«Attacker» Criminal Organization (from Attackers)
«Attacker» Sabotaging Employee (from Attackers)
«Attacker» Competing Businesses (from Attackers)
«Public Sector» SIC (from State)
«Public Sector» MinICT (from State)
«Public Sector» MinFinance (from State)
«Public Sector» MinJustice (from State)
«Public Sector» MinDefence (from State)
«Public Sector» MinCIT (from State)
«Public Sector» Judicial Branch (from State)
«Public Sector» FSC (from State)
Law
Regulation
Strategy
«Public Sector» CRC (from State)
«Public Sector» NPD (from State)
«Public Sector» CERTCol (from State)
«Public Sector» CPC (from State)
«Public Sector» CCG (from State)
Risk
Resource
Capability
Threat
Assets
Investigation and Development
«Private Sector» Small and Medium Business (from Private sector companies)
«Private Sector» Big Business (from Private sector companies)
«Private Sector» ICT (from Private sector companies)
«Private Sector» Financing (from Private sector companies)
«Private Sector» Contracted Labour (from Private sector companies)
«Private Sector» Independent (from Private sector companies)
«Critical Infrastructure» Critical Infrastructure (from Private sector companies)
«Public Sector» Public Administration (from State)
«Citizen» Telecommunications user (from Citizens)
«Citizen» Citizens Organization (from Citizens)
«Citizen» Underage Citizen (from Citizens)
«Citizen» Internet user (from Citizens)
«Citizen» Resident (from Citizens)
«Research Center» Research and Innovation Center (from Research centers)
«Research Center» Excellency Center (from Research centers)
«Research Center» Think Thank (from Research centers)
«Research Center» Academic Institution (from Research centers)
«Research Center» Colciencias (from Research centers)
«Meta» Entity (from Meta Model of the cyber security ecosystem)
Sovereignty
+Affect
+Generate
+Enforce
+Make
+Promote
+Identify
+Report
+Acquire
+Conduct
+Manage
+Reduce
+Protect
1
0..*
1..*
0..1

Figure 14. Domain Model of the Cyber Security Ecosystem of Colombia.

Using as reference point what was suggested in the meta model based on the results of the analysis of each component and the relationships studied from the classical point of view to the application of influence diagrams in system dynamics, the domain model is composed of three sections that group in a conceptual basis the entities of the Cyber security Ecosystem of Colombia: State, Attackers and Sectors.

At the left, it's shown that Assets generate and are composed by Resources, which can be affected by an <<Attacker>> and acquired by the <<Private Sector>>, the <<Public Sector>>, a <<Citizen>> or a <<Research Center>>. Also, Resources generate Investigation and Development, whose results can be transformed into Capabilities that allow the addition of new Assets.

Laws are composed by Sanctions, Regulations and Indicators and Recommendations, and are applied by the <<Public Sector>> (ministries), are created by the Congress and the President and are promoted by them and, in some specific cases, by the Chancellor's Office. Besides, Regulations and Indicators and Recommendations are composed by Strategies that are generated by the <<Public Sector>>, which identifies the existing Vulnerabilities and reports Cybercrime that must have a Sanction defined.

The <<Private Sector>>, <<Public Sector>>, <<Research Center>>, <<Citizen>> and <<Critical Infrastructure>> are responsible of handling their own Risks by using their Resources, their Capabilities and their knowledge of existing Vulnerabilities, Indicators and Recommendations.

1. **State** (Figure 15): composed by the organisms or institutions that have a direct relationship with anything related to cyber security in the public sector:

    <<Public Sector>> President.
    <<Public Sector>> Congress.
    <<Public Sector>> Chancellor´s Office.
    <<Public Sector>> NIA.
    <<Public Sector>> MinDefence.
        <<Public Sector>> CPC.
        <<Public Sector>> CCG.
        <<Public Sector>> CERTCol.
    <<Public Sector>> NPD.
    <<Public Sector>> MinICT.
        <<Public Sector>> CRC.
    <<Public Sector>> MinJustice.
    <<Public Sector>> MinCIT.
        <<Public Sector>> SIC.
    <<Public Sector>> MinFinance.
        <<Public Sector>> FSC.
    <<Public Sector>> Judicial Branch.
    <<Public Sector>> Attorney General Office – TBI
    <<Public Sector>> Public Administration.
    <<Critical Infrastructure>> Critical Infrastructure.

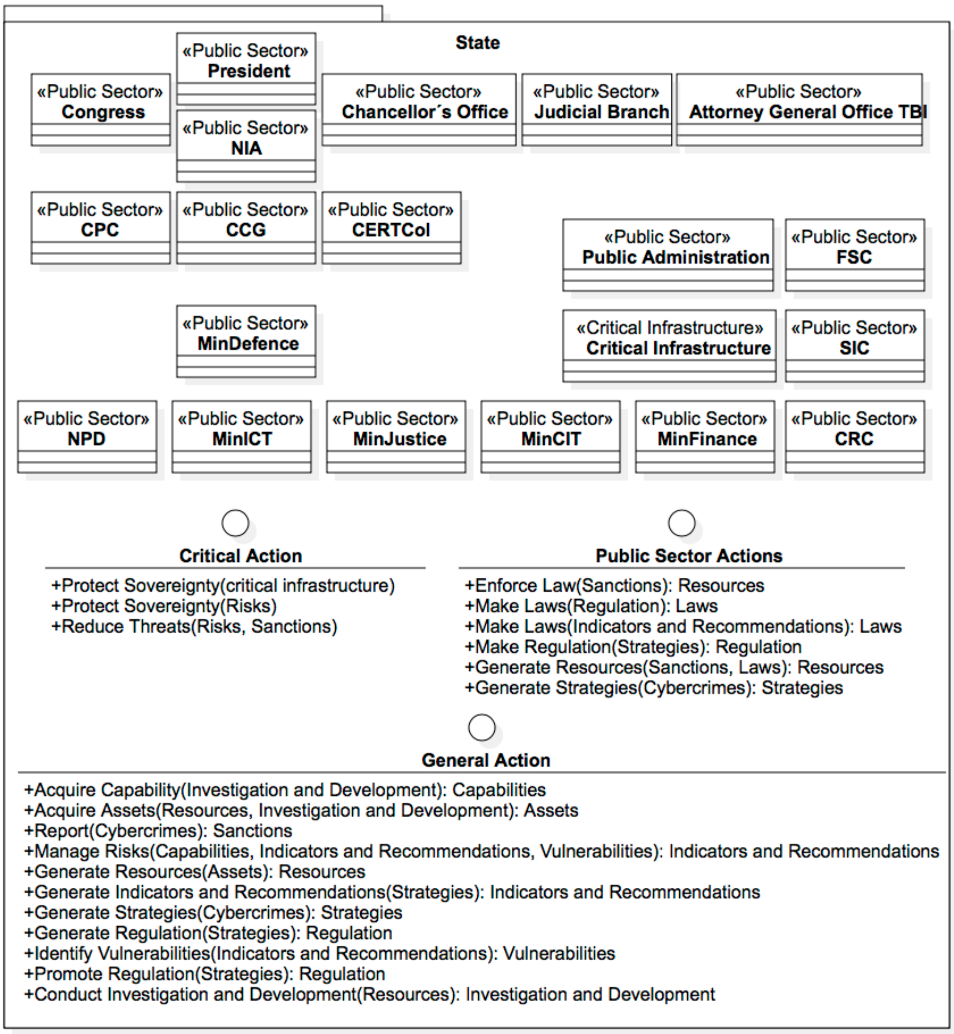

State
«Public Sector» President
«Public Sector» Congress
«Public Sector» NIA
«Public Sector» Chancellor´s Office
«Public Sector» Judicial Branch
«Public Sector» Attorney General Office TBI
«Public Sector» CPC
«Public Sector» CCG
«Public Sector» CERTCol
«Public Sector» Public Administration
«Public Sector» FSC
«Public Sector» MinDefence
«Critical Infrastructure» Critical Infrastructure
«Public Sector» SIC
«Public Sector» NPD
«Public Sector» MinICT
«Public Sector» MinJustice
«Public Sector» MinCIT
«Public Sector» MinFinance
«Public Sector» CRC
Critical Action
+Protect Sovereignty(critical infrastructure)
+Protect Sovereignty(Risks)
+Reduce Threats(Risks, Sanctions)
Public Sector Actions
+Enforce Law(Sanctions): Resources
+Make Laws(Regulation): Laws
+Make Laws(Indicators and Recommendations): Laws
+Make Regulation(Strategies): Regulation
+Generate Resources(Sanctions, Laws): Resources
+Generate Strategies(Cybercrimes): Strategies
General Action
+Acquire Capability(Investigation and Development): Capabilities
+Acquire Assets(Resources, Investigation and Development): Assets
+Report(Cybercrimes): Sanctions
+Manage Risks(Capabilities, Indicators and Recommendations, Vulnerabilities): Indicators and Recommendations
+Generate Resources(Assets): Resources
+Generate Indicators and Recommendations(Strategies): Indicators and Recommendations
+Generate Strategies(Cybercrimes): Strategies
+Generate Regulation(Strategies): Regulation
+Identify Vulnerabilities(Indicators and Recommendations): Vulnerabilities
+Promote Regulation(Strategies): Regulation
+Conduct Investigation and Development(Resources): Investigation and Development

Figure 15. State Entities.

The aforementioned elements that make part of the State correspond to the current vision of the Cyber security Ecosystem of Colombia and represent the entities that generate a reaction that affects all the other elements in the system if they were to take some sort of action, for this reason coordination and collaboration are fundamental within public entities when it comes to cyber security. The package also includes three interfaces that define the actions that could take place in terms of cyber security, being a result of the analysis of influence diagrams described in Section 4.1.

2. **Attackers** (Figure 16): entities capable of affecting other entities or their assets. Any entity found in the model can be included in this group if their actions lead to the commitment of a cybercrime.

<<Attackers>> Hacktivist.
<<Attackers>> Hacker.
<<Attackers>> Contractor.
<<Attackers>> Criminal organization.
<<Attackers>> Terrorist group.
<<Attackers>> Competing businesses.
<<Attackers>> Sabotaging employee

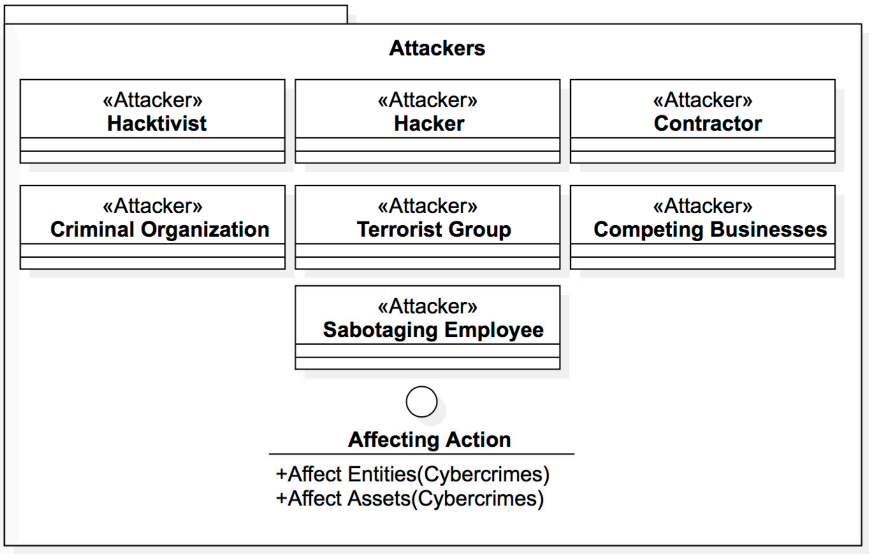


Figure 16. Attackers.

The attackers represent all the entities seen as potential cybercrime offenders. The model shows these entities in a separate package, but it's necessary to note that, as happens in the Object Oriented Programing paradigm, where one object may inherit attributes and methods from another one, any of the entities presented in the model can play the role of an attacker, or, as should be said in terms of the model, they may generalize the behavior of the Attacking class at any time.

3. **Sectors** (Figure 17) (Private sector, citizens, research centers):

<<Private Sector>> Big business.
<<Private Sector>> Small and medium business.
<<Private Sector>> Independent.
<<Private Sector>> Contracted labor.
<<Private Sector>> Financing.
<<Private Sector>> ICT.
<<Critical Infrastructure>> Critical Infrastructure.
<<Citizen>> Internet user.
<<Citizen>> Telecommunications user.
<<Citizen>> Citizens Organizations.
<<Citizen>> Underage citizens.
<<Citizen>> Residents.
<<Research center>> Colciencias.
<<Research center>> Academic institutions.
<<Research center>> Excellency center.
<<Research center>> Think thank.
<<Research center>> Research and innovation center.

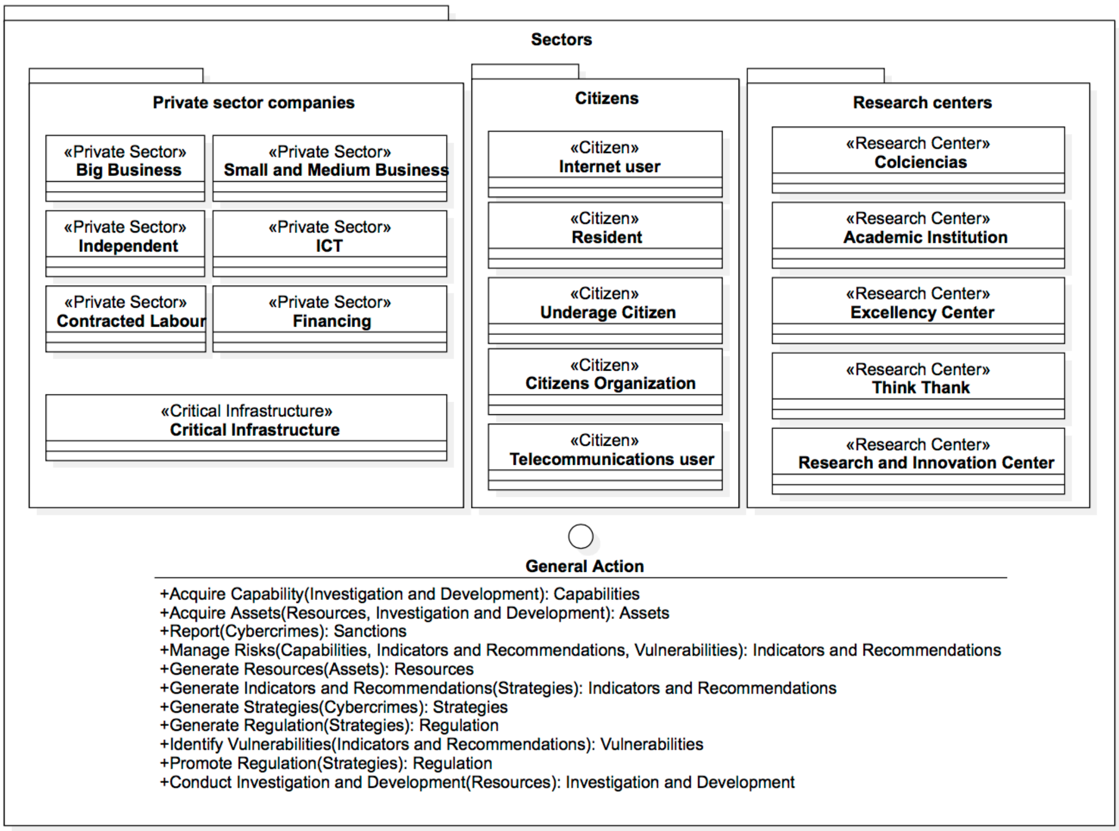

Sectors
Private sector companies
«Private Sector» Big Business
«Private Sector» Small and Medium Business
«Private Sector» Independent
«Private Sector» ICT
«Private Sector» Contracted Labour
«Private Sector» Financing
«Critical Infrastructure» Critical Infrastructure
Citizens
«Citizen» Internet user
«Citizen» Resident
«Citizen» Underage Citizen
«Citizen» Citizens Organization
«Citizen» Telecommunications user
Research centers
«Research Center» Colciencias
«Research Center» Academic Institution
«Research Center» Excellency Center
«Research Center» Think Thank
«Research Center» Research and Innovation Center
General Action
+Acquire Capability(Investigation and Development): Capabilities
+Acquire Assets(Resources, Investigation and Development): Assets
+Report(Cybercrimes): Sanctions
+Manage Risks(Capabilities, Indicators and Recommendations, Vulnerabilities): Indicators and Recommendations
+Generate Resources(Assets): Resources
+Generate Indicators and Recommendations(Strategies): Indicators and Recommendations
+Generate Strategies(Cybercrimes): Strategies
+Generate Regulation(Strategies): Regulation
+Identify Vulnerabilities(Indicators and Recommendations): Vulnerabilities
+Promote Regulation(Strategies): Regulation
+Conduct Investigation and Development(Resources): Investigation and Development

Figure 17. Sectors.

Critical action (Figure 18): procedures and actions carried out by entities for the protection of the country when faced with cybernetic incidents. This interface was determined as one of the most relevant derivations of the actions that are taken by the different groups of the model and that represent the effort that Colombia makes when it comes to cyber security.

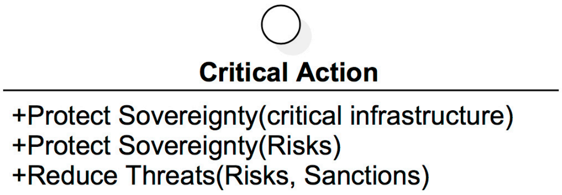

Critical Action
+Protect Sovereignty(critical infrastructure)
+Protect Sovereignty(Risks)
+Reduce Threats(Risks, Sanctions)

Figure 18. State critical actions.

The methods, actions or procedures that the State must carry out are:
Protect the Sovereignty (critical infrastructure).
Protect Sovereignty (Risks).
Reduce Threats (Risks, Sanctions).

Public sector actions (Figure 19): models the behaviour of public sector entities.

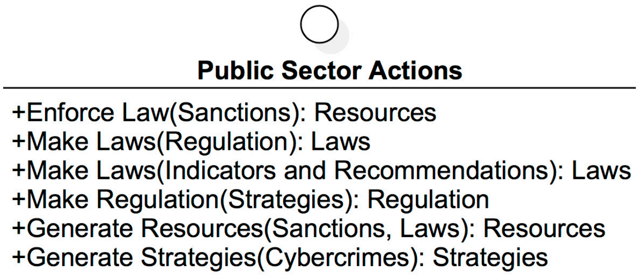

Public Sector Actions
+Enforce Law(Sanctions): Resources
+Make Laws(Regulation): Laws
+Make Laws(Indicators and Recommendations): Laws
+Make Regulation(Strategies): Regulation
+Generate Resources(Sanctions, Laws): Resources
+Generate Strategies(Cybercrimes): Strategies

Figure 19. Public sector actions.

The methods, actions, or procedures that the public sector must carry out are:
Enforce Sanctions (Laws): Resources.
Make Laws (Regulation): Laws.
Make Laws (Indicators and Recommendations): Laws.
Make Regulation (Strategies): Regulation.
Generate Resources (Sanctions, Laws): Resources.
Generate Strategies (Cybercrimes): Strategies.

General action (Figure 20): this interface contains the general actions that Colombian entities make in terms of cyber security.

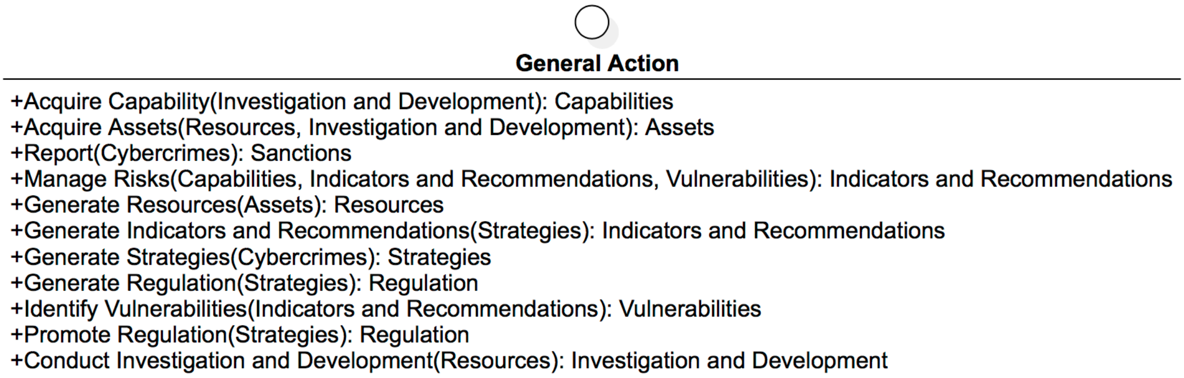

General Action
+Acquire Capability(Investigation and Development): Capabilities
+Acquire Assets(Resources, Investigation and Development): Assets
+Report(Cybercrimes): Sanctions
+Manage Risks(Capabilities, Indicators and Recommendations, Vulnerabilities): Indicators and Recommendations
+Generate Resources(Assets): Resources
+Generate Indicators and Recommendations(Strategies): Indicators and Recommendations
+Generate Strategies(Cybercrimes): Strategies
+Generate Regulation(Strategies): Regulation
+Identify Vulnerabilities(Indicators and Recommendations): Vulnerabilities
+Promote Regulation(Strategies): Regulation
+Conduct Investigation and Development(Resources): Investigation and Development

Figure 20. Entities' General actions.

The methods, actions, or procedures that must be carried out by entities on a general level are:
Acquire Capability (Investigation and Development): Capabilities.
Acquire Assets (Resources, Investigation and Development): Assets.
Report (Cybercrimes): Sanctions.
Manage Risks (Capabilities, Indicators and Recommendations, Vulnerabilities): Indicators and Recommendations.
Generate Resources (Assets): Resources.
Generate Indicators and Recommendations (Strategies): Indicators and Recommendations.
Generate Strategies (Cybercrimes): Strategies.Generate Regulation (Strategies): Regulation.
Identify Vulnerabilities (Indicators and Recommendations): Vulnerabilities.
Promote Regulation (Strategies): Regulation.
Realize Investigation and Development (Resources): Investigation and Development.

Affecting action (Figure 21): this shows an interface that defines the behaviour of illegal entities:

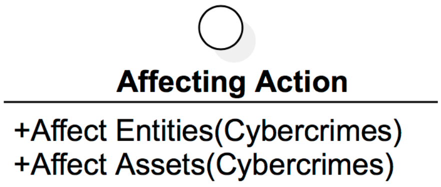


Figure 21. Attackers' Actions.

The methods that illegal entities use are:
Affect Entities (Cybercrimes).
Affect Assets (Cybercrimes).

Relationships have been omitted in the diagrams in order to simplify them and ease their understanding by the reader. However, it's possible to visualize the interactions between entities if packages are seen as relation elements.

5. Conclusions

Through the execution of an iterative process, Influence Diagrams contributed to the generation of Domain Diagrams for understanding the complexity in the interdisciplinary work of the authors, and for specifying a pattern that could help to identify entities and their methods for the Domain Model: (a) an entity corresponds to a variable in the Influence Diagram whose first letter is capitalized; (b) an action corresponds to the result of merging both origin and destination of a relationship that ends in an entity (first letter in lowercase); (c) an input (or method argument) is the variable from which the relationship to an entity came from; (d) the result of the aforementioned action are the variables to which the relationship will lead to.

The analysis of the Ecosystem is based on two languages, and it integrates Software Engineering with System Dynamics. The Domain Model shows the Ecosystem in a static way; it was created as a proposed alternative for the comprehension of the system's dynamic structure which was modeled with the Influences Diagram.

The Influence Diagram facilitates an analysis that shows that cybercrimes influence four actions, and the problems that arise if they are exploited by illegal entities. This helps to understand the importance of avoiding cybercrimes. Additionally, it is observed that sovereignty is the only element that doesn't influence others elements, therefore, it's possible to conclude that sovereignty is the main element to be protected in the Cyber security Ecosystem of Colombia along with entities whose resources and assets can be affected by the commission of cybercrimes.

The activities to be carried out by entities in the Domain Model presented in the interfaces that do not generate products (Figures 12–21) are the most essential actions in the Cyber security Ecosystem of Colombia: "protecting sovereignty" and "reducing threats". This is coherent with the results obtained in the Influence Diagram. The remaining methods can be considered actions that should contribute to achieving these essential objectives.

The Domain Model can be used to design a knowledge management system oriented to coordinate the efforts that Colombian entities make in regards to cyber security in the ecosystem.

Finally, the analysis of dynamic complexity formulated and specified in the Domain Model clearly shows the importance of cyber security as a fundamental and strategic component of national security.

Acknowledgments: The authors would like to express their gratitude to the Administrative Department of Science, Technology, and Innovation (Colciencias), the Ministry of Information and Communication Technologies (MinICT), since this article is made possible as a result of the research project "Feasibility study of the creation of a National Cyber security Observatory in Colombia", which was approved by Colciencias' program calling 668 of 2014, for the strengthening of cyber security in government institutions. Additionally, we are grateful with the project executing entity: Universidad Pontificia Boliviariana and the beneficiary businesses attached to this project: Secretary of Information and Communication Technologies of Santander (SETIC), TYT S.A.S, ISL

S.A., ESI Colombia S.A.S, and TICService Solutions S.A.S. Finally, we express our gratitude to the international consultants of EstudNet S.L. who immensely contributed to the development of this initiative.

Author Contributions: Angélica Flórez contributed to the design of the proposed Ciber security Ecosystem of Colombia, supervised the research activities, and then carried out the coordination activities and the analysis of results. Lenin Serrano and Urbano Gómez conceived and wrote the domain model and the influence diagram. Hugo Rodríguez conceived and wrote the legal component. Luis Suárez and Alejandro Villarraga contributed to the advancement of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Organización de los Estados Americanos. Misión de Asistencia Técnica en Seguridad Cibernética: Conclusiones y Recomendaciones. Available online: http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_SPA.pdf (accessed on 10 March 2015).
2. Schaffernicht, M. *Indagación de Situaciones Complejas Mediante la Dinámica de Sistemas*; Editorial Universidad de Talca: Santiago de Chile, Chile, 2009.
3. Oropeza Cortés, M.G.; Urciaga García, J.I.; Ponce Díaz, G. Importancia Económica y Social de los Servicios de los Ecosistemas: Una revisión de la Agenda de Investigación. *Rev. Glob. Negoc.* **2015**, *3*, 103–113.
4. García-Holgado, A.; García-Penalvo, F.J. Análisis de integración de soluciones basadas en software como servicio para la implantación de ecosistemas tecnológicos corporativos. *Repos. Doc. Univ. Salamanca* **2013**. Available online: http://gredos.usal.es/jspui/handle/10366/122472 (accessed on 4 July 2016).
5. Andrade, H.; Dyner, I.; Espinosa, A.; López, H.; Sotaquirá, R. *Pensamiento Sistémico: Diversidad en Búsqueda de Unidad*; Universidad Industrial de Santander: Santander, Colombia, 2001.
6. Gómez, U.E.; Andrade, H.H.; Vásquez, C.A. Lineamientos Metodológicos para construir Ambientes de Aprendizaje en Sistemas Productivos Agropecuarios soportados en Dinámica de Sistemas. *Inf. Tecnol.* **2015**, *26*, 125–136. [CrossRef]
7. ISO/IEC. *International Standard ISO/IEC 27032: Information Technology—Security techniques—Guidelines for Cybersecurity*; ISO/IEC: Geneva, Switzerland, 2012.
8. Larman, C. *UML y Patrones*, 2nd ed.; Pearson Prentice Hall: Madrid, Spain, 2005; pp. 121–165.
9. Consejo Nacional de Política Económica y Social. República de Colombia. Departamento Nacional de Planeación. Documento CONPES 3701. Available online: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf (accessed on 12 June 2015).
10. República de Colombia. Constitución Política de Colombia. Available online: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html (accessed on 10 June 2015).
11. El Congreso de Colombia. Ley No. 1341. Available online: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf (accessed on 12 June 2015).
12. Ministerio de Defensa Nacional. Decreto 1512 de 2000. Available online: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Sobre_el_Ministerio/fondelibertad/Dec_1512_2000.pdf (accessed on 12 June 2015).
13. Ministerio de Defensa Nacional. Resolución 127 de 2012. Available online: http://www.icbf.gov.co/cargues/avance/docs/resolucion_mindefensa_0127_2012.htm (accessed on 10 June 2015).
14. Ministerio de Defensa Nacional. Resolución 3933 de 2013. Available online: http://www.icbf.gov.co/cargues/avance/docs/resolucion_mindefensa_3933_2013.htm (accessed on 12 June 2015).
15. Presidente de la República de Colombia. Decreto 3355 de 2009. Available online: https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/decreto_3355_2009.htm (accessed on 5 June 2015).
16. Departamento Nacional de Planeación. Subdirección de Seguridad y Defensa: Gobierno de Colombia. Available online: https://www.dnp.gov.co/programas/justicia-seguridad-y-gobierno/Paginas/subdireccion-de-seguridad-y-defensa.aspx (accessed on 12 June 2015).
17. Departamento Administrativo de la Función Pública. Decreto Número 2897 de 2011. Available online: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Agosto/11/dec289711082011.pdf (accessed on 5 June 2015).
18. Ministerio de Hacienda y Crédito Público. Ministerio de Hacienda y Crédito Público: ¿Conoces el Ministerio? Available online: http://www.minhacienda.gov.co/HomeMinhacienda/elministerio (accessed on 10 June 2015).

19. Ministerio de Comercio, Industrial y Turismo. Misión, Visión, Objetivos, Normas y Principios Éticos. Available online: http://www.mincit.gov.co/publicaciones.php?id=13 (accessed on 5 June 2015).
20. Superintendencia Financiera de Colombia. Acerca de la Superintentencia Finanaciera de Colombia. Available online: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=60607#funciones2 (accessed on 7 June 2015).
21. Superintendencia Financiera de Colombia. Circular Externa 052 de 2007. Available online: https://www.superfinanciera.gov.co/SFCant/ConsumidorFinanciero/ce05207.docx (accessed on 12 June 2015).
22. El Congreso de Colombia. Ley Estatutaria No. 1581. Available online: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf (accessed on 4 June 2015).
23. Departamento de Seguridad Nacional de España. Estrategia de Seguridad Nacional: Un Proyecto Compartido. Anvailable online: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfialaccesiblebpdf.pdf (accessed on 9 May 2015).
24. Booch, G.; Rumbaugh, J.; Jacoboson, I. *El Lenguaje Unificado de Modelado*; Pearson: Madrid, Spain, 2004.