PROFESSIONAL ARTICLE DOI 10.52781/cmm.e007

The management of internally displaced persons and enhanced human security in North East Nigeria

La gestión de personas desplazadas internamente y el fortalecimiento de la seguridad humana en el Nordeste de Nigeria

Jibril Aliyu Haruna Baba
Nigerian Army.
Abuja,Nigeria.
ahbjibril@gmail.com

Abstract: Human security entails protecting people from severe and pervasive threats in ways that enhance their survival, livelihood and dignity. It broadens the understanding of security from territorial security to the security of people, particularly vulnerable groups such as IDPs who suffer emotional problems such as human right abuses, assault and loss of livelihood among others. These problems have raised the need for attention to the efficient management of IDPs for the enhancement of human security in NE Nigeria. This research therefore unravelled the strategies to mitigate the challenges against effective management of IDPs for enhanced human security in NE Nigeria. The main objective of this research is to appraise the management of IDPs for enhanced human security in NE Nigeria. Questionnaires which were administered to respondents were analysed using Statistical Package for Social Science (SPSS) AAEA.

Keywords: Nigeria. Human security. Internally displaced persons.

Resumen: La seguridad humana implica proteger a las personas de amenazas graves y generalizadas a fin de fortalecer su supervivencia, sus medios de vida y su dignidad. La comprensión de la seguridad se amplía de la seguridad territorial a la seguridad de las personas, en particular los grupos vulnerables como los desplazados Internos, que sufren problemas emocionales como violaciones de los derechos humanos, agresiones y pérdida de medios de vida, entre otros. Estos problemas han planteado la necesidad de prestar atención a la gestión eficiente de las PDIs para mejorar la seguridad humana en el noreste de Nigeria. Por lo tanto, esta investigación desentrañó estrategias para mitigar los desafíos contra la gestión efectiva de las PDIs para fortalecer la seguridad humana en el noreste de Nigeria. El objetivo principal de esta investigación es evaluar la gestión de las PDIs para fortalecer la seguridad humana en el noreste de Nigeria. Los cuestionarios que se administraron a los encuestados se analizaron utilizando el Paquete Estadístico para Ciencias Sociales (SPSS) AAEA.

Palabras-clave: Nigeria. Seguridad humana. Personas desplazadas internas.

Received: Apr. 5, 2020
Accepted: Jul. 27, 2020

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introduction

The Twenty First Century global community is confronted with contemporary threats including political upheavals, armed conflicts, trans-national organised crime and terrorism. Many of these threats have had adverse implications on the security and well--being of people. They have, unilaterally or in combination, engendered huge humanitarian crisis such as death, hunger, poverty and mass displacement of people. The forced migration of people from their homes has often resulted in the problem of refugees and Internally Displaced Persons (IDPs).

An IDP connotes any person that has been compelled to leave his or her place of abode, due to real or imagined threats, to another location within a country's border. The IDPs are distinct from refugees, who are people that have fled across an internationally recognized border to escape war, persecution or natural disaster (RUSSELL, 2016). According to a UNDP 1994 report, IDPs are exposed to threats such as disease, hunger, unemployment, crime, abuse, social conflict and political repression, especially when not well managed. In addressing these threats, the establishment of a robust mechanism for the management of IDPs becomes imperative. The management of IDPs is primarily a national government responsibility. It involves the utilization of available resources to address the problems inhibiting the safety, security and well-being of IDPs, hence human security.

Globally, the number of IDPs has been on a steady rise from 6.6 million in 2005 to over 40.8 million by December 2015, according to the 2016 Global Report on Internal Displacement (GRID). Bagshaw and Paul (2004), argue that the management of IDPs has therefore, increasingly become one of the most daunting challenges in recent times. In Pakistan, since 2004, conflict induced IDPs have resulted from fighting between the Pakistani Military and Non-State Armed Groups (NSAGs) such as al-Qaeda with adverse effects on human security. The IDPs have also resulted from sectarian violence and tribal clashes over resources. Specifically, conflict in the Khyber Pakhtunkhwa (KP) Province and Federally Administered Tribal Areas (FATA) resulted in 1,292,406 IDPs including 17,578 living in camps (UNHCR, 2016). These IDPs were faced with several problems including disease, loss of access to livelihood and other security threats that impinged on human security in Pakistan. Africa is home to over 13 million IDPs arising from disasters such as conflicts and complex emergencies, representing about one third of the global figure, according to the Norwegian Refugee Council (NRC). In the Democratic Republic of Congo (DRC), communities have over the years been exposed to waves of violence resulting in about 2.9 million IDPs with negative impacts on human security (STACEY, 2014). Due to the huge number of displaced persons and fragile nature of the national institutions, the management of IDPs has been taken up by the UN and other international organisations in DRC. These include the OCHA, UN High Commission for Refugees

(UNHCR), United States Agency for International Development (USAID) and International Organisation for Migration (IOM), amongst others.

In 2014 and 2015, about $633,660,856 was expended by the international community on the management of IDPs in the DRC (INTERNAL DISPLACEMENT MONITORING CENTRE, 2016). These supports spanning across areas such as food, health, education and shelter were delivered through UN agencies, International Committee of the Red Cross (ICRC) and partner Non-Governmental Organisations (NGOs) such as Oxfam. According to the UN, several of these efforts are steadily yielding results with over 74,000 people from 20 villages in Katanga returning home between 2012 and 2014. The efforts of the Government at addressing the insecurity and management of the IDPs, in collaboration with her partners, have therefore enhanced human security in the DRC.

In Nigeria, armed attacks perpetrated by Boko Haram Terrorists (BHT) in the North East (NE) states of Adamawa, Bauchi, Borno, Gombe, Taraba and Yobe have led to over 1,856,616 IDPs as of April 2016 (INTERNATIONAL ORGANIZATION FOR MIGRATION, 2016). The IDPs spreading across the NE and North Central (NC) zones of Nigeria as well as the Federal Capital Territory (FCT) account for about 86.16 per cent of IDPs in the country, according to IOM. However, majority of these IDPs are located in Borno with 1,427,999 representing 76.9 per cent, followed by Yobe with 150,718 representing 8.1 per cent and Adamawa with 134,415 representing 9.4 per cent of the total figure. These IDPs suffer emotional problems associated with memory of fearful events, loss of livelihood, frustration, assault and human rights abuse, amongst others. The activities of BHT have also festered social vices such as crime, assassination and sexual abuse against the IDPs, particularly the children, which represent

53.72 per cent of the IDP population (OLUKOLAJO; OGUNGBENRO, 2017). These problems have raised the need for attention to the efficient management of IDPs for the enhancement of human security in NE Nigeria.

The Federal Government of Nigeria (FGN) has been constrained in effectively managing the IDPs for enhanced human security in NE Nigeria. For instance, due to the absence of a clear and specific national policy on IDPs, the National Emergency Management Agency (NEMA) has remained the de-facto lead government agency (LADAN, 2016). However, IDPs have unique needs such as protection of their rights, which an emergency management agency such as NEMA cannot effectively provide. This has thus hampered the FGN's ability to provide a comprehensive support package that addresses the wide-ranging issues confronting IDPs in the NE. The purpose of this study, therefore, is to appraise the management of IDPs in the NE Nigeria in order to address pertinent issues impeding human security in the region. Thus, the main objective of this study is to appraise the management of IDPs for enhanced human security in NE Nigeria. Furthermore, the Alternate Hypothesis was used in the research to establish a significant relationship between management of IDPs and human security. The study was additionally elaborated by time, space and content.

The methodology of the study covers the type of research, sources of data, methods of data collection, sampling technique, sample population, method of data analysis and method of

data presentation. The field survey method was adopted to enable the researcher obtain views on the subject matter as well as examine responses from informed perspectives on the topic. Data for the research was obtained from primary sources such as questionnaires and unstructured interviews. Secondary sources such as books, conference reports, official publications, newspapers and magazines were also exploited. A combination of field method and document analysis were used for data collection, while the purposive non-probabilistic sampling method was used to select respondents in line with the objectives of the study. The data collected from the primary and secondary sources were analysed using the qualitative and quantitative methods of data analysis. The data obtained were presented in a descriptive and analytic form using tables, charts and graphs.

2 Literature review

The chapter presents a review of some relevant literature and provides a theoretical framework to guide the study. It also highlights examples of management of IDPs and human security from other countries in order to draw lessons. The 2 key variables in this study are management of IDPs as the independent variable and human security as the dependent variable.

Review of existing literature

Several studies have been conducted over the years on the management of IDPs and human security. However, most of these studies vary in approach, content, theories and methodology. The literature are reviewed with a view to identifying the gaps the study seeks to fill.

Adesote and Peters (2015) in their study, provided a historical comparative analysis of IDPs arising from conflict situations in Nigeria including those in NE Nigeria. Their work was descriptive in nature and interrogated the human security impacts of various cases of violence on IDPs. It also noted and proffered some options for government in addressing the myriad of challenges militating against the management of IDPs.

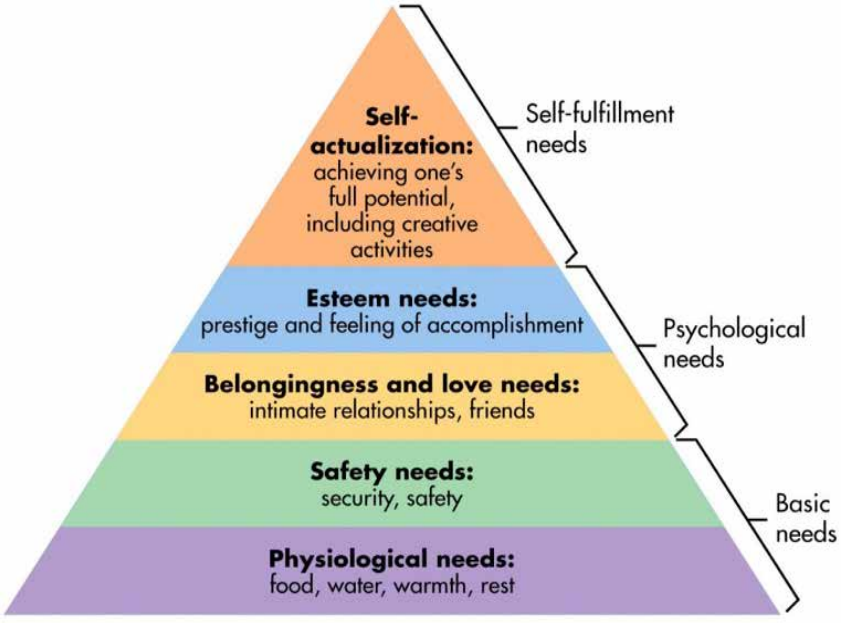
Daodu (2010) examined how the US and Nigeria have responded and managed IDPs. The main assertion of the study is that there is no difference between the handling of IDPs in the US and Nigeria. This was in spite of the inability of the emergency agencies to meet the peculiar needs of IDPs in both countries. Cohen and Deng (1998) conducted case studies of some countries in Africa, Eastern Europe and Latin America that have suffered severe problems of internal displacement. The result of their studies showed striking similarities in the challenges confronting the management of IDPs in these countries as well as the broader implications for national security.

All the reviewed works have made significant contributions to this field of study, by providing insights on the region-specific dynamics in IDPs management as well as their underlying issues. However, majority of the literature addressed the management of IDPs from a broader national security perspective, as against human security which is a component thereof. This leaves a knowledge gap on the effects of the managements of IDPs on human security. It is this gap that this study seeks to address by appraising the management of IDPs for enhanced human security in NE Nigeria.

Theoretical frame work

The theory considered most suitable for this study is the Hierarchy of Needs Theory (HNT), which seeks to explain the hierarchical nature of human needs as well as their interrelationship. The pioneer proponent of this theory was Abraham Maslow, who posited that "human needs are organised into a hierarchy of relative pre-potency (HOPPER, 2019). This hierarchy ranges from more concrete needs such as food and water, to more abstract concepts such as self- fulfilment. Maslow further stated that human beings were motivated by 5 categories of needs; physiological, safety, love, esteem and self-actualisation. Graph 1 below depicts Maslow's Hierarchy of Needs Theory.

Graph 1 – Maslow's Hierarchy of Needs Theory



Source: McLeod, 2018.

HNT is considered relevant to this study as it provides a basis for understanding the most essential needs of IDPs and how these could affect their management for enhanced human security in Nigeria.

Examples of management of internally displaced persons and human security from other countries

Examples of the management of IDPs and human security from Colombia and Uganda were examined in order to draw lessons from the study. These countries were selected because they have experienced the impact of the management of IDPs arising from armed conflict on human security with similarities to the situation in NE Nigeria.

Management of internally displaced persons and human security in Colombia

Colombia has been involved in a civil war for over 50 years between the government forces and insurgent forces such as the Fuerzas Armadas Revolucionarias de Colombia (FARC). These crises as well as operations against drug cartels have resulted to a large IDP population estimated at 6 million as at December 2014, representing about a tenth of the country's population, according to OXFAM (2012). Louise noted that several women and children were exposed to sexual exploitation, violence and malnutrition while majority of the children engaged as child workers reached about 1.1 million in 2014. The displacements resulted in loss of abode, loss of means of livelihood and impacted negatively on the well-being of the people. The Colombian Government however, made some efforts to address the challenges facing the IDPs. According to the US Commerce Department Bureau of Economic Analysis 2014 Report, the Colombian Government utilised resources from the growing economy, with an average GDP growth of 4.3 per cent per annum, to improve its support to IDPs. The Government also established a single registry for IDPs, which provided centralised information on the displacement dynamics for the judicious appropriation of funds and resources. These efforts of the Colombian Government at effectively managing the IDPs have thus gone a long way in enhancing human security in the country.

Management of internally displaced persons and human security in Uganda

In Uganda, the insurgent activities of the Lord's Resistance Army (LRA) resulted in over 1.5 million IDPs in 1998 (NORWEGIAN REFUGEE COUNCIL, 2012). At the peak of the crisis in 2005, there were about 1.84 million IDPs living in 242 camps across 11 districts in Northern Uganda. Several local and international actors were involved in the management of the IDPs including the World Food Programme (WFP), which provided food. Others include

the UNHCR, which took up the protection role and the World Health Organisation (WHO) that provided health services. The UN Children Emergency Fund (UNICEF) focussed on children along with other UN agencies and NGOs that also took up diverse roles under the coordination umbrella of the national authorities.

As at 2005, a total of 539,550 IDPs had returned to their homes while an additional 381,000 moved to new sites closer to their homes by June 2007 (GOMEZ; GASPER, 2016). In October 2007, Uganda launched the Peace, Recovery and Development Plan (PRDP) for Northern Uganda as a 3-year framework to enable development and restore law and order in affected areas. The PRDP with a budget of $600 million was built on 4 strategic objectives namely; consolidation of state authority, empowering communities, revitalising the economy and peace building and reconciliation. Due to the commitment of the government, the initiative received the support of other organisations. It facilitated the return of several IDPs resulting in the decrease of the IDP population to about 30,000 by December 2011. The PRDP, thus, improved the management of IDPs and enhanced human security in Uganda.

Lessons learnt from Colombia and Uganda

The lessons learnt from Colombia and Uganda's management of IDPs and human security includes political will and importance of policy framework.

Political Will. Political will and commitment to the plight of IDPs is a lesson drawn from the examples studied. The governments in Colombia and Uganda displayed strong commitment in taking lead roles in the management of IDPs in their countries. They set in place appropriate mechanisms, which facilitated the involvement of a wide array of actors to achieve sustainable results. The need for political will that unencumbers bureaucratic and administrative bottlenecks is therefore crucial.

Importance of Policy Framework. The importance of appropriate policy frameworks for the management of IDPs was underscored in Colombia and Uganda. The Victims Law in Colombia and National Policy on Internally Displaced Persons (NPI) in Uganda provided a useful platform for delineation of roles amongst stakeholders. These policies were further backed by relevant legislation that guaranteed the rights of IDPs, through damages and restitution, enabling stakeholders hold government to account. The policy framework, backed by legislation, thus spurred the commitment of government agencies involved in the management of IDPs and enhanced human security in these countries.

3 Presentation of research data

In this section, research data generated from the questionnaires and those obtained from relevant institutions are presented. Out of the 384 respondents, 330 were IDPs while 54 were humanitarian workers. It is pertinent to note that some of the questions were directed at the humanitarian workers only, based on the technical nature of the questions.

The issues associated with the management of IDPs and human security in NE Nigeria would be discussed. The analyses of collected data are also embedded in subsequent sections of this Chapter.

Issues associated with the management of internally displaced persons and human security in north east Nigeria

The issues associated with the management of IDPs and human security in NE Nigeria include policy framework, institutional capacity and coordination of assistance and support services. Others are Internal Displacement Data Management (IDDM) as well as the Return, Resettlement and Reintegration (RRR) programme. These are subsequently discussed within the context of the HNT.

Policy framework

Policy framework entails the plan of action, backed by appropriate legislation that forms the basis of making rules and guidelines that align the priorities of institutions in a state with overall national goals. In 2012, the FGN revised the draft NPI in line with the African Union Convention for the Protection and Assistance of Internally Displaced Persons (ACPAI) to serve as a normative framework for preventing internal displacement and assisting IDPs across the country, including the NE. The revised NPI outlines the obligations of government, humanitarian actors and even host communities with respect to IDPs as well as implementation strategies for the management of IDPs towards enhanced human security. In line with its mandate, NEMA's efforts have thus been focussed on providing immediate basic needs of IDPs. This has resulted in limited attention to the medium and long term needs of IDPs, such as their rights and dignity.

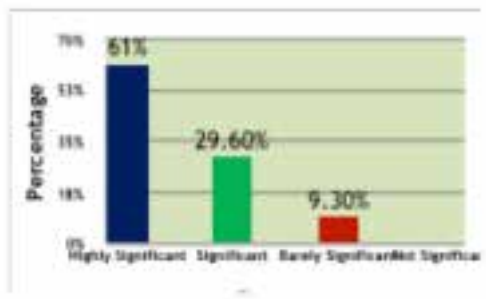
This opinion was supported by responses from humanitarian workers in the field survey undertaken in this research, as depicted in Table 1 and Graph 2, on the influence of a NPI on the management of IDPs in NE Nigeria.

Table 1 – What is the Influence of Policy Framework Framework on the Management of IDPs in the NE?

Serial	Respondent	Response	Percentage
(a)	(b)	(c)	(d)
1.	Highly Significant	33	**61.1%**
2.	Significant	16	**29.6%**
3.	Barely Significant	**5**	9.3%
4.	Not Significant	**0**	**0**
	Total	54	100

Source: Researcher's Analysis, 2019.

Graph 2 – What is the Influence of Policy on the Management of IDPs in the NE?



Source: Researcher's Analysis, 2019.

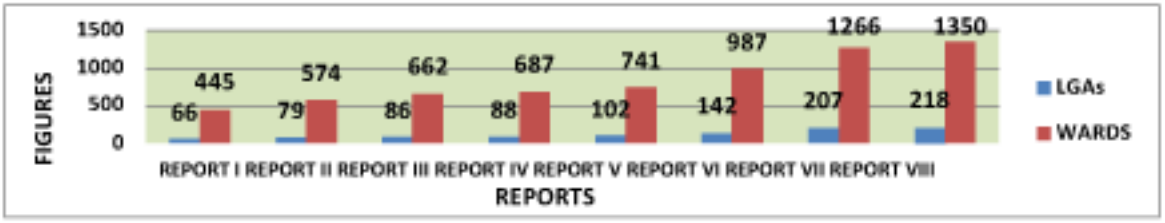
In the survey, 33 of the respondents representing 61.1 per cent, opined that a NPI is highly significant to the effective management of IDPs in the NE. Also, 16 respondents representing 29.6 per cent felt it was significant and 9.3 per cent believed it was barely significant.

Interestingly, no respondent felt that a NPI was not significant, underlining the importance of policy framework to the management of IDPs in the NE.

Internal displacement data management

The IDDM entails the systematic collection of data through assessments, documentation and registration to determine the size and characteristics of displaced populations. It facilitates access to basic rights, family reunification and helps to identify persons in need of special assistance. Several agencies including NEMA, in collaboration with International Office for Migration (IOM), SEMAs and other organisations are currently involved in IDDM in NE Nigeria. The NEMA/IOM Displacement Tracking Matrix (DTM) assessments provide the major source of information on IDPs in Nigeria. It is conducted through interviews with household heads as well as detailed surveys and registration, including biometric capture with particular focus on IDPs in camps[1]. The wide range of baseline information collected, at ward level, covers displacement history, access to basic needs, return intention and assistance received (INTERNATIONAL ORGANIZATION FOR MIGRATION, 2016a). As at February 2016, eight rounds of DTM assessments had been conducted with increasing coverage and information on the displacement situation in NE Nigeria as shown in Graph 3.

Graph 3 – Coverage of Displacement Tracking Matrix Report I – VII



Source: International Organization for Migration, 2016.

The Round I Report covered only 66 LGAs and 445 wards while the Round VIII Report covered 218 LGAs and 1,350 wards translating to an increased coverage of over 200 per cent.

1 NEMA, SEMA and IOM commence Registration and Biometric capture of IDPs in Borno State. Available at: http://nema.gov.ng/nema-sema-and-iom-commence-registration-and-biometric-capture-of-idps-in-borno- state/. Access on: Apr 28, 2016.

Return resettlement and reintegration programme

The RRR programme covers the support provided to IDPs to facilitate their safe return to their abodes or resettlement in new homes and reintegration into communities. Article 11 of ACPAI and Principle 28 of UNGPI require state parties to develop durable frameworks that ensure returns are voluntary with due attention to human security (UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, 2004, p. 14). It also advocates the full participation of IDPs in the planning and management of RRR.

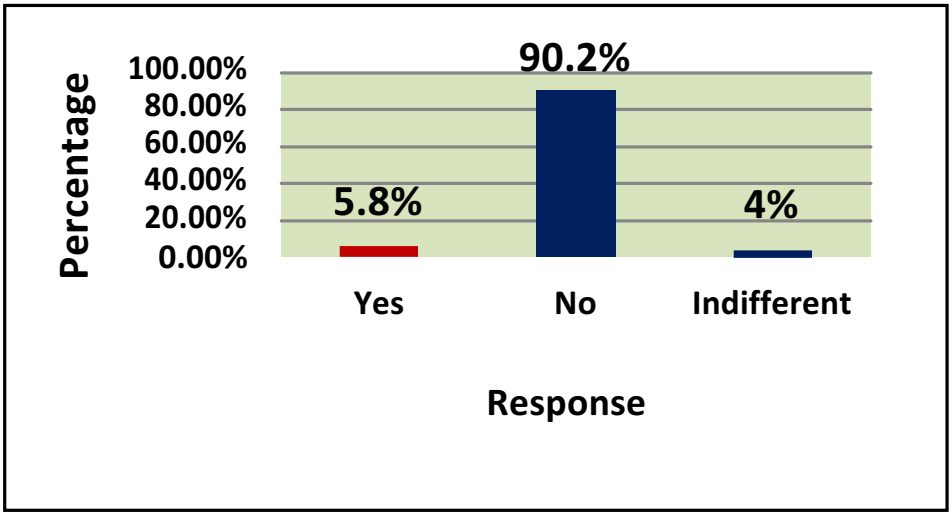
The 2-year Emergency Assistance and Economic Stabilisation Plan (EAESP) was developed under the Presidential Initiative for the North East (PINE) in 2014. It was designed to facilitate RRR of IDPs in the NE through the employment of 150,000 youths in reconstruction activities (PINE Report, 2014). In July 2015, the FGN also released a Resettlement and Reintegration Plan (RRP) for victims of insurgency in the NE. The RRP was developed to, inter alia, address the immediate needs of the returning IDPs. The results of the field survey on the familiarity of IDPs and humanitarian actors with the FGN's RRR programmes are at Table 2 and Graph 3.5.

Table 2 – Are you familiar with the FGN's RRR programme for IDPs in the NE?

Serial	Response	Respondent	Percentage
(a)	(b	(c)	(d)
1.	Yes	31	5.8%
2.	No	362	90.2%
3.	Indifferent	17	4%
	Total	384	100

Source: Researcher's Analysis, 2016.

Graph 4 – Are you familiar with the FGN's RRR programme for IDPs in the NE?



Source: Researcher's Analysis, 2016.

Summary of research findings

This research set out to carry out an appraisal of the management of IDPs and its effects on human security in NE Nigeria. Based on the aforementioned, the following findings were made:

a) Policy framework, institutional capacity, coordination of assistance and support services, IDDM as well as RRR are issues associated with the management IDPs and human security in NE Nigeria.
b) There is too much emphasis on the emergency relief phase covering basic needs such as food and shelter with less attention to medium and long term issues facing IDPs in the NE.
c) The current adhoc registration and documentation process does not facilitate a comprehensive approach to the management of IDPs thus impinging on human security in NE Nigeria.
d) The management of IDPs in the NE has reduced access to education, led to food insecurity as well as compromised public health and communal relationships thereby impinging on human security in NE Nigeria.

e) The effects of the management of IDPs on human security in the NE is also established by the results from SPSS as summarized in Table 3. This confirms the relationship set in place in the conceptual discourse.

Table 3 – Effects of the Management of IDPs on Human Security in NE Nigeria

Série	Management of IDPs (Independent Variable)	Attributes of Human Security (Dependent Variable)	Relationship to Human Security (Dependent Variable)
(a)	(b)	(c)	(d)
1.	Access to Education	Economic	Significant Negative Effect
2.	Food Security	Food	Significant Negative Effect
3.	Public Health	Health	Significant Negative Effect
4.	Inter-Communal Relationship	Community	Negative Effect

Source: Researcher's Analysis, 2016.

These findings lend credence to the HNT propounded by Maslow. It underlines the primacy of human needs from the basic to the abstract, and how these could affect the efforts at managing IDPs to enhance human security.

Challenges militating against the effective management of internally displaced persons for enhanced human security in north east Nigeria

The challenges militating against the effective management of IDPs for enhanced human security in the NE include non-adoption of the NPI inadequate budgetary allocation and inter- agency rivalry. Others include absence of centralised database for IDPs as well as failure to adopt durable solutions for RRR. These challenges are discussed subsequently.

Non-adoption of draft national policy on internally displaced persons

The non-adoption of the draft NPI has hampered the effective management of IDPs for enhanced human security in NE Nigeria. It has prevented the employment of holistic strategies in the management of IDPs in NE Nigeria as outlined in the extracts of the draft NPI. The current approach has inadvertently concentrated government's efforts on basic physiological needs. This has led to support gaps in specialised areas such as means of livelihood, cultural identity, compensation, personal dignity and psychosocial care as captured in Maslow's Hierarchy of Needs in Graph 5.

Graph 5 – Maslow's Hierarchy of Needs

Source: Kasali, 2015.

According to Kasali, the higher needs of safety, belonging, self-esteem and self-actualisation are gaps arising from the current approach adopted in the management of IDPs in the NE. The non-adoption of the NPI has thus resulted in support gaps in specialised areas that impinge on human security in NE Nigeria.

Inadequate budgetary allocation

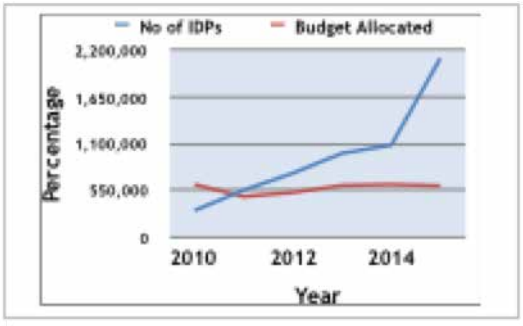
Inadequate budgetary allocation to statutory agencies involved in the management of IDPs has inhibited their institutional capacity to effectively manage IDPs in the NE. The annual budget allocation to the National Commission for Refugees, Migrants and Internally Displaced Persons (NCFRMI) declined from 616 million naira in 2010 to 600 million naira in 2015. This was in spite of a converse increase in the number of IDPs in the NE from 307,000 to 2,100,000 within same period as highlighted in Table 4 and Graph 6.

Table 4 – Budget of NCFRMI 2011-2015

Serial	Year	Number of IDPs	(Million Naira)
1.	2010	307,000	616,090
2.	2011	550,000	473,956
3.	2012	750,000	521,333
4.	2013	982,000	604,965
5.	2014	1,080,000	616,093
6.	2015	2,100,000	600,000

Source: NCFRMI, NEMA, CBN, 2016.

Graph 6 – Budget of NCFRMI 2011-2015



Source: NCFRMI, NEMA, CBN, 2016.

Graph 6 reveals a net decrease in allocations to NCFRMI, despite the huge increase of over 584 per cent in the number of IDPs in the NE from 2010 to 2015.

Absence of centralised database for internally displaced persons

The absence of a centralised database on IDPs has made it difficult to obtain credible information on IDPs. A centralised and comprehensive database with aggregated displacement data such as age, gender and location that would facilitate attention to peculiar needs of IDP groups is unavailable. This has made it difficult to specifically target, plan and implement gender related programmes to address the needs of women, estimated to constitute 53 per cent of IDP population (DTM Report).

The absence of a centralised database has also prevented the exchange of information among stakeholders resulting in duplication of efforts with adverse effects on the humanitarian response in the NE. Specifically, Nafuta noted that the failure of Yobe State Emergency

Management Agency (SEMA) to share its database on IDPs enabled 192 IDPs in YBC settlement to simultaneously collect cash transfers from WFP and ICRC.

6 Strategies to mitigate the challenges in the management of internally displaced persons for enhanced human security in north east Nigeria

Some strategies are proposed in this study to mitigate the challenges of the management of IDPs for enhanced human security in NE Nigeria. These include review and adoption of the draft NPI, establishment of a National Humanitarian Intervention Fund (NHIF) and harmonisation of provisions in NEMA and NCFRMI Acts.

Review and adoption of the draft national policy on internally displaced persons

The review and adoption of the draft NPI could address the challenge of non-adoption of the draft NPI. This could help outline the obligations of government, humanitarian actors as well as implementation strategies for the effective management of IDPs and enhanced human security in NE Nigeria. It would designate an IDP Focal Coordinating Institution (IFCI) and help to delineate relief and protection support roles between agencies involved in the management of IDPs in Nigeria to cover existing gaps and eliminate overlaps. The Presidency could task the Presidential Committee for North East Initiatives (PCNI) to convene a meeting of stakeholders to review the draft NPI in line with current realities in Nigeria, drawing lessons from the situation in the NE. The review could also take due cognisance of UNGPI, ACPAI and all related obligations of Nigeria under international law.

Establishment of a national humanitarian intervention fund

The establishment of a NHIF in collaboration with the private sector could alleviate the challenge of inadequate budgetary allocation to agencies involved in the management of IDPs in the NE. This could address the funding gaps arising from dwindling government revenue. It could provide a sustainable funding alternative to agencies involved in the management of IDPs and enable them address institutional capacity gaps to enhance human security in the NE. It could also offer the private sector the opportunity to fulfil corporate social responsibility obligations and contribute to national development. The Presidency could task the Office of the Secretary to the

Government of the Federation (OSGF) to liaise with the private sector and other stakeholders to develop modalities for setting up the Fund.

Harmonization of provisions in national emergency management agency and national commission for refugees migrants and internally displaced person acts

The harmonization of the provisions in the legislative Acts establishing NEMA and NCFRMI could mitigate the challenge of inter-agency rivalry between the 2 agencies. The harmonisation could clearly delineate the roles of both agencies in terms of response phase and function thereby facilitating effective management of IDPs for enhanced human security in NE Nigeria. It could also facilitate positive engagement with international partners as well as engender coordination and collaboration in the delivery of support to IDPs. This would ultimately promote human security in the NE and across the country. The FGN could direct the Federal Ministry of Justice (FMOJ) to liaise with NEMA and NCFRMI as well as other relevant stakeholders for a review of their mandates with respect to IDPs. This review could also take due cognizance of all international legal and normative instruments applicable to Nigeria.

7 Conclusion and recommendations

This chapter comprises the conclusion and recommendations. The conclusion summed up the entire study providing a summary of major findings and deductions following the presentation and analysis of data collected. Thereafter, the recommendations of the study were presented.

Conclusion

The study examined the management of IDPs and human security in NE Nigeria. The study was anchored on the Hierarchy of Needs Theory and adopted the field survey method to obtain views on the subject matter. The study took a cursory look at the management of IDPs and human security in general before dwelling on the situation in NE Nigeria It observed that despite several efforts towards the effective management of IDPs, several gaps that inhibit human security in the NE still exist.

The study examined some issues associated with the management of IDPs for enhanced human security in NE Nigeria. It identified policy framework as a major consideration for the holistic management of IDPs in the NE for enhanced human security in Nigeria. The study noted that there were several adhoc documentation efforts aimed at enhancing the management of IDPs and human security in NE Nigeria. It, however, observed that the absence of a coherent

mechanism for IDP registration, documentation and monitoring in the NE was hampering the delivery of support to the IDPs.

The study identified some challenges militating against the effective management of IDPs in the NE. This include the non-adoption of draft national policy on IDPs, inadequate budgetary allocation and absence of centralised database for IDPs. The strategies proffered to mitigate the challenges militating against the management of IDPs management for enhanced human security include the review and adoption of the draft NPI. This would cover existing support gaps and eliminate overlaps in the management of IDPs and could commence by Fourth Quarter of 2020. The establishment of NHIF in collaboration with the private sector could provide a sustainable funding alternative for the management of IDPs and enhancement of human security in NE Nigeria. This could commence by Second Quarter of 2020. Another strategy is the harmonization of provisions in the Act establishing NEMA and NCFRMI to delineate roles between both agencies. This could commence by the Second Quarter of 2020.

Recommendations

It is recommended that:

a) The PCNI should commence the review and adoption of the draft NPI by First Quarter of 2020.
b) The OSGF should establish the NHIF in collaboration with the private sector by Fourth Quarter of 2020.
c) The FMOJ should forward draft bills on amendments of Acts establishing NEMA and NCFRMI to NASS by Third Quarter of 2020.

Acknowledgement

My unreserved gratitude goes first to Almighty Allah for the gift of life and health, and for giving me the strength, ability and good health to go through this course and undertake this research work. I wish to acknowledge the Commandant of the College for his leadership and attention to the plight of Participants while on the course. I am particularly indebted and grateful to my supervisor, for his guidance, patience and support throughout this research work. Finally, I must acknowledge the special contributions of my wife Zainab who kept the home front intact and provided the much-needed support throughout the whole course. May Allah bless you and our children, ameen.

REFERENCES

ADESOTE, S. A.; PETERS, A. O. A historical analysis of violence and internal population displacement in Nigeria's fourth republic, 1999-2011. **International Journal of Peace and Conflict Studies**, v. 2, n 3, 2015. Available at: https://rcmss.com/2015/ijpcs/september/A%20HISTORICAL%20ANALYSIS%20OF%20VIOLENCE%20AND%20INTERNAL%20POPULATION%20DISPLACEMENT%20IN%20NIGERIAG%C3%87%C3%96S%20FOURTH%20REPUBLIC%201999-2011.pdf. Access on: May 28, 2020.

BAGSHAW, S.; PAUL, D. **Protect or neglect?**: Toward a More Effective United Nation Approach to the Protection of Internally Displaced Persons: an Evaluation. Washington, D.C.: Brookings Institution Press, Nov 2004. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/protection_survey.pdf. Access on: May 28, 2020.

BRING hope to internally displaced persons. **Peoples' Daily News**, China, June 7, 2015. Available at: http://www.peoplesdailyng.com/bring-hope-to-internally-displaced-persons/. Access on: Aug 22, 2019.

BUREAU OF ECONOMIC ANALYSIS. **Broad growth across states in 2014.** Suitland: Bureau of Economic Analysis, Jun 10, 2015. Available at: http://www.bea.gov/newsreleases/regional/gdp_state/gsp_newsrelease.htm. Access on: July, 17, 2019.

COHEN, R.; DENG, F. M. (ed.). **The forsaken people**: case studies of the internally displaced. Washington, D.C.: Brookings Institution Press, 1998.

DAODU, B. An overview of the management of internally displaced persons in the United States of America and Nigeria. **Express**, [S. l.], 2010.

GÓMEZ, O. A.; GASPER, D. **Human security**: a thematic guidance note for regional and national human development report teams. New York: United Nations, Feb 22, 2016. (United Nations Development Programme Human Development Report). Available at: http://hdr.undp.org/en/content/human-security-guidance-note. Access on: June 10, 2020.

HOPPER, E. Maslow's hierarchy of needs explained. In: THOUGHT CO. Science, tech, math. Social sciences. New York: California Privacy Notice, Feb 29, 2019. Available at: https://www.thoughtco.com/maslows-hierarchy-of-needs-4582571. Access: Aug 11, 2019.

IMMIGRATION AND REFUGEE BOARD OF CANADA. Research Directorate. **Colombia**: Internally Displaced Persons (IDPs), including relocation options available to IDs; whether IDPs are issued documents that indicate their status, including requirements and procedures to obtain copies of these documents (2012- June 2013) [COL104433.E]. Ottawa: IRB, 2013. Available at: http://www.ecoi.net/local_link/275814/405014_de.html. Access on: July 2, 2019.

INTERNAL DISPACEMENT MONITORING CENTRE. Nigeria IDP figures analysis. Geneva: IDMC, [201-?]. Available at: http://www.internal-displacement.org/sub-saharan-africa/nigeria/figures-analysis. Access on: Aug 14, 2019.

INTERNAL DISPLACEMENT MONITORING CENTRE. **Global figures**. Geneva: IDMC, [201-?]. Available at: http://www.internal-displacement.org/global-figures. Access on: July 18, 2019.

INTERNATIONAL ORGANIZATION FOR MIGRATION. **Displacement tracking matrix - DTM**: round 2. Camerron: IOM, Feb 2016a. Available at: https://reliefweb.int/report/cameroon/cameroon-displacement-tracking-matrix-round-2-february-2016. Access on: May 28, 2020.

INTERNATIONAL ORGANIZATION FOR MIGRATION. **Displacement tracking matrix - DTM**: round report IX. Nigeria: IOM, Apr 2016b. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/01_IOMDTMNigeria_RoundIXReport.pdf. Access on: May 28, 2020.

INTERNATIONAL ORGANIZATION FOR MIGRATION. **Displacement tracking matrix - DTM**: round VI report. Nigeria: IOM, Oct 2015. Available at: https://reliefweb.int/report/nigeria/displacement-tracking-matrix-dtm-round-vi-report-october-2015. Access on: May 28, 2020.

INTERNATIONAL ORGANIZATION FOR MIGRATION. **Displacement tracking matrix - DTM**: round VII report. Nigeria: IOM, Dec 2015. Available at: https://reliefweb.int/report/nigeria/displacement-tracking-matrix-dtm-round-vii-report-december-2015. Access on: May 28, 2020.

JONATHAN, Z. Over 1.9 million displaced persons live in camps, others – NEMA. **Punch Newspaper**, Nigeria, Nov 17, 2015. Available at: https://punchng.com/over-1-9million-displaced-persons-live-in-camps-others-nema/. Access on: May 30, 2020.

KASALI, T. **An integrated approach to rehabilitating IDPs**. [S. l.: s. n.], 2015.

LADAN, M. T. **Strategies for adopting national policy on IDPs**. Abuja: Civil Society Legislative Advocacy Centre, Nov 3, 2015. Paper presented at the National Summit on IDPs in Nigeria.

LOUISE, H. **Colombia's invisible crisis**: internally displaced persons. Colombia: Council on Hemispheric Affairs, 2015.

MASLOW, A. H. A theory of human motivation. **Psychological Review**, [S. l.], v. 50, n. 4, p. 370-396, 1943.

MCLEOD, S. Maslow's hierarchy of needs. In: SIMPLY PSYCHOLOGY. [S. l.: s. n.], 2018. Available at: https://www.simplypsychology.org/maslow.html. Access on: May 31, 2020.

NATIONAL EMERGENCY MANAGEMENT AGENCY. Close to 2 million IDPS live in formal camps, host communities and satellite camps. **This day Newspaper**, [S. l.], Apr 24, 2016.

NATIONAL EMERGENCY MANEGEMENT AGENCY. **NEMA, SEMA and IOM commence Registration and Biometric capture of IDPs in Borno State**. Nigeria: NEMA, [201-?]. Available at: http://nema.gov.ng/nema-sema-and-iom-commence-registration-and-biometric-capture-of-idps-in-borno-state/. Access on: Apr 28, 2016.

OXFAM. **Working for peace and human rights in Colombia**. Nairobi: Oxfam, 2012.

NORWEGIAN REFUGEE COUNCIL. Internal Displacement Monitoring Centre. **Uganda**: need to focus on returnees and remaining IDPs in transition to development. Switzerland: IDMC, May 2012. p. 25.

RUSSELL, S. S. **Refugees**: risks and challenges worldwide. Washington, D.C.: Migration Policy Institute, 2016.

STACEY, W. **Now what?**: the international response to internal displacement in the Democratic Republic of the Congo. Washington, D.C.: Brookings Institution, 2014. Available at: https://www.brookings.edu/wp-content/uploads/2016/07/The-International-Response-to-Internal-Displacement-in-the-DRC-December-2014.pdf. Access on: May 28, 2020.

UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES. **African union convention for the protection and assistance of internally displaced persons in Africa (Kampala Convention). Uganda**: UNHCR, 2009. Adopted by the Special Summit of the Union, Uganda, October 22, 2009. Available at: http://www.unhcr.org/4ae9bede9.html. Access on: Aug 11, 2019.

UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS. **Guiding principles on Internal displacement**. New York: OCHA, 2001. Available at: https://www.unhcr.org/43ce1cff2.pdf. Access on: June 4, 2020.

WILLIAM, S. UNHCR closes chapter on Uganda's internally displaced people. In: UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES. News and stories. **Briefing notes**, Geneva, Jan 6, 2012. Available at: https://www.unhcr.org/news/briefing/2012/1/4f06e2a79/unhcr-closes-chapter-ugandas-internally-displaced-people.html. Access on: Jan 17, 2016.

UNSTRUCTURED INTERVIEW

ABAGANI, R. Leader of IDPs, Gidan Yashi, interviewed on "Management of Internally Displaced Persons and Human Security: An Appraisal in North East Nigeria" by phone on Aug 21,2019.

AHANOLU, V. Programme Officer IDPs, NCFRMI, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria" at NCFRMI Office, Abuja, dated Aug 2, 2019.

AJAYI, A. Regional Desk Officer, OCHA, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria", by phone on Aug 21, 2019.

BUKAR, K. Head of IDPs, Pompomari Camp, Maiduguri, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria", by phone on Aug 20, 2019.

DANJUMA, M. Chief of Staff, PINE, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria", by phone on Aug 18, 2019.

DUKU, J. Journalist, Nation Newspaper, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria" by phone on Aug 23, 2019.

ESSIEN, M. Acting Federal Commissioner, NCFRMI, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria" by phone on July 28, 2019.

EZUGWU, B. O. GOC 7 Division, interviewed on "Management of internally displaced persons and human security: an appraisal in North East Nigeria", by phone on Aug 21, 2019.

PROFESSIONAL ARTICLE DOI 10.52781/cmm.e008

How technology is controlling our critical infrastructure, civilians and military working together to minimize cyberattacks

Como la tecnología controla nuestra infraestructura crítica, los civiles y los militares trabajan juntos para minimizar los ataques cibernéticos

Abstract: The purpose of this document is to analyze the influence of technological development and how that development increases the risks in our critical infrastructure. When we study our state, we look around and see how technology is taking control of all our important and critical systems. So, It is necessary to find the way of minimizing the cyberattacks through all the possible ways that our state has, such as, the military cyber units, legislation, protocols of act, and the most important part: the civilians that work in private companies (banks, hospitals, the electricity company, and others). This work should do this with two main objectives: first, working together as one indivisible partnership against those threats, and second, trying to maintain the systems that form our critical infrastructure safe and secure. To develop this topic, Will be used the descriptive method, and it is collected the information from important works, such as, The National Cyber Security Strategy Policy (Guatemala, Mingob 2018), books about terrorism or cyber terrorism and some web sites that describe diagnosis of cyber-attacks and how those cyber units have protected their critical infrastructure.

Keywords: Technology. Critical Infrastructure. Cyberattacks.

Resumen: El propósito de este artículo es analizar la influencia del desarrollo tecnológico y cómo este desarrollo aumenta los riesgos en nuestra infraestructura crítica. Cuando estudiamos nuestro Estado, miramos a nuestro alrededor y vemos cómo la tecnología está tomando el control de todos nuestros sistemas importantes y críticos. Por lo tanto, es necesario encontrar una manera de minimizar los ataques cibernéticos a través de todas las formas posibles que tiene nuestro estado, como las unidades cibernéticas militares, la legislación, los protocolos de acción, y la parte más importante: los civiles que trabajan en empresas privadas (bancos, hospitales, Compañía Eléctrica y otros). Este trabajo debe hacerlo con dos objetivos principales: primero, trabajar juntos como una asociación indivisible contra estas amenazas y, segundo, tratar de mantener seguros los sistemas que forman nuestra infraestructura crítica. Para desarrollar este tema, se utilizará el método descriptivo, y la información se recopila de trabajos importantes como la Política de Estrategia Nacional de Seguridad Cibernética (Guatemala, Mingob 2018), libros sobre terrorismo o ciberterrorismo y algunos sitios web que describen el diagnóstico de ataques cibernéticos y cómo estas unidades cibernéticas protegieron su infraestructura crítica.

Palabras-clave: Tecnología. Infraestructura crítica. Ataques cibernéticos.

Aram Albert Jordan Sandoval
Guatemalan Army.
Ciudad de Guatemala, Guatemala.
jordanaram15@gmail.com

Received: Mar. 06, 2020
Approved: Aug. 10, 2020

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introduction

Since the last two decades, technology had become a transversal axis in the human development. People use technology in our daily work, science, medicine, engineering and education, and many others. It had become an easy way to manage all our services around the world, e-banking, e-transportation, internet of the things, and we are right now very comfortable with it. Those facilities are our critical infrastructure (CARVALHO, 2016). Every country in the world has one and perhaps most of them are interconnected with each other.

As Paul Shemella in his book named "Fighting Back" explains something about motivations of terrorist acts will be paraphrase in understandable words like, most of those first world countries are getting concerned about how to maintain their systems safe and secure. They have created some public institutions (cyber units), who are fighting to minimize cyberattacks or fighting against hackers who might steal critical information, for money, personal assets, or even worse, destabilize a country or a group of countries who have strong relationships.

To start this work, it is necessary to answer this question: How can civilians and military work together in a strategical way to minimize those cyberattacks? during the development of this article, is compulsory find the way in which those main actors could work as a strategical team to fight against transnational threats.

In a new tech-world digging will be discover the meaning of critical infrastructure, its components, and the importance of maintaining that infrastructure safe and secure in order to let citizens have stable and dependable systems.

It is necessary to find a way to work together (Civilians and military) applying the international standards that include monitoring the infrastructure 24/7/365, avoiding and minimizing attacks and detecting and responding those transnational threats (protocols of action).

In this research report readers will find information about cyber terminology, the critical infrastructure generalities and components, international standards, and the national institutions that were created or improved such as the Computer Emergency Response Team (CERTS) and the Computer Security Incident Response Team (CSIRTs), (URVIO, 2017) that show the ethical way of monitoring, combating, and responding to cyberattacks and how they could affect our critical infrastructure.

Besides that, this research presents cases of study about two countries that are fighting against the cyberattacks in the same way, and both are creating strategies, specific laws on cybernetics, risk assessments and an awareness culture in their societies in order to protect their sovereignty and the honor of their nation. That information will be a source of study to minimize cyberattacks and how to prevent and combat those cyberattacks.

At the end to this research, it is expected from civilians and military to work as a national team in order to share experiences and for them to have a view of the nation about transnational threats such as cyber threats. Through sharing those experiences, they could work on new national defense strategies.

2 General characteristics

2.1 Cyber Defense: "Cyber defense is a computer network defense mechanism which includes responses to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks. Cyber defense focuses on preventing, detecting, and providing timely responses to attacks or threats so that no infrastructure or information is tampered with" (CYBER..., 2019, n.p.), CND (computer network defense).

2.2 Critical Infrastructure: "Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety. Although critical infrastructure is similar in all nations due to the basic requirements of life, the infrastructure deemed critical can vary according to a nation's needs, resources and development level" (CRITICAL..., 2019, n.p.).

2.3 Cyberattack: It "[...] is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use a malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. [...] [and it] is also known as a computer network attack (CNA) (CYBERATTACK, 2019, n. p.).

2.4 Computer Emergency Response Team (CERT): it "[...] is a group of experts who respond to cybersecurity incidents. These teams deal with the evolution of malware, viruses and other cyberattacks (COMPUTER..., 2019a, n.p.).

2.5 Computer Security Incident Response Team (CSIRT): is a team that responds to computer security incidents when they occur. An incident could be a denial of service or the discovering of unauthorized access to a computer system (COMPUTER..., 2019b, n.p.).

3 Critical infrastructure

3.1 Generalities

The concept of infrastructure started in the 80's. It included the public sector services, such as, railroads, bridges, airports, public transportation, water supplies facilities, and all the resources that the states had inside their territory. They took an important part on the development of all the country. They provided what the population needed because, in that part of the history, the government had all the power of the country. However, the concept changed in the 90's into a concept of National Security because the terrorist attacks increased dramatically.

The subsistence of the countries and their population development included national security, not only because of the meaning of the word, but also because they needed to close gaps between the terrorist attacks and the security of their critical and strategical infrastructure combined with critical information about their population and all of the state actives that states have.

They are the core of all the countries around the world. Then, after the events of 9/11 the concept of infrastructure changes again and despite of the facts, it appears now including the word "critical" not only for the public sector as in the 80's, but for the new concept or the new way to talk about infrastructure.

One of the main challenges in this concept is resilience because this word goes beyond its meaning. It includes the capacity of those countries to give their people flexibility, adaptability, and many capabilities of change or redefining the way to react when the situation demands that kind of resilience.

Nowadays, the critical infrastructure concept turns into a huge challenge for all the countries around the world, because of the population increasement, the needs of communicating or making more electronic bank transactions, and the spread of technology that could take an important part in human life, and it has become a transversal axis in everybody's daily routines.

The states will invest a lot of money in modern equipment, more severe policies, and more training for the people who will manage the new systems that will help them to keep those three aspects working as a whole in order to prevent some phishing information or to prevent some system intrusions.

Meanwhile, all of the national services (public and private) would work properly and giving their population all of the supplies and confidence that they need (O'ROURKE, 2007).

3.2 Components

The components of Critical Infrastructure directed to the public sector, the private sector, food systems, defense-industrial systems, national monuments, banking, financial systems, and many others that are taking an active part in all the countries.

They are vital for a country in order to provide their population with all the basic services, keeping the globalization process with other countries. This concept is not only for cyberattacks but also for natural disasters, economic recessions, lack of vital services, or weak countries. It is necessary to protect and maintain safe and secure every part of this infrastructure, because if one of these is missing the country would collapse in a very short term (O'ROURKE, 2007).

Now, one of the most important needs, is identifying the location of our strategical resources because they represent the most valuable actives of the country. These strategic resources have become a huge part of critical infrastructure and it is essential to monitor, protect, and identify where they are and how big or how useful they are. We should add them to the catalog of national infrastructure.

4 International standards

The International Organization of Standardization (IOS) plays an important role in cyber security and cyber defense because they present guidelines on how to manage and how to connect security and defense. It refers to working together, civilians and military. Then, those countries around the world need to work hard as a national team in order to create scenarios to help and find some national strategies and national policies to discuss some important challenges together, private and public sectors. Those standards have become invaluable tools for sharing information, knowledge, and experiences that contribute to keep the critical infrastructure safe, and to maintain credibility in technology. This way the population will use those in the best way they can in order to give a very clear spectrum of cyber security and cyber defense.

The following standards will present a guide on how to work in this new cybernetic world.

4.1 The IOS 27032

The IOS 27032 present some Information Technologies (IT´s), about security techniques in order to empower a state in cybersecurity using the most important techniques and strategic points related to network security, internet security, and applications security. This standard intends to guarantee the network information interchanges so that they could face cybercrimes.

The first area of this guideline is approaching cyber space and cyber security issues in order to close gaps within different cyber space domains and give an orientation to approach common cyber security risks that include social engineering attacks, piracy, malwares, spywares, and other new malicious software.

That techniques guide has provided some skills on how to be prepared for malware attacks, detection and tracking attacks, and responses for those attacks.

The second focusing area is the most important one. It is called "collaboration" because it is necessary to be effective and efficient in order to share and interchange information and coordinate how incidents will be managed. This collaboration will be secure and trustworthy in order to protect the stakeholders´ information. The standard includes system integration and interoperability in both ways (JUMBO VIVANCO, 2019).

4.2 The IOS 31000

The IOS 31000 according to (PALACIOS GUILLEM; GISBERT SOLER; PÉREZ BERNABEU, 2015) describes, in an understandable way, the meaning of risk management. Hence, in this case, it is very important to take advantage on planning or the decision-making process, because those states must be aware of cyberattacks, natural disasters, or any attack which destabilized countries.

It is necessary to make some risk assessments about our critical infrastructure without any restriction, but in a parallel way it is urgent to have a plan that assigns responsibilities to all the different sectors included and provide them with possible ways to prevent, mitigate, and recover on a different types of attack. It is also important to give them the opportunity to work in the same team, military and civilians, in order to protect the infrastructure and assist the risks together trying to minimize damages, especially if it is about a cyberattack because the damage could be immediate and calamitous. The consequences would be worse, for instance, if the cyberattack blocks the energy supplies or the banking sector or makes the critical infrastructure collapse.

4.3 IOS 27005

When one of the main targets is to protect the critical infrastructure, it refers to the information security risk management that present IOS 27005. It has been a reference framework about the methodology between risk management and information security, and it provides five important stages:

a) The interior and exterior plan
b) The definition of the organizational context (interior and exterior)
c) The valorization of technological risks
d) The treatment of technological risks
e) Monitoring and a continuous development management process

First, a communication plan that would be spread in the interior and exterior of the critical infrastructure of the public and private sector, and through this plan, determine risks and objectives in order to present a brief on the advances in the process. The best way to spread that information would be using written material and training people on those aspects.

On the other hand, this communication plan would be made in order to create awareness and security, and the most important, to evidence the existence of risks.

This plan would have three different aspects to be considered: primary communication which includes general concepts, implications and advantages. Next, communication on the way. This aspect presents advances of risk managements in order to have feedback and support from the people who is working on the risk. And last, outcome communications that will try to share and spread the information that reached through this plan.

The second stage of risk management is an organizational context that integrates mission, vision, policies, strategies, roles, and responsibilities. The importance of this context is the order in which the critical infrastructure will be protected when a cyberattack comes, and find the limitations to protect all of the information systems, and how a national response team would accept the risk level and this way, they would determine those reaches and limitations that the critical infrastructure has.

The third aspect is the valorization of technological risk. In this stage, the national information actives could be identified and this way, it could determine which is the most

important one to be protected. It can also establish the threats that the critical infrastructure is being exposed to in order to mitigate the risks. This valorization could be about cost-acquisition, renovation, recovery, or maintenance. On the other hand, it is necessary to identify the critical infrastructure threats that could be physical, logical, or strategical, and according to their origin: natural, technical, accidental, or intentional. It would help to identify the risks of those threats and to determine the impact in all the stakeholders.

The fourth aspect is the way to deal with technological risks because in this stage it is required an evaluation of the damage in order to mitigate the risks and collateral damages. That action could be used to reduce, accept, and eliminate damages.

This plan needs to define policies and guidelines and create a command and control unit in order to accomplish the recovery tasks and get the critical infrastructure to its normal state. This way, all the services and trustfulness would be given back to the stakeholders.

And finally, the continuous improvement. Through this, change controls on actives, process, vulnerabilities, threats and policies could be created with the purpose of establishing the following actions and keeping management updated in order to evaluate indicators according to the ones that appear in exterior or interior plans (RAMIREZ CASTRO; ORTIZ BAYONA, 2011).

5 Protecting the critical infrastructure cases of study: federative republic of Brazil and republic of Guatemala

5.1 Guatemalan National Cyber Security Strategy

Talking about Guatemala, in 2018, the ministry of interior published the national cyber security strategy in order to provide the governmental institutions guidelines about a theme that only the ministry of defense and ministry of interior have approached. It is a necessity to let the rest of the state know about the trending themes on national security in order to create social awareness and the responsibility that those institutions have as public servers. It is also important to tell the Guatemalan population about the national security issues that they need to fight against and how to deal with them.

The national cyber security strategy, as it is mentioned in the abstract of this research (GUATEMALA, 2018), includes:

a) Critical infrastructure
b) Information and communication technologies
c) Research and cyber incidents response
d) Legal frameworks
e) Governance
f) Mission, vision, objectives, and others

First, this new strategy refers to the Organization of American States (OAS) in their resolution AG/RES 2004 "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity". That resolution is the spearhead of the Guatemalan cyber security strategy model. That strategy literally says in its first five resolution points:

> 1. To adopt the Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, attached hereto as Appendix A.
> 2. To urge member states to implement the said Strategy.
> 3. To urge member states to establish or identify national "alert, watch, and warning" groups, also known as "Computer Security Incident Response Teams" (CSIRTs).
> 4. To place renewed emphasis on the importance of achieving secure Internet information systems throughout the Hemisphere.
> 5. To request that the Permanent Council, through the Committee on Hemispheric Security, continue to address this issue and to facilitate the coordination efforts to implement the Strategy, in particular the efforts of government experts, the Inter- American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), the Group of Governmental Experts on Cyber-crime of the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA), and other appropriate organs of the OAS (ORGANIZATION OF AMERICAN STATES, 2004, n.p., emphasis added).

This OAS resolution provides the guidelines on how Latin-America is facing the cyber security issues with a multidimensional and multidisciplinary perspective in order to create a cyber culture in the countries that are part of it. This organization is encouraging those latin countries to implement this strategy as their national strategy in order to create regional standards in cybersecurity. Those countries have their own way to detect, prevent, and respond to any cyberattack, but they do not have a common strategy that lets them work together in a multidimensional manner. The OAS encourages these countries to establish and identify Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) in order to integrate all this national, regional, and international teams as a huge team. Those teams will have a special trustable relationship in the way to share vital information against a cyberattack. Finally, the Interamerican Committee Against Terrorism (CICTE) will work as a coordinator for this strategy, meanwhile the other OAS departments would take part of the strategy when needed.

This strategy is the utmost important for the Guatemalan cyber security model because the transnational threats and the cyberattacks evolve, and daily electronic activities

take part in the digital zone, and the national systems are interconnected. It will be necessary to have a strategy that provides all Guatemalan sectors the opportunity to create technical frameworks and legal frameworks to strengthen the national and global cyber security. This strategy presents an important component with a great value, resilience. It will be necessary in order to reset as soon as possible all the services, avoiding with this recovery, the loss of information and collateral damages in order to protect the most valuable active in the country, its population.

This strategy was created in the beginning from a process that involved more than one hundred national and regional key actors from the different sectors of the Guatemalan society (military and civilians) according to the national security strategic plan (2016-2020), the national risks and threats agenda, and the nation security strategic agenda. This strategy analyzes the scenario that Guatemala needs in order to mitigate the risks and threats that are coming from the cyberspace.

The objectives that this strategy shows are oriented to strengthen the capabilities and the protocols of action from the institutions that are part of the national security system in Guatemala, assigning them the responsibilities to act based on a legal frame in order to maintain the rule of law in Guatemala.

Guatemala is involved in international frameworks that regulate the cooperation in terms of critical infrastructures, and, of course, they are leaded by the United States that is the first country to build a document related to the critical infrastructure protection. This document explains the necessity of creating a committee. This committee would evaluate terrorist attacks vulnerabilities in order to protect that infrastructure within a transnational dimension. Guatemala has many public infrastructures and other ones from the private sector, but they do not have the way to articulate all of them and the way to work with the best practices in information security procedures.

As a corollary of this strategy, Guatemala created two things after publishing this. The first one was a technical committee that includes the governmental sector, the private sector, the academies, the critical infrastructures, the financial sector, and the ITC′s sector in order to reinforce the relations of collaboration, cooperation, and coordination among them, promoting analysis and initiatives that increase the cyber security ecosystem in Guatemala.

The second one, according to the Guatemalan governmental agreement 65-2019 the Informatic and Technology Command was created by the ministry of defense. This command is responsible for the coordination of all the cyber defense themes, working with national and international institutions that manage these topics and becoming a part of that national and international effort.

5.2 The Brazilian cybernetic threats

In 2005, after a long time without a defense policy in Brazil, the Brazilian government emitted a National Defense Policy (PND in Portuguese). The main objective of this policy is to create an awareness for all the sectors in the country, in order to defend the nation, and establish the strategical importance of the cybernetic sector. That sector should be stronger

because Brazil has many systems with vulnerabilities and they need to create more capabilities to avoid those vulnerabilities and to recover, as soon as possible, all their ICT′s (information and communications technologies). That policy includes all the critical infrastructure security actions and enforces all the devices and procedures that help to reduce or to minimize vulnerabilities when they affect their national defense systems from cyberattacks. There are institutions in charge of that important challenge. Those institutions are: the Civil House or the Presidency, the Ministry of Defense, the Ministry of Communications, the Ministry of Science and Technology, and the cabinet of Institutional Security (AMARAL, 2014).

The previous information is a proof that the Brazilian government is working with civilians and military, through their national strategic policy, in order to protect the defense systems from cyberattacks, and that work includes the protection of their critical infrastructure.

The policy is setting all the national sectors in the same direction, whether these are private or public sectors, and they will generate more capabilities in order to gain a lot of cybernetic knowledge. They are getting trained to prevent, to protect, and to respond to any national or international threat that could take Brazil into a critical situation that could cause the loss of their hegemony and leadership in cyber security and cyber defense in South America.

The Cabinet of Institutional Security built in 2010 the Green Book of cyber security, with the main purpose of creating a cyber security environment in order to protect the Brazilian society and the nation. This green book was made to face the new challenges and mutual agendas in the private, public sectors, academies, and the "third sector" referring to the private institutions but non-lucrative according to (what is the third sector) (¿QUE ES..., 2018).

It is an joint effort civilians an military for creating a common thought and build together the guidelines of cyber security with that vectors: politic-strategic, economic, environment, communications, technology, education, legal framework, international cooperation, transportation, water supply, finance and energy supply, and when located those vectors in the same pot they creating their critical infrastructure.

The most important thing for the cybernetic sector was to assign that huge responsibility to an armed force through the Ministry of Defense, and after that, they created a cyber defense command. That unit has the mission of contributing to increase the cyber security level. This cyber unit has the know-how in order to work with different sectors and the Brazilian society. That military unit is trying to focus in creating human resources, doctrine, and security enforcement with the purpose of offering the population a quick incident response, learned lessons, and protection against cyberattacks (AMARAL, 2014).

In 2012, the ministry of defense published a document that contained a new cyber defense policy. It established the way to run a military cyber defense system. This document was written to define the tasks of the armed force in order to prevent the internet and other networks from the criminal use, and to protect all the information data and the essential communications. With this policy, the Brazilian army was empowered and took all the cybernetic control in the whole country. That control includes the responsibility to gather with all sectors assigning them their own responsibilities in this national security theme.

It also included instructions on how to share information, protocols of action, and the immediate way to respond in case of a cyberattack, building with this control, trustable relations among those sectors and the army in order to give the first national alert and making the cyber security plan go on.

Immediately after a cyberattack a national response team will contact all of their members and provide specific information from the field in order to meet them as soon as possible depending on the type of cyberattack, place of events, main damages, and determine which could be the first decisions to make. One of key challenges is to mitigate the damage and to try to solve de problem immediately. With that reaction, the cyber defense unit will coordinate with other institutions that have the responsibility to investigate and criminalize this attack according to their legal framework.

This short description explains the first actions against a cyberattack, how to activate the cyber security plan, and the way to criminalize the cybercrime if it exists, or if this attack is part of a cyber terrorism issue in order to warn the Brazilian neighbor countries or countries around the world.

Nowadays, Brazil has a step ahead compared to its neighbors. It is very close to consolidate their cyber security and cyber defense system from the highest political level with a national coverage, represented by the National Security Cabinet, the Federal Public Administration, and the Ministry of Defense, who builds the politic-strategic link, to the lowest levels of army units. Those units work on operational and tactical levels in the cyber security and cyber defense system including in that level the civilians who work in middle and lower levels in all kinds of sectors in order to defend their national cybernetic interests.

In the cyber security and cyber defense system, the Cabinet that was mentioned in the last paragraph has the task to coordinate all the actions that affect the society, for instance, cyber security, information and communication issues, and the national critical infrastructure security.

The ministry of Defense oversees all the issues related to cyber defense and received orders as follows:

a) Strategic Level: The Ministry of Defense will be responsible for creating protocols that let them be a part of the legal framework according to their national laws and their international agreements of actions that get them involved in a situation of crisis or armed conflicts and peace keeping operations.

b) Operative Level: here the Ministry of Defense, as all of armies around the world, should be prepared to conduct military defensive or offensive operations in order to preserve their sovereignty and the honor of the nation. In this concept the Brazilian army also includes all the problems that affect their cybernetic environment (AMARAL, 2014).

With that important policy, the Brazilian ministry of defense and the Brazilian army are taking control of all the critical infrastructure around the country. They are the link between the national institutions and private companies that are interconnected and interchanging clas-

sified information from the people who are living in Brazil or the people who are making electronic transactions, in or out of the Brazilian boundaries. They are expecting the Brazilian government to provide them a high security level of their personal information in order not to be an objective for a cyberattack, or to get their information stolen (phishing), or to be victims of extorsion from the organized crime.

The security level must be offered to those people in order to increase foreign investors and to make the business environment become more reliable. This way the Brazilian international trade will be more trustworthy.

On the other hand, the Brazilian government has a stronger critical infrastructure in order to conserve its natural resources in safe places and it also protects its strategical areas.

Nowadays, those strategical areas are being affected by organized crime and transnational threats that need to have these areas in order to increase their wealth.

That is why the national security team and the national defense team, combining their resources and capabilities, need to work together to become more powerful, and this way, they will detect, prevent, and respond to all the acts that could affect their national critical infrastructure and the systems that manage that infrastructure.

6 Conclusions

In order to make conclusions, it is compulsory to consider how technology is becoming an important part of the life of people around the world. Technology has made an increase of more than 50% of all the discoveries during the last century. It helps in all the daily activities as a transversal axis in science, domestic chores, military actions, and many others that include the critical infrastructure in all the countries.

Humans found a set of things that made their activities and even their lives easier in order to gain more time to do other activities. That is why those activities are the scope of this research because they need a way to provide more technological tools for people around the world. The software and hardware developers or the companies that have managed systems did not realize how dangerous those discoveries were not only because of the tools but also because of the way people use these tools.

Technological development should carry on, besides it, a big component of security in order to provide trustworthy connections and maintain the national security level on top in every country and collective security in their region.

After saying this, it is necessary to refer to the governments that created many institutions that have the responsibility to set up guidelines in order to provide cybersecurity for internal issues, and cyber defense teams to solve internal, external, regional and continental issues. Those institutions are combining their best efforts to work together, civilians and military, and now the new challenge is to work with many different agencies not only for sharing information but for building a common strategy to combat and mini-

mize cyberattacks too. Those attacks could affect the stability of any country and therefore, the stability of any region because most of their systems are interconnected to provide people e-banking, financial transactions, power light supplies, and many others, for instance, that should be secured through a national security level, and as a part of the government, it must be done inside the country.

In addition to this, it is necessary to talk about national security teams that play an important role in this security theme, because the Computer Emergency Response Team and Computer Security Incident Response Team are strategic tools for governments. They are the first defense line when a cyberattack takes place. Those teams have the capability to fight against an attack or attacks in order to prevent, combat, and respond to performing tasks that they are trained for.

Those teams work together in the private and public sectors. By taking advantage of their expertise, they will mitigate the collateral damage after an attack strike in any critical infrastructure area, and they have the responsibility to stop the attack, also the responsibility to take things to a normal status in a minimum amount of time. Those were the most important objectives when those teams were created.

On the other hand, those teams that are creating international standards must be taken into account in order to follow the rules of risk assessment that are an important part of this tool because, before those risk assessments, those governments did not know what their threats were, or how the critical infrastructure was composed, or what was their national security level. After having risk assessments, the international standards give them a precise guideline to make a strategical plan on how to prevent, combat and respond to a cyberattack, and how to recover the stability after that.

When talking about critical infrastructure its components cannot be put away. Those components are the reason of the nation and its stakeholders because they have no risk separately but when they work together like a gear in a country they become an important infrastructure that needs to be secured to provide at first confidence to people and also confidence to a region in order to invest and increase technological transactions in commerce, finances, banking, and other aspects. As shown in the body of this research, each country has its own critical infrastructure but at some point, these countries need to be intersected with the systems of other countries and this way, it becomes to be a goal to be protected by collective security.

It is important to say that it is necessary to review the critical infrastructure plan periodically so that the political-strategical level in the country keeps track on which institutions have been created, and check if they need to get inside their critical infrastructure and this way, they can keep their risk assessment plan updated.

To follow the logical order in this research, two countries that have almost the same issues and the same efforts to fight against cyberattacks were included. Those countries are the Republic of Guatemala and the Federative Republic of Brazil. Each of them owns problems, but they are assuming the difficult task of working together, civilians and military, private and

public sectors, as a team against those problems that they need to fight. They are working together in an interagency labor in order to minimize cyberattacks securing its critical infrastructure.

At the end of this research, it is necessary to highlight the need of the countries to provide a especial strategy to work together against cyber threats, but it is also necessary to create an awareness culture in all the societies because people are eyes of the nation on the streets and in the social networks. Since people and the social networks are in touch every day, they could provide important information to feed the national intelligence systems. All countries must deeply investigate the people who manage the critical infrastructure systems in order to have teams with a high level of confidentiality, honesty, and transparency.

References

AMARAL, A. C. La amenaza cibernética para la seguridad y defensa de Brasil. **Revista Visión Conjunta**, Buenos Aires, n. 10, p. 19-22, 2014. Available at: http://cefadigital.edu.ar/bitstream/1847939/32/3/VC%2010-2014%20AMARAL.pdf. Access on: Apr 19, 2020.

CARVALHO, P. S. M. de. A defesa cibernética e as infraestruturas críticas nacionais. In: EXÉRCITO. Comando Militar do Sul. Núcleo de Estudos Estratégicos. **Biblioteca do NEE**. Porto Alegre: Núcleo de Estudos Estratégicos, 2016. Available at: http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf. Access on: Apr 19, 2020.

COMPUTER emergency response team (CERT). In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019a. Available at: https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert. Access on: Nov 10, 2019.

COMPUTER security incident response team (CSIRT). In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019b. Available at: https://www.techopedia.com/definition/24837/computer-security-incident- response-team-csirt. Access on: Nov 10, 2019.

CYBER defense. In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019. Available at: https://www.techopedia.com/definition/6705/cyber-defense. Access on: Nov 10, 2019.

CYBERATTACK. In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019. Available at: https://www.techopedia.com/definition/24748/cyberattack. Access on: Nov 10, 2019.

CRITICAL infrastructure. In: WHATLS.COM. Newton, MA: Tech Target, 2019. Available at: https://whatis.techtarget.com/definition/critical-infrastructure. Access on: Nov 10, 2019.

GUATEMALA. Ministerio de Gobernación. **Estrategia nacional de seguridad cibernética**. Guatemala de la Asunción: Ministerio de Gobernación, mar 2018. E-book. (Documento técnico, n. 1). Available at: https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf. Access on: Apr 19, 2020.

JUMBO VIVANCO, P. L. **Implementación de un siem para el comando de ciberdefensa utilizando herramientas de código abierto bajo el estándar ISO 27032**. 2019. Thesis (Ingeniero en Sistemas Informáticos) – Universidad Tecnlógica Israel, Quito, Ecuador, 2019. Available at: http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf. Access on: Apr 19, 2020.

O'ROURKE, T. D. Critical infrastructure, interdependencies, and resilience. **The Bridge**, Washington, DC, v. 37, n. 1, p. 22-29, 2007.

ORGANIZATION OF AMERICAN STATES. The General Assembly. **AG/RES 2004 (XXXIV-O/04)**: Adoption of a comprehensive inter-american strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity. [Washington, DC]: June 8, 2004. (Adopted at the fourth plenary session held on June 8, 2004). Available at: https://2009-2017.state.gov/p/wha/rls/59284.htm. Access on: Apr 22, 2020.

PALACIOS GUILLEM, M.; GISBERT SOLER, V.; PÉREZ BERNABEU, E. Sistemas de gestión de la calidad: lean manufacturing, kaizen, gestión de riesgos (UNE-ISO 31000) e ISO 9001. **3C Tecnología**: Glosas de Innovación Aplicadas a La Pyme, [Alicante], v. 4, n. 4, p. 175-188, 2015. Available at: https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/324. Access on: Apr 22, 2020.

¿QUE ES el tercer sector?. In: AYUDA EN ACCION, Madrid, 7 feb 2018. Available at: https://ayudaenaccion.org/ong/blog/solidaridad/que-es-el-tercer-sector/. Access on: Nov 19, 2019.

SHEMELLA, P. (ed.). **Fighting back**: what government can do about terrorism. California: Stanford University Press, 2011.

RAMIREZ CASTRO, A.; ORTIZ BAYONA, Z. Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. **Ingeniería**, Bogotá, v. 16, n. 2, p. 56-66, Jul/Dic 2011. Available at: https://revistas.udistrital.edu.co/index.php/reving/article/view/3833. Access on: Apr 26, 2021.

URVIO: Revista Latinoamericana de Estudios de Seguridad. Quito, Ecuador: FLACSO, n. 20, jun./nov. 2017. Available at: https://revistas.flacsoandes.edu.ec/urvio/issue/view/150. Access on: Apr 19, 2020.