Cyber security and cyber defense for Venezuela: an approach from the Soft Systems Methodology

Douglas Torres^{1,2}

Received: 8 June 2015 / Accepted: 7 February 2018 / Published online: 6 March 2018
© The Author(s) 2018. This article is an open access publication

Abstract

The use of the Internet by large sectors of society represents the interaction through information technology infrastructure, communication networks, information systems and telecommunications, as it determines the presence and exposure of cyber threats. The Soft Systems Methodology (SSM) was used to transit between observed reality and the world of systems, where emerges a Strategic Cyber Security and Cyber Defense Model (SCSCDM), proposed as a component of the security, defense and integral development of Venezuela. The human activities system foresees five subsystems: universal and inalienable guarantees of fundamental rights and freedoms of citizens; research, prevention, detection and management of cyber incidents; strengthening of economic welfare and social progress based on the development of information technology and communication; democratic, participatory, protagonist and pluralistic society; international cooperation and projection of cyber realm. The proposed system of human activities provides interaction with the environment where it is inserted, so the elements with which it interacts are identified.

Keywords Cyber security · Cyber defense · Soft Systems Methodology · Strategic model

Abbreviations

CAIDA	Center for Applied Internet Data Analysis	PLCs	Programmable Logic Controllers
CATWOE	Clients; Actors; Transformation; Weltanschauung, Owner, Environment	PWC	PricewaterhouseCoopers
CERT	Computer Emergency Readiness Team	SDSC	San Diego Supercomputer Center of the University of California San Diego
CSDP	Common Security and Defense Policy of the European Union	SCADA	Supervisory Control and Data Acquisition
DDoS	Distributed Denial of Service	SCSCDM	Strategic Cyber Security and Cyber Defense Model
DoS	Denial-of-Service	SOC	Command and Control Center for Cyber Threats of Israel
EMCSR	European Meeting on Cybernetics and Systems Research	SSF	Strategic Support Force of People's Republic of China
EU	The European Union	SSM	Soft Systems Methodology
IBM	International Business Machines	UCSD	University of California San Diego
INCB	Israel National Cyber Bureau	UNODC	United Nations Office on Drugs and Crime
ITU	International Telecommunication Union	VenCERT	Venezuela Computer Emergency Readiness Team
NATO	North Atlantic Treaty Organization	YAHAV	Mission of the Unit for Cyber Security in the Government of Israel
NCB	National Cyber Bureau of Israel		
OCO	Offensive Cyber Operations of North Korea		

✉ Douglas Torres
torres.douglas@gmail.com; dtorres@unefa.edu.ve

¹ Centro de Investigaciones Postdoctorales CIPOST-UCV, Caracas, Venezuela

² UNEFA, Caracas, Venezuela

Introduction

The development of information technology and telecommunications has shown a positive impact on society. Along with these advances illegal actions have appeared and carried out

with the use of these technologies. On April 2007, the Republic of Estonia was subjected to a cyber attack, when for three consecutive weeks their computer networks collapsed motivated to a systematic distributed denial-of-service (DDoS), forwarding official Internet pages to false pages and blocking Internet sites pages, among other modalities. The head of IT security at Estonia's in 2007, Mikhail Tammet indicated that Estonia depends of internet, have e-government, all the bank services are on the internet and the parliament is elected by internet [1].

On August 2008 Russia invaded Georgia, both Republics of the former Soviet Union, to gain control of the breakaway Georgian regions of South Ossetia and Abkhazia. This military escalation is also said to be cybernetic. These military acts between Russia and Georgia on August 2008 have the distinction of events that coincided operations of conventional warfare and cyber warfare and was a first step towards a new era in which virtual attacks could accompany the actual fire [2]. Lesk [3] and Guadamuz [4] indicated that this event was called as Internet War I. Clarke [5] mentions the attack of Israeli fighter bombers on September 7, 2007, on secret facilities in Syria. In this event there was electronic intervention of Syria detection radars, through cyber manipulation, conducted by the Israeli secret services [5].

The North Atlantic Treaty Organization (NATO) is a cooperation and military security agency, and considered this attack as new, important and dangerous and led to the creation in 2007, of the NATO Cooperative Cyber Defense Centre of Excellence based in Tallinn, capital of Estonia [6]. Between March 2015 and February 2017, one-third of the Internet was subject to some kind of cyber attack [7].

Cyber incidents and STUXNET as a new phase in cyber operations

In 2010 the nuclear development project of the Islamic Republic of Iran was attacked by a “worm” called Stuxnet which affected at least 60,000 computers. This sophisticated virus in its conception was aimed to modify software of SCADA (Supervisory Control and Data Acquisition) systems that controlled the process of uranium enrichment in Iran's nuclear program. Symantec shows in *W32.Stuxnet Dossier* [8], that the goal of Stuxnet is reprogramming the Programmable Logic Controllers (PLCs). Authorities of Iran reaffirmed its determination to maintain its controversial nuclear program, and recognized that Stuxnet computer virus affected the operation of centrifuges that enriched uranium.

The cyber attack against Iranian nuclear was subsequently recognized by the United States. The President Obama decided accelerate the attacks, initiated by the Bush administration, in operation called Olympic Games and ordered sophisticated attacks against the computer systems that ran Iran's nuclear main enrichment [9].

On February 17, 2011, Canada suffered a cyber attack on a large scale in at least three key departments of government: the Finance Department, the Treasury Board, and Defense Research and Development. The Canadian Prime Minister Harper Stephen assured that cyber security must be a key element in Canada's homeland security [10]. This attack forced the government departments of Canada that were attacked, to disconnect temporarily from the internet.

On August 2012 Saudi Arabian Oil Co., the world's largest state-owned crude oil exporter, received cyber attacks with significant effects on their operational processes and loss of confidential data. Aramco's computer system was disabled for a month, as more than 30,000 computers and 2000 servers were affected, destroyed the hard drives of more than 60% of computers, wiped out data on the company's servers, including the domain management servers [10].

On January 2013 several newspapers of United States announced they had received cyber attacks: The Washington Post, The New York Times and The Wall Street Journal, revealed they have suffered cyber attacks and suspected the involvement of Chinese hackers. These leaks consisted on computer espionage and extraction of information related to confidential data, key journalists access to computer services and other damages. These cyber attacks against US interests are considered attacks to national security and may require a reaction. The US president has the authority to order preventive cyber attacks if discovered evidence of preparing a large digital attack on the country [11].

The US authorities have understood the strategic nature of this new dimension, the importance of their actions and the impact that their security and defense policies represent to this new reality and The Pentagon has created a cyber command, cyber weapons and cyber policies. The attacks against Iran show infrastructures of a nation can be attacked through cyberspace [11].

The concern over cyber attacks has been in discussions at the United Nations, where besides appreciating the danger of these actions, is reaffirmed the need to cooperate and act in terms of international agreements. The then Secretary-General of the International Telecommunication Union (ITU) Hamadoun Touré (2007–2014) said that after the cases of Estonia and Georgia we need to avoid a cyber war because it will be worse than a tsunami [12].

National strategies in cyber security and cyber defense

On February 2003 the government of the United States issued *The National Strategy to Secure Cyberspace* where performs an analysis of the threats and vulnerabilities of cyberspace and establishes five joint national priorities: (I) A National Cyberspace Security Response System, (II)

A National Cyberspace Security Threat and Vulnerability Reduction Program, (III) A National Cyberspace Security Awareness and Training Program, (IV) Securing Governments' Cyberspace, (V) National Security and International Cyberspace Security Cooperation [13]. In the United States the concern is permanent, and has been established in various official documents [14–16].

The Russian Federation published the document: *Военная доктрина Российской Федерации (2011)* [17], which translates to “Military doctrine of the Russian Federation”, where in 53 sections this new military doctrine is defined, for the second decade of the 21st century. Aspects of cyber security and defense activities are presented, in sections, 9: C; 41: E and 41: G.

The United Nations Office on Drugs and Crime (UNODC) published in September 2012, *The use of the Internet for terrorist purposes* [18] and presented a detailed report on: (A) Use of the Internet for terrorist purposes; (B) The international context; (C) Policy and legislative frameworks; (D) Investigations and intelligence-gathering; (E) International cooperation; (F) Prosecution; (G) Private sector cooperation.

The European Union (EU) establishes in *Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace* [19], a set of principles that should guide cyber security policies of member countries. The vision of the EU identifies five priority strategies: achieving cyber resilience; drastically reducing cybercrime; developing cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP); develop the industrial and technological resources for cybersecurity and establish a coherent international cyberspace policy for the European Union and promote core EU values. The European Union adopted a new regulatory framework to guarantee privacy and protect the information of European citizens, the protection of natural persons regarding the processing of personal data and the free movement of such data [20] making compliance mandatory, as of May 28, 2018. The EU aims to give back control of their personal data to its citizens, to ensure high protection standards adapted to the digital environment.

The People's Republic of China, in, *China's National Defense in 2008* [21], proposes a strategic framework for modernizing national defense and the armed forces through the automation of China's national defense and armed forces; to use the services of economic development planning in the construction of national defense; and deepening the reform of national defense and the armed forces. China states that national defense is an organic part of social and economic development and this is only possible when the purposes are carried out jointly with the armed forces. Specific goals such as develop by 2020 a complete set of scientific modes of organization, institutions and ways of operation to consolidate the achievements of the society and armed forces [21].

The Israeli government established on August 7, 2011 the Advancing National Cyberspace Capabilities, Resolution No. 3611, where cyber policies are established to be developed by the Jewish state to protect the country's cyber networks and create the National Cyber Bureau NCB, in order to assess and establish cyber policies for the State of Israel [22]. Subsequently on February 15, 2015, adopted the Resolution No. 2443, Advancing National Regulation and Governmental Leadership in Cyber Security, which establishes a unit for cyber security in the government (YAHAV) and a governmental command and control center for cyber threats (SOC) as part of the National CERT, based on its technological and operational infrastructure. Israel has been a key international player in the development of cyber security and cyber defense technologies. Israel believes that the State and its citizens must work together for safety in cyberspace, protecting critical national infrastructure against cyber attacks while encouraging cooperation with universities, industries, the private sector and the bodies or special bodies to become an engine for the development of information technologies [23].

The Democratic People's Republic of North Korea is one of the most enigmatic countries. It has a dynastic political regime, difficult to access, even in the times of Web 2.0, by the technical constraints imposed by the regime, which translates into limited diplomatic contacts and little information. In the Military and Security Developments involving the Democratic People's Republic of North Korea [24] indicates that this country has the world's fourth largest army, more than 1,120,000 formal military soldiers, excluding reserve armies, in a country of 24 million people. This report indicates that North Korea has a military Offensive Cyber Operations (OCO) and is implicated in malicious cyber activity since 2009 and was allegedly responsible of a series of distributed denial of service (DDoS) against government agencies and companies in South Korea, between 2009 and 2011. Additionally, the report notes that in 2013, attacks were made from North Korean territory to banking, media and government networks in South Korea. The Report does not mention any third country involved, but it is understood that China could be, because is a strategic partner of North Korea [24]. Regarding the use of the Internet in North Korea, there are no official statistics. The International Telecommunication Union (ITU) did not report any statistics for North Korea either. Coincidentally South Korea has one of the highest levels of Internet penetration in the world (Percentage of Individuals using the Internet): 92.72 people for every 100 [25].

Russia and China signed a cyber-security deal on Friday May 8, 2015 where they agreed to not conduct cyber-attacks against each other, to exchange information between law enforcement agencies, exchange technologies and ensure security of information infrastructure, and working together in the development of cybernetics technologies. This non-

aggression agreement has as main objective to prevent the internal political and socio-economic environment of these countries from being destabilized and not to interfere with the internal affairs of their states [26].

The Department of Defense of United States of America (2017) in Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2017 [27], indicate that since 2015, China has developed a Strategic Support Force (SSF) and unified space, cyber and electronic warfare capabilities. China is developing a Cyber Command that combines cyber reconnaissance, attack, and defense capabilities, i.e., offensive and defensive cyber capabilities under one military organization. In 2016, USA recognizes cyber activities from China against agencies of its government, including The Department of Defense, focused on accessing networks and extracting information to support China's military modernization. China identifies the cyberspace as a critical domain for national security and assigns substantial resources to maintain a dominant position [27].

IBM reports in Force Threat Intelligence Index 2017 [28], that 2016, is the year of the mega breach with more than 4 billion records leaked, more than the combined total of 2014 and 2015 where the numbers of vulnerability disclosures recorded the highest number: 10,197 vulnerabilities, where the web application vulnerability disclosures made up 22% of the total. The top attack types are: XSS, Physical access, Brute force, Misconfig, Malvertising, Watering hole, Phishing, SQLi, DDoS, Malware, Heartbleed, and Undisclosed. The industries most frequently breached in 2016 were: Information and communications, Government, Media and entertainment, Financial Services and Professional services. IBM indicates that in 2016 are reported more than 54 million security events, 1019 attacks and 93 security incidents, in monitored client environments. But in 2016 is redefined the meaning of the term “mega breach.” which consists of an incident that results in the leakage of massive data with notable publicly disclosed incidents [28].

The White House presented on May 11th, 2017 a new Presidential Executive Order, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [29]. This Executive Order establishes five sections: (1) cybersecurity of federal networks, (2) cybersecurity of critical infrastructure, (3) cybersecurity for the Nation, (4) definitions for the purposes of this order, and (5) general provisions, and includes the commitment and the priorities assumed by the agencies and offices of the US, to maintain a safe and reliable Internet, promoter of economic and technological prosperity.

The Center for Applied Internet Data Analysis (CAIDA), based at the San Diego Supercomputer Center (SDSC) at the University of California San Diego present the study: *Millions of Targets Under Attack: a Macroscopic Character-*

ization of the DoS Ecosystem, in IMC 2017, November 1–3, 2017, London, UK [7], where they found millions of network addresses subjected to denial-of-service attacks over two years, from March 2015 to February 2017, 731 days in total, and concluded that about one-third of the IPv4 address space worldwide was subject to some kind of DoS attacks, primarily through two types of DoS attacks: “Direct” attacks, which involve traffic sent directly to the target from some infrastructure controlled by the attackers and, “Reflection” attacks, during which third-party servers are involuntarily used to reflect attack traffic toward its victim. To detect attacks, the study employed two raw data sources: the Network Telescope of the UCSD with 12.47M events, and the Amplification Honeypot (distributed denial-of-service) with 8.43M events, to a combined of 20.90M DoS attacks, with targeting of 2.19M of /24 IPv4 network blocks, more than one-third of those estimated to be active on the Internet. This study reflects an average of 28.7K attacks per day and 64% of the web sites from .com, .net, .org domains were hosted on IP addresses targeted by attacks. On average, 3% of Web sites were involved daily [7].

Soft Systems Methodology (SSM)

The Soft Systems Methodology (SSM) was developed by Peter Checkland [30–35] at University Lancaster, UK to describe human activity systems and it has been in constant use in research studies in different application domains worldwide. The author indicates that everything that an observer could see as a figure against the background of the rest of the reality could be described as a system. The SSM is established as an organized, flexible process to deal in problematic situations, which call for action to be taken to improve them, and provide ways to make them more acceptable. Is an organized process of thinking your way to taking sensible ‘action to improve’ the situation; and it is a process based on a particular body of ideas, namely system ideas [35]. Checkland states that SSM is an iterative learning cycle, with the participation of different actors and using a permanent use of reflection on systems. The Soft Systems Methodology is composed of seven phases or stages indicated in Fig. 1.

The Soft Systems Methodology SSM is developed in two spaces: the real world and the systems thinking, where the stages: 1, 2, 5, 6 and 7 are developed in the real world; and the phases: 3, 4, 4a and 4b, are systems thinking activities. The stages 1 and 2 are a phase of “expression” during which an attempt is made to build the richest possible image, not the “problem” but the situation in which there is a problem.

The stage 3 specifies some systems that might be relevant to the problem and prepare concise delimitations of what these systems are. The root definition corresponds to an accurately constructed description of a system of human activity that enunciates what the system is.

Fig. 1 Soft Systems Methodology in summary [32]

A well-formulated root definition will make explicit each of the *CATWOE* elements, which is a mnemonic for:

- C:** Customers, the beneficiary or victim of the system's activity
- A:** Actors, the persons who carry out activities in the system
- T:** Transformation process of a human activity system which causes the conversion of input to output
- W:** Weltanschauung, the image or model of the world which makes this particular human activity system a meaningful one to consider
- O:** Owner: the person or persons who could modify or demolish the system
- E:** Environmental constraints. External constraints does this system take as given [28–35].

The stage 4 consists on the creation of conceptual models of the human activity systems defined in the root definitions. Checkland characterizes the conceptual model as, a systemic description of a system of human activity, constructed on the basis of the root definition of the system, in the form of a structured group of verbs. This model should contain the minimum activities necessary for the selected system to be in accordance with the root definition considered. The systems of human activity are described by Checkland as a notional system that expresses some human activity of definite purpose. Are notional in the sense that are intellectual constructs; they are ideal types to be used in a debate about the possible changes that could be introduced in a real-world problem situation.

In the methodological proposals of Checkland, the root definition does state: “what the system is,” while the conceptual model says, “what the system does”. The models of

stage 4 models are then introduced, in stage 5, “in the real world” and are confronted with perceptions of what exists there. The purpose of this “comparison” is to generate a debate with people interested in the problem situation that, in stage 6, will define possible changes that simultaneously satisfy two criteria: that they are desirable and at the same time viable changes. Bergvall-Kåreborn [36], indicates that the SSM is built on the interpretative or hermeneutic paradigm and as a methodology involves many different stakeholders.

The system environment is what is “outside” the system. When we say that something is “outside” of the system, it is interpreted that the system cannot do anything about its characteristics or behavior. The environment integrates things and people that are “constant” or given from the point of view of systems. This corresponds to the data provided to the system and, constitutes its limitations [37].

Systemic study of the cyber security in Venezuela

According to the regulator of telecommunications in Venezuela, CONATEL, in the Q4 2016, the country had 27.600.893 mobile subscribers and 89 active mobile phone lines per 100 habitants. The penetration rate of Internet users is 62 users per 100 habitants [38]. Venezuela is member of the Organization of the Petroleum Exporting Countries OPEC and has the largest oil reserves in the world: 298 billion barrels, representing the 24.7% of the reserves of OPEC [39]. The Venezuelan oil industry is also vulnerable to cyber attacks because it's high interaction with internet operations. Cyber security starts to become a key aspect for today's society. It is the presence of new types of crimes known to the law and doctrine as cybercrime [40–42].

On October 30, 2001, was enacted in Venezuela, the Special Law against Cybercrime [40], to establish a framework of legal protection for systems using information technology, prevention and punishment of crimes against such systems or crimes committed through the use of these technologies. Among them are: security systems using information technology; the property; confidentiality and privacy of electronic communications; the interests of the child or adolescent; the intellectual property; rights and interests of consumers and users; safety compliance and e-commerce transactions; access to knowledge as a form of personal development; access and use of Internet as a priority policy of the Venezuelan State for cultural, economic, social and political development of the Republic [40,41].

Cyber vulnerabilities are present in all countries and Venezuela in its dynamic emerging society and increasing use of information and communication technologies, does not escape this reality. Venezuela has a Computer Emergency Readiness Team (VenCERT) [43]; it is a government agency

for the prevention, detection and management of cybernetic incidents, generated in the information systems of national public administration and public entities. VenCERT reported 2753 incidents in 2014: 1123 incidents with Malware, 396 with Botnet, 388 defacement of Web portals, 77 denial of distributed services DDoS, 29 unauthorized access and 13 disclosure of sensitive information, among others events [44].

Akamai Technologies during the Q3 of 2014, observed attack traffic originating from 201 unique countries/regions. The top 10 countries that originating 82% of observed attacks, by source of IP address are: China 49%, United States 17%, Taiwan 3.8%, India 2.9%, Russia 2.1%, Indonesia 1.9%, Brazil 1.9%, South Korea 1.4%, Turkey 1.3%, Venezuela 1.2%; and Others 18% [44].

PWC presented the *Global Economic Crime Survey (2016)* [42], where presents three types of economic crime most commonly: Asset misappropriation (64%), Cybercrime (32%) and Bribery and corruption (24%). In 2015, the 24% of the organizations suffered some Cybercrime in the past 2 years. The two kinds of cybercrime most commons are, the Cyber fraud and Transfer-of-wealth/IP attacks.

This study indicates that only 37% of organizations have a cyber incident response plan. The five categories of threat vectors are: Nation-states, Insiders, Terrorists, Organized crime syndicates and Hacktivists. With regard to perception of law enforcement agencies, these are not adequately resourced to combat economic Cybercrimes, highlight: United States (52%), France (51%), Venezuela (50%) and India (49%), in positions 12–15, respectively. This report concludes the importance of considering a multi-layered defense.

Officially in Venezuela there are no reports of economic losses caused for cybercrime. It is taboo; no bank or company wants its customers to learn about their vulnerabilities. Either way, Venezuela is no stranger to cybernetic crime around the world. All companies in the country have been victims of some kind of cyber crime. Cyber malicious codes could affect critical infrastructure facilities in the country: electrical, communications, financial, defense, among others. Therefore Venezuela requires urgent measures to introduce an interdisciplinary framework for addressing this emerging reality, as are other countries doing so.

Cyber security is a matter of State and national security, where the establishment of policies with the active participation of Venezuelan society and private entities, enable the implementation of best practices for preservation the security in access and use of the Internet.

Akamai Technologies [45] during the Q2 of 2017 observed that top 10 source countries for web application attacks are: USA (33.8%), China (10.2%), Brazil (8.2%), Netherlands (6.4%), India (3.3%), Ukraine (3.3), Russia (3.1%), France (2.9%), Germany (2.9%) and Canada (2.2%). The Top 10 Target Countries are: USA; United Kingdom, Brazil, Japan,

Singapore, Sweden, Germany, India, China and Netherlands. Therefore, the United States retained the top position for both the source (112 million) and the target (218 million) of web application attacks.

The year 2017 was a time of intense attacks to information security. Hundreds of organizations around the world were infected and harmed by WannaCry and Petya malware. Akamai reports that attacks across cyberspace intensified during this period, with 25% of increase in total web application attacks and 28% increase in total DDoS attacks [43].

Strategic Cyber Security and Cyber Defense Model (SCSCDM) for Venezuela

Human activity system is an intellectual construct, ideal types to use in a debate about possible changes, which might be introduced into a real-world problem situation. The human activity system of this investigation is: *a human activities system where cyber security and cyber defense constitutes an important element in security, defense and integral development of the nation, while projecting the cybernetic ambit as a dimension in the operative environment of the Bolivarian Republic of Venezuela*. The Root Definition is a condensed statement about the system and has to consider the six crucial characteristics, present in a root definition, which represent the initials of the mnemonic CATWOE: Clients; Actors; Transformation; Weltanschauung, Owner, Environment (environmental restrictions). After several reflective iterations, immersed in the “world of systems”, the following six elements or factors grouped under the mnemonic CATWOE are established, which represent the critical particularities that the root definition of the relevant human activities system must contain, where cyber security and defense activities constitute an element of the nation’s security, defense and integral development, projecting the cyberspace as a dimension. The root system definition is established as:

A system that recognizes and applies the Universal Declaration of Human Rights, where natural and juridical persons, national or foreign, public or private, in the geographic space of the Republic, participate and contribute in the continuous processes of cyber security and cyber defense and in the construction of a social and democratic state that propitiate for superior values from its law system, liberty, justice, solidarity, economic welfare, social progress, ethic and political pluralism, promoting the international cooperation with the intention to strengthen the security in the infrastructure of TIC, networks and information and telecommunication systems, while projecting the cybernetic ambit as a dimension in the operative environment of the Bolivarian Republic of Venezuela.

The verbs derived from the root definition are: Recognize Apply, Participate, Contribute, Propitiate, Promote, Strengthen, and Project. The elements of mnemonic CATWOE are:

C: Customers and Actors: A

Natural or juridical persons, public or private, national or foreign, that are or not, in the geographic space of the Republic, who use ICT infrastructure, networks, information systems and telecommunications of the nation.

Inputs transformation: T

Activities performed through ICT infrastructure, networks and information systems and telecommunications by Customers and Actors.

Outputs transformation: T

Activities of Customers and Actors that participate in the ongoing processes of protection and security of information, with sensibility and resilience, in order to strengthen security networks, information systems and telecommunications, projecting the cyber domain as a new dimension in the operating environment of Venezuela.

Weltanschauung: W

Venezuela is a democratic and social state of law and justice, which holds as superior values of its legal system and its performance, life, freedom, justice, equality, solidarity, democracy, social responsibility and in general, the preeminence of human rights, ethics and political pluralism. (As stated by article 2 in the Bolivarian Republic of Venezuela Constitution) [46].

Owner: O

Constitutional Law State characterized by the Venezuelan State and civil society organized.

Environment: E

- Universal Declaration of Human Rights
- Venezuelan Legal System;
- The International Treaties competent in the matter
- International Cooperation;
- Social Determinants present in Venezuelan Society;
- Scientific and Technological developments;
- Activities in Internet through the infrastructures of ICT, networks, information systems and telecommunications of the Nation.

These seven elements represent, at least, the environment with which the formulated system, designed in the world of systems, interacts. These are the environmental restrictions of the system of the human activities system, which are constituted by agents external to the system.

Initial conceptual model

Figure 2 presents the initial conceptual model, which indicates the exchanges with the environment, requirement of any open system. The characterization of open system is fundamental in the study of systems due to the exchange of information flows, materials, energy, among others; between the system and its environment. The activities included in the conceptual model represent the minimum requirements for the operation of the system.

The conceptual model is a product of reflexive activity in the “systems world”, stages 3 and 4 of the Soft Systems Methodology. It is the model that the researcher designs with the information provided by key informants and the deep reflective process that requires the use of the methodology. The language to make the model is based on the verbs that come from the root definition, which in turn is constructed with CATWOE elements, therefore the modeling process, is the necessary, sufficient and coherent articulation of the minimum necessary activities that make possible the process of expected transformation of the system of human activities. The processes are the verb sets that appear explicitly or implicitly in the selected root definition.

Figure 3 shows the sub-systems identified in the system. These are: Universal and inalienable guaranties of rights and fundamental freedoms of citizens; Investigation, prevention, detection and management of cybernetic incidents; Strengthening the economic welfare and social progress based in the development of information and communications technology; A democratic, participative, protagonist and pluralist society; International cooperation; Projection of the cybernetic domain. The interrelationship between the activities made it possible to identify the main subsystems.

Figure 4 shows the Strategic Cyber Security and Cyber Defense Model (SCSCDM) for Venezuela, with the proposed activities and their interrelationships.

Minimum activities contemplated by the Strategic Cyber Security and Cyber Defense Model (SCSCDM) for Venezuela

Recognize and apply

All universal and inalienable citizens’ fundamental rights and freedoms are effectively guaranteed.

Fig. 2 Initial conceptual model

Activities in Internet through the infrastructures of ICT, networks, information systems and telecommunications of the Nation, performed by the citizens and legal persons, of public and private law, national or foreign, present or not, in the geographical space of the Republic, which use lawfully or for criminal purposes, the networks, information systems and telecommunications of the Nation.

Activities in Internet through of the infrastructures of ICT, networks, information systems and telecommunications of the Nation, performed by the citizens and legal persons, of public and private law, national or foreign, present or not, in the geographical space of the Republic, which use lawfully or for criminal purposes, the networks, information systems and telecommunications of the Nation, who participate in the continuous processes of cyber security and cyber defense, with elements of protection and security of information and critical infrastructures, resilience capacity and citizen awareness, in order to strengthen security in networks, information systems and telecommunications, all of which project the cybernetic field as a new dimension in the operational environment of the Bolivarian Republic of Venezuela.

Recognize

1. Comply with the universal guarantees of the inalienable rights of citizens who use the Internet, from the national geographic space.
2. Ensure the universal and effective respect for the fundamental rights and freedoms of citizens.
3. Establish progressive measures, national and international, recognition and universal and effective application of the rights of citizens who use the Internet and telecommunications (Fig. 5).

Apply

4. Make effective use of the principles and actions contained in the Universal Declaration of Human Rights in the national geographic space.
5. Protect intangible assets and citizen values such as freedom, transparency and trust of citizens who use the Internet and telecommunications.

6. Preserve the high interests of children and adolescents in cyberspace.
7. Respect the privacy of the citizens, communications, data and personal information of citizens in cyberspace.
8. Enjoy freedom of expression, belief and conscience in cyberspace with absolute adherence to the fundamental laws and principles of individuals and institutions.
9. Work so that citizens, public and private institutions, both Venezuelan and Foreign, inspire their actions with the spirit of the Universal Declaration of Human Rights.

Participate

In the systems of investigation, prevention, detection and management of cyber incidents (Fig. 6)

10. Understand the threats and challenges of cyber security and defense as opportunities to strengthen research and innovation spaces in the area of Information Technology and Communications in universities, research centers of the nation.

Fig. 3 Subsystems of Strategic Cyber Security and Cyber Defense Model SCSCDM

11. Create research and innovation centers of reference and excellence, in conjunction with Venezuelan universities for the development and strengthening of capacities in computer security.
12. Strengthen the cyber security and response capacities in public-sector agencies and critical national infrastructures.
13. Improve cyber security and responsiveness to cyber incidents in national public sector networks, information systems and telecommunications.
14. Promote awareness of cyber security through training, innovation and the adoption of computer security standards, to share with all sectors of Venezuelan society (Fig. 7).
16. Impulse ICT as economic and social accelerators, for natural and juridical persons from both public and private law of the nation, which make possible the economic prosperity, progress and social welfare.
17. Develop schemes of participation and cooperation among citizens, public and private sectors of the nation that make possible action lines, strategies, and security and cyber defense policies.
18. Stimulate: action and plans for the execution of protection policies and informational security in networks, information and telecommunication systems (Fig. 8).

Propitiate

Strengthening the economic welfare and social progress based in the development of Information and Communications Technologies (ICTs).

15. Implement a state policy to grant massive, inclusive and participative access to ICTs, in all sectors of Venezuelan society.

Contribute

In the construction of democratic, participatory, protagonist and pluralist society.

19. Impulse through education, teaching and citizen participation, the respect, the rights and fundamental freedoms of all citizens, of public and private sector institutions that carry out activities through the Internet and telecommunications.
20. Support a participatory and collaborative environment between society, the private sector and the State.

Fig. 4 Strategic Cyber Security and Cyber Defense Model (SCSCDM) for Venezuela

21. Enhance the legislation on security and cybercrime, without jeopardizing the guaranties, rights and fundamental freedoms of Venezuelan citizens.
22. Prevent and minimize criminal behavior in systems that use information and communication technologies of the nation, or the use of these for any type of crime or illegal acts.
23. Convert security and cyber defense into one of the priorities of the nation's security, defense and integral development policies.

24. Assume international leadership to stimulate Cyber security policies (Fig. 9).

Promote

The international technical and scientific cooperation with other democratic nations

25. Construct a policy of international cooperation in cyber-security and cyber defense, with the support of international organizations and integration agreements in which Venezuela participates.

Fig. 5 Activities derived from the action: *Recognize*, in the SCSCDM model

Fig. 6 Activities derived from the action: *Apply*, in the SCSCDM model

Fig. 7 Activities derived from the action: *Participate*, in the SCSCDM model

Fig. 8 Activities derived from the action: *Propitiate* in the SCSCDM model

26. Advertise an international cyber security and cyber defense policy, consistent with Venezuela's democratic values.
27. Encourage the establishment of a common and specific legislative framework.
28. Impulse the establishment of research centers with regional scope and action, through the integration mechanisms in which the nation participates.
29. Position ourselves as a regional reference in the area of cyber security through political and technological leadership in the international scenarios where the nation (Fig. 10).

Strengthen

Security in the nation's networks, information systems and telecommunications

30. Create a National Cyber Awareness System in the Bolivarian Republic of Venezuela and research centers, strengthening the technical instances currently in operation.
31. Consider cyber security and cyber defense as a matter of State and therefore of security, defense and integral development.

Fig. 9 Activities derived from the action: *Contribute* in the SCSCDM model

Fig. 11 Activities derived from the action: *Strengthen* in the SCSCDM model

Fig. 10 Activities derived from the action: *Promote*, in the SCSCDM model

Fig. 12 Activities derived from the action: *Project* in the SCSCDM model

- 32. Establish a single authority in the area of security and defense, where competences and co-responsibility are transversal between the State and the Venezuelan society
- 33. Reinforce the public entities of the national System of Investigation, Prevention, Detection and Management of Cyber Incidents VenCERT.
- 34. Privilege the activity of the Cyber Incident Management Centers of the Bolivarian Republic of Venezuela (Fig. 11).

Project

The cyberspace as a dimension in the operational environment, of the Bolivarian Republic of Venezuela.

- 35. Consider cyber security and cyber defense as a State issue.
- 36. Motivate cyberspace as a dimension in the operational environment of the Bolivarian Republic of Venezuela (Fig. 12).

The 36 activities that make up the conceptual model are the minimum requirements for the functioning of the systems of human activities that considers cyber security and cyber defense, as an element of the security, defense and integral development of the Nation. This system is the one that derives from the “systems world”; it is the formulated system, product of the interactions with the key informants and in the reflective process of the research, in participant activity, in the “systems world”.

Conclusions

This work provides the academic community two components: a Strategic Cyber Security and Cyber Defense Model (SCSCDM), and the projection of cyber ambit as a new dimension in the operating environment of the Nation. The system was designed as a human activities system where cyber security and cyber defense constitute an element of security, defense and integral development of the nation. In the methodological proposals of Checkland, the root definition does state: “what the system is,” while the conceptual model says, “what the system does”. It was designed with the set of verbs and constitutes the activities that represent the minimum requirements for system operation. The verbs derived from the root definition, are: Recognize, Apply, Participate, Contribute, Propitiate, Promote, Consolidate, Project.

Cyber incidents have evolved, for citizens, public and private institutions and to the States; from the perspective of data protection, to an approach of risks and threats. That is why cyber securitization should be permanent, because the threats are permanent.

The information and communication technologies hold a frenzied dynamic in its development and operation, requiring human, technical and financial resources to respond the complexity of the actions of citizens and institutions. The security theories and international relations are attentive to incorporate transcendent threats and risks in security schemes; the expansive theories have to take cyber security into consideration by the enormous implications that flow from it. In the daily activity of citizens, businesses and States, the use of cybernetics is fundamental.

The intensive use of the ICTs will improve business and government processes, as well as citizens’ quality of life.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. BBC News (2007) Estonia hit by ‘Moscow cyber war’. May 17, 2007. <http://news.bbc.co.uk/2/hi/europe/6665145.stm>. Accessed 5 Jan 2010
2. Arun N (2008) Caucasus foes fight cyber war. In: BBC News. Aug 14, 2008. <http://news.bbc.co.uk/2/hi/europe/7559850.stm>. Accessed 5 Jan 2010
3. Lesk M (2007) The new front line: Estonia under cyberassault. *IEEE Secur Priv* 5(4):76–79. <https://doi.org/10.1109/MSP.2007.98>
4. Guadamuz A (2010) Networks, complexity and Internet regulation. Scale-free law. University of Edinburgh, Edward Elgar EE Publishing, Northampton
5. Clarke R, Knake R (2010) Cyber war—the next threat to national security and what to do about it. HarperCollins, London
6. The NATO Cooperative Cyber Defence Centre of Excellence. <https://ccdcoc.org/index.html>. Accessed 18 Dec 2013
7. Jonker M, King A, Kruppet J, Rossow C, Sperotto A, Dainotti A. Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. <https://conferences.sigcomm.org/imc/2017/papers/imc17-103.pdf>. Accessed 01 Dec 2017
8. Symantec (2011) W32.Stuxnet Dossier. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Accessed 01 Dec 2017. Accessed 15 Mar 2013
9. Sanger D (2012) Obama order sped up wave of cyberattacks against Iran. The New York Times. Jun 1, 2012. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>. Accessed 15 Jun 2012
10. Riley M (2012) Code in aramco cyber attack indicates lone perpetrator. Oct 25, 2012. <http://www.bloomberg.com/news/articles/2012-10-25/code-in-aramco-cyber-attack-indicates-lone-perpetrator>. Accessed 28 Oct 2012
11. Sanger D, Shanker T (2013) Broad powers seen for Obama in cyberstrikes. The New York Times. Feb 3, 2013. <http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html>. Accessed 8 Feb 2013
12. Meyer D (2010) ITU head: cyberwar could be ‘worse than tsunami’. Sep 3, 2010. <http://www.zdnet.com/article/itu-head-cyberwar-could-be-worse-than-tsunami>. Accessed 30 Sept 2010
13. The White House United States of America (2003) The national strategy to secure cyberspace. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. Accessed 20 Jun 2010
14. The White House United States of America (2009) Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf. Accessed 24 Jun 2010
15. The White House United States of America (2011) Trustworthy cyberspace: strategic plan for the federal cybersecurity research and development program. https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf. Accessed 10 Jan 2012
16. Department of Defense United States of America (2012) Sustaining US global leadership: priorities for 21st century defense (2012). http://www.defense.gov/news/Defense_Strategic_Guidance.pdf. Accessed 15 Feb 2012
17. Президент России (2011) Военная доктрина Российской Федерации. http://news.kremlin.ru/ref_notes/461 (in Russian). Accessed 4 Jan 2012
18. The United Nations Office on Drugs and Crime UNODC (2012) The house of the Internet for terrorist purposes. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. Accessed 3 Jan 2013
19. The European Commission (2013) Cybersecurity strategy of the European Union: an open, safe and secure cyberspace. http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf. Accessed 25 Feb 2013
20. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Accessed 15 Nov 2017
21. Office of the State Council of the People’s Republic of China (2009) China’s National Defense in 2008. <http://www.mcsstw.org/>

- download/2008DefenseWhitePaper_Jan2009.pdf. Accessed 15 Jan 2014
22. Israel Prime Minister's Office (2011) Advancing national cyberspace capabilities. <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf>. Accessed 10 Dec 2013
 23. The Government Secretary. Resolution: advancing national regulation and governmental leadership in cyber security. Government Resolution No. 2443 of February 15, 2015. <https://ccdcoc.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf>. Accessed 1 Nov 2017
 24. Military and Security Developments Involving the Democratic People's Republic of Korea 2013 (2014). http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf. Accessed 15 Jan 2014
 25. International Telecommunication Union (ITU) ICT Statistic. Percentage of individuals using the Internet. https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2017/Individuals_Internet_2000-2016.xls. Accessed 10 Dec 2017
 26. Razumovskaya O. Russia and China pledge not to hack each other. <https://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/>. Accessed 18 Mar 2016
 27. Office of the Secretary of Defense. Annual report to Congress. Military and security developments involving the People's Republic of China 2017. https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770. Accessed 20 Nov 2017
 28. IBM X-Force Threat Intelligence Index 2017. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&>. Accessed 25 Nov 2017
 29. The White House. Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure. May 11, 2017. <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>. Accessed 18 Jun 2017
 30. Checkland PB (1981) Systems thinking, systems practice. Wiley, Chichester
 31. Checkland P (1985) From optimizing to learning: a development of systems thinking for the 1990s. *J Oper Res Soc* 36(9):757–767
 32. Checkland P, Scholes J (1990) Soft systems methodology in action. Wiley, Chichester
 33. Checkland P (1994) La metodología de sistemas suaves en acción. In: Megabyte Editors (**in Spanish**)
 34. Checkland P (2000) Soft systems methodology: a thirty year retrospective. *Syst Res Behav Sci* 17:11–58
 35. Checkland P, Poulter J (2006) Learning for action: a short definitive account of soft systems methodology, and its use practitioners, teachers and students. Wiley, Chichester
 36. Bergvall-Kåreborn B, Mirijamdotter A, Basden A (2004) Basic principles of SSM modeling: an examination of CATWOE. From a soft perspective. *Syst Pract Action Res* 17(2):55–73. <https://doi.org/10.1023/B:SPAA.0000018903.18767.18>
 37. Churchman CW (1979) El Enfoque de Sistemas. FCE (**in Spanish**)
 38. Comisión Nacional de Telecomunicaciones. Resumen del Sector Telecomunicaciones 2016. <http://www.conatel.gob.ve/resumen-del-sector-telecomunicaciones-2015/> (**in Spanish**). Accessed 18 Oct 2017
 39. Organization of the Petroleum Exporting Countries (2015). http://www.opec.org/opec_web/en/data_graphs/330.htm. Accessed 19 Jan 2015
 40. Ley Especial contra Delitos Informáticos (2001) Gaceta Oficial República Bolivariana de Venezuela N° 37.313. http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf (**in Spanish**)
 41. Torres D (2012) Cybercrime in the Bolivarian Republic of Venezuela: a systemic perspective. In: Proceedings of EMCSR 2012, book of abstracts European meeting on cybernetics and systems research (EMCSR), pp 178–181. http://www.emcsr.net/wp-content/uploads/2012/Book_of_Abstracts_EMCSR_2012.pdf. Accessed 17 Dec 2012
 42. PWC Global Economic Crime Survey 2016. <http://www.pwc.com/crimesurvey>. Accessed 18 Oct 2017
 43. VenCERT. Venezuela Computer Emergency Readiness Team. Accessed 02 Dec 2017. http://www.suscerte.gob.ve/?page_id=1736. Accessed 30 Jan 2015
 44. Akamai Technologies (2015) Akamai's state of the Internet Q3 2014 report. <https://www.akamai.com/us/en/multimedia/documents/content/akamai-state-of-the-internet-report-q3-2014.pdf>. Accessed 28 Dec 2015
 45. Akamai Technologies (2017) State of the internet/security Q2 2017 report. <https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp>. Accessed 02 Dec 2017
 46. Constitución de la República Bolivariana de Venezuela (2009) Gaceta Oficial República Bolivariana de Venezuela N° 5908 Extraordinario. Febrero 19 (**in Spanish**). <http://www.ministeriopublico.gob.ve/LEYES/constitucion/constitucion1.html>. Accessed 01 Mar 2009

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.