Cybersecurity

A Proposal for the Systematization of National Critical Infrastructures

Brig Gen (Reserve) Pedro Arthur Linhares Lima,
PhD, Brazilian Air Force

Introduction

With the advent of the Information Age, also known as the Digital Age, and its successor, the Knowledge Age, information has been elevated to the level of a strategic asset for organizations and nation-states. This has conferred to those who support and use it effectively and in a timely manner an unquestionable advantage in competitive environments and in contested international spheres.

The Internet, providing real-time connectivity and global reach, has brought unprecedented growth in the volume of information available to modern decision makers. However, its great vulnerability, together with the existence of new actors

with sinister intentions in the international stage, raises the concern for the protection of the information it transmits.

According to Raphael Mandarino, critical infrastructures (CI) are "the facilities, services, goods, and systems that, if interrupted or destroyed, would cause serious social, economic, political or international impact, to the security of the state and society."[1]

The most-common definition of CI is that which, once damaged by natural phenomena such as earthquakes or floods or by intentional acts of sabotage or terrorism, causes great negative impact to an entire nation and its society. Among the classic examples of CI are telephone networks, water collection and distribution systems, and energy-generating sources and distribution networks.[2]

With a hyperconnected world, the vulnerability of CI has become one of the greatest challenges of the modern day, as confirmed in the analysis presented by the Boston Consulting Group.[3] Standing out is the evidence of technological risks in industrial control systems used to monitor CI processes, as these systems have undergone a significant transformation. They have changed from the use of proprietary and isolated technologies to the use of open architectures—interconnected, above all, with corporate systems and worldwide computer networks.[4]

Following this line of reasoning, any impact, whether positive or negative, on *Infraestruturas Críticas Nacionais* (national critical infrastructures, ICN) will affect national power, dependent on a nation's people and resource capabilities, and its will to achieve and maintain national objectives in five areas: political, economic, psychosocial, military, and scientific-technological. Therefore, it is imperative for the state to organize itself to face any action, whether natural or intentional, that places CI at risk. This article proposes certain strategic alternatives to contribute to the improvement of the structuring, systematization, and integration of ICNs within the strategic governing bodies of the government and the armed forces.

The Cyberenvironment and the Threats to Critical Infrastructures

Technological evolution has rapidly accelerated the capability of automated data processing and the exchange of information among people and institutions, bringing great benefits to humanity. However, it has also made possible the appearance of intrusion tools in the computerized systems used by people in their personal and professional activities.

At the most diverse levels of public or private sector businesses with a public interest, computerized resources are used in varied activities, including the control systems of a nation's strategic areas, such as energy ICNs, telecommunications, transportation, water supply, finance, and defense, among others. Upon analyzing current virtual attacks that have had the CIs of some countries as their objectives,

it has been verified that the complexity and planning of these attacks had, at their root, states wanting to assert their will over others. In this context, diverse cyberattacks against computer and communications networks used in strategic systems can even affect national security, insofar as they can interrupt or degrade the functioning of structures essential to society and the Brazilian state, as is the case of the ICN.

Measures Implemented in Brazil Related to the Cyber Sector

National Defense Strategy and Cybersecurity and Defense Measures

The Brazilian *Estratégia Nacional de Defesa* (*National Defense Strategy*, *END*) established, in its guidelines, the strengthening of three areas of strategic importance and essential for national defense: space, nuclear, and cyber.[5] This decree establishes that cyber capabilities will include, as a priority, the communication capabilities between all contingents of the armed forces, to ensure their ability to network. The *END* emphasizes that the space and cyber sectors must be able to network with the armed forces as well. It also highlights that all state organizations shall contribute to the increase in the level of national security, with particular emphasis on the following aspects of cyber: security measures for CI and the improvement of security mechanisms and procedures that reduce the vulnerability of national defense systems against cyberattacks and, if necessary, allow for their prompt recovery.

Within the context of *END*, cyber is not restricted to activities related to cybersecurity and defense, but also covers *Tecnologia da Informação e Comunicações* (information and communications technology, TIC), a basic tool for the implementation of computer networks. Based on the END, the following are cybernetwork components: command, control, communications, computers, and intelligence (C4I) used for the operation and administration of the armed forces; TIC resources; and a matrix architecture that facilitates transmission of information for real-time decision making.

Cybersecurity

At the policy level, activities related to information and cybersecurity are managed by the following organizations:

a. *Conselho de Defesa Nacional* (National Defense Council, CDN):[6] state advisory body to the president of the republic in matters related to national sovereignty and the defense of the democratic rule of law. It has an executive

secretariat led by the minister of the *Gabinete de Segurança Institucional da Presidência da República* (Cabinet of Institutional Security of the Presidency of the Republic, GSI-PR). The jurisdictions of the CDN are provided in Article 91 of the *Constituição Federal* (Federal Constitution) of 1988,7 and the regulation of its organization and operation is contained in Law No. 8.153 of 11 April 1991.[8]

b. *Câmara de Relações Exteriores e Defesa Nacional* (Ministry of Foreign Affairs and National Defense, CREDEN): a governing body that advises the president of the republic on matters pertaining to foreign relations and national defense. It is headed by the minister of the GSI-PR and, among its responsibilities, is the security of information, an activity that is included within the cyber sector. Its jurisdictions, organization, and operating rules are contained in Decree No. 4,801 of 6 August 2003.[9]

c. *Casa Civil da Presidência da República* (Office of the President's Chief of Staff):[10] among its responsibilities, as it relates to the cyber sector, are the execution of policies for technical certificates and standards, and the operations approved by the *Comitê da Infraestrutura de Chaves Públicas Brasileiras* (Brazilian Public Key Infrastructure Committee, ICP-Brazil). This is due to the responsibilities of the *Instituto Nacional de Tecnologia da Informação* (National Institute of Information Technology), a federal authority linked to the Office of the President's Chief of Staff, which has the objective of maintaining ICP-Brazil, which is the *Autoridade Certificadora Raiz* (root certification authority) in the certification chain.

d. *Gabinete de Segurança Institucional da Presidência da República*:[11] is an organization under the presidency of the republic responsible for coordination within the *Administração Pública Federal* (Federal Public Administration, APF) on strategic matters that affect the security of society and the state, such as ICN security, *Segurança da Informação e Comunicações* (information and communications security, SIC), and cybersecurity.

To coordinate information security activities, the GSI-PR is organized with three subordinate bodies, namely:

a. Departamento de Segurança da Informação e Comunicações (Department of Information and Communications Security, DSIC) which has the authority to implement SIC activities in the APF. It provides regulation of SIC in the APF, training of federal workers as well as contractors, carrying out international agreements regarding the exchange of confidential information, representing the country before the Organization of American States

on cyberterrorism matters, and maintaining the Centro de Tratamento e Resposta a Incidentes de Redes da APF (Treatment and Response Center of the APF, CTIR-GOV).

b. *Agência Brasileira de Inteligência* (Brazilian Intelligence Agency, ABIN): is the central body of the Sistema Brasileiro de Inteligência (Brazilian Intelligence System, SISBIN), whose strategic objective is to develop intelligence actions to defend the democratic rule of law, society, and the effectiveness of public power and national sovereignty. Among its responsibilities, specifically regarding cyber, stand out the evaluation of internal and external threats to the constitutional order, among them cyber.

c. *Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações* (Center for Research and Development of Communications Security, CEPESC), is responsible for promoting scientific and technological research as it applies to communication security projects.

Another important document that deals with this issue is Decree No. 3,505 of 13 June 2000, which approved the policy for information security policy as it applies to APF organizations.[12] It confers the executive secretariat of the CDN, under the guidance of the Information Security Administration Committee created by the same decree and supported by ABIN through its Research and Development Center for Communications Security, with varied responsibilities for the implementation of measures related to this matter.

Analyzing these legal provisions and Decree No. 9,031 of 12 April 2017, which approves the regimental structure of the GSI-PR, shows that the GSI-PR centralizes the coordination of the vast majority of measures related to cybersecurity, information security, communications, and the security of CIs.[13] In addition to the Committee on Information Security, the GSI-PR coordinates with other important organizations, such as working and technical groups related to the security of CIs, security of critical information infrastructures, cybersecurity, and cryptography.

With regards to the ICN, the END selected six areas of priority, namely energy, telecommunications, transportation, water, finance, and information, with the latter permeating through all the previous ones, as the ICs increasingly rely on computer networks for their management and control.

Cyberdefense

The Ministry of Defense (MD) and the armed forces, as members of the APF, are already actively involved in the national effort regarding information and com-

munications security, cybersecurity and critical infrastructure security. The MD leads the expansion of these activities and frameworks to tend to the broad spectrum of operations characteristic of cyberdefense, including:

a. At the strategic level: the cyberactions necessary for the performance of the Armed Forces in crisis situations or armed conflict, and even in peaceful situations or as an institutional norm upon receiving a mandate to do so, as it happened, for example, in the 2014 World Cup and in the 2016 Olympic Games.

b. At the operational level: cyber, defensive and offensive actions, related to the preparation (training) and employment in military operations, of any nature and intensity, typical of a cyberwar environment.

The END formulates guidelines for the preparation and use of the armed forces, defining tasks that must be observed in time of peace, especially those related to the three established strategic areas—space, cyber, and nuclear. To implement the provisions of the END, on 9 November 2009, the MD issued Ministerial Guideline No. 14, which defined responsibilities for coordination and leadership in carrying out actions dealing with nuclear, cyber, and space areas, respectively, for the Navy, Army, and Air Force.[14]

The aforementioned guideline established that these responsibilities should be developed in two phases: First, the objectives and scope of each area should be defined; and second, strategic tasks should be defined and proposed frameworks elaborated, with the maximum use and adaptation of existing ones.

The Army concluded the first phase in December 2009, based on the studies and proposals of a *Grupo de Trabalho* (Working Group, GT). The work of the GT continued, and the Army concluded the second phase in March 2010. The MD approved the Army's proposals, which established the strategic objectives for cyber, together with forecasted strategic tasks.[15] The approved strategic objectives included specific tasks for information and communications security, cybersecurity and security of CIs, both for the MD and in collaborative participation at a national level with other institutions involved, mainly with the GSI-PR.

This collaborative participation between the MD and the institutions involved at the national level was put in practice in the last two major international events that took place in Brazil, which were the 2014 World Cup and the 2016 Olympic Games, according to the model presented in fig. 1, where, despite the diversity of the organizations involved, the work flowed, collaborating for the success of those events.

Figure 1. Collaborative participation model used in the last two major events in Brazil. (Source: ComDCiber, 18 August 2018)

In the area of cyberdefense, it is worth mentioning two consolidated strategic actions based on strategic objective number one, which established the creation of a cyberdefense framework subordinate to the Joint Chiefs of Staff of the Armed Forces: To include this topic in joint military planning, and the creation of a *Comando de Defesa Cibernética das Forças Armadas* (Information Security Command, ComDCiber) to implement the strategic objectives established for this area and its corresponding strategic tasks.

Under the coordination of the ComDCiber Nucleus, as of 2015, and after its implementation in 2016, several defense measures were consolidated, such as the implementation of the Cyber Defense Military System, and several others were initiated. These include the promotion of cyberinteroperability in national defense, the creation and implementation of the National School of Cyber Defense, the creation and implementation of the Cyber Defense Products Evaluation and Certification System, the training and generation of human resources needed to conduct cyberactivities in national defense, the implementation of the Information Security System with a focus on SIC, the promotion of research and development of defense products, and the production of knowledge intelligence from cyber.

As we can see, in the area of cyberdefense, the basic parameters for expansion—for example, improvement and consolidation—have been established in accor-

dance with the provisions of the *END* and the demands to achieve an effective systematic framework at the national level.

Proposed Actions

When analyzing the current security and cyberdefense situation in Brazil, we note that there are several rules that structure and guide the sector; yet, even so, we do not have the organizations that make up the ICN, strategic government organizations, and the MD integrated and interacting systemically. We ask: Why hasn't closer integration of all the entities involved in this process been accomplished? What is missing? The following are some suggested actions to try to answer these questions.

With regards to cybersecurity, as has been shown, several measures have already been implemented to protect and guarantee the use of strategic information assets, mainly those related to critical information infrastructures controlled by the ICNs. However, we have not yet achieved an effective interaction that provides the long-awaited integration of all the public and private organizations involved in the operation of the ICNs, especially the APF.

Therefore, it is imperative that all entities involved with cybersecurity of the ICNs first implement actions that guarantee that their critical information assets are minimally protected against internal and external threats. To do this, they must promote internal actions within their own organizations to reduce the fragility of their information assets against malicious attacks, and increase their resilience.

Procedures for Risk Assessment and Management and Business Continuity

As a first step to reduce the vulnerabilities of information assets, it is necessary to perform a risk assessment. Only after this evaluation will there be a notion of the measures that must be taken to minimize the risks encountered.

To meet this objective, in 2010 the GSI-PR published the "Reference Guide for the Security of Critical Information Infrastructures - Version 01" with the objective of guiding all APF organizations.[16] This guide, in addition to the characterization and contextualization on the topic of security of critical information infrastructures, presents a system for risk assessment with a more detailed proposal of risk management and business continuity. All the organizations involved in protecting ICNs must execute the actions proposed in this guide, since they are fundamental for carrying out the next step, which includes the implementation of threat-monitoring centers and equipment, which will allow the interaction and exchange of information with the monitoring and control bodies.

Creation of Centers and Equipment for Dealing with Network Incidents

To address incidents in APF computer networks, GSI-PR's *Departamento de Segurança da Informação e Comunicações* (Department of Information Security and Communications, DSIC) instituted the *Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública* (Federal Center for the Incident Treatment of Computer Network Security in the Federal Public Administration, CTIR Gov), which is the Computer Network Security Incident Handling Center for federal public administration.

It is the responsibility of the CTIR Gov to coordinate responses to computer security incidents related to networks; promote scientific-technological exchange related to network security incidents of computers with other centers; support federal public administration organizations and entities in the treatment of computer network security incidents; monitor and perform technical analysis of security incidents in the computer networks of the federal public administration; implement mechanisms that allow the evaluation of damages caused by security incidents in computer networks of the federal public administration; and support, encourage and contribute within the federal public administration for training in handling security incidents in computer networks. [17]

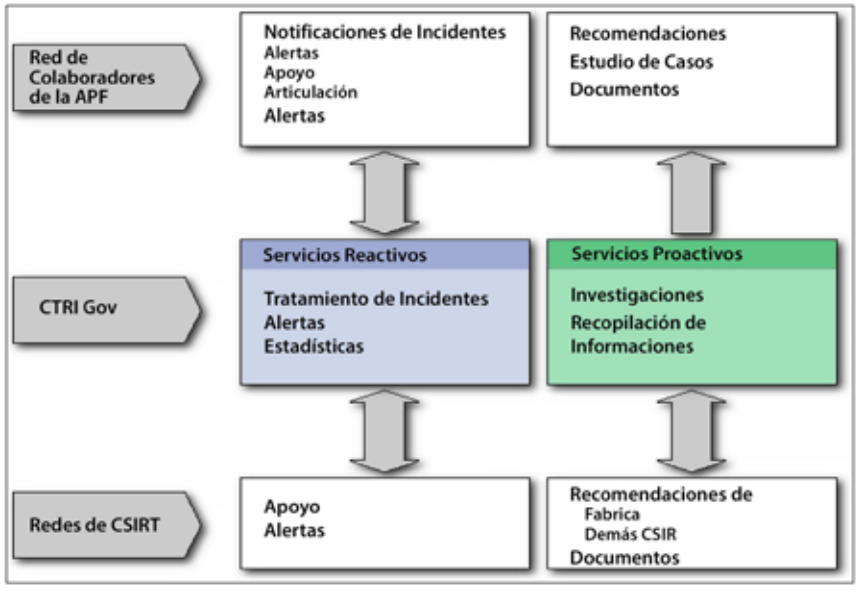

Figure 2. CTIR-Gov interactions

A security incident is any adverse event, confirmed or suspected, related to the security of computer systems or computer networks. The process of handling incidents, as shown in fig. 2, is basically divided as follows:

a. Notification of the incident: The receipt of incident notifications allows the CTIR-Gov to act as a central point to coordinate solutions to the resulting problems, through the collection of reported activities and incidents, analysis of the information, and correlation of these in the field from the informant organization or the APF community. The information can also be used to determine trends and patterns of attack activities and to recommend appropriate prevention strategies for the entire APF.

b. Incident analysis: This activity consists in examining all available information about the incident, including artifacts and other evidence related to the event. The purpose of the analysis is to identify the scope of the incident, its extent, its nature and the damages caused. It is also part of the analysis of the incident to propose containment and recovery strategies.

c. Support for incident response: In this case, the CTIR-Gov assists in the recovery process. This help is provided via e-mail or by suggesting documents that can help in the recovery process. This activity may involve assistance in the interpretation of the data collected and in the recommendation of containment and recovery strategies.

d. Coordination in the response of incidents: In this activity, the CTIR-Gov coordinates the actions among those involved in an incident, which may include networks and other computer security response teams (CSIRT) outside their scope of action. The coordination process involves the collection of contact information; the notification of those responsible for the networks, computers, or systems that may be involved or compromised; and the generation of indicators and statistics related to the incidents. The CTIR-Gov acts as a facilitator in the recovery of the incidents and in the exchange of information among the parties involved.

e. Distribution of warnings, recommendations, and statistics: This activity consists in disseminating information related to new attacks or tendencies of attacks observed by the CTIR-Gov, other treatment centers, or specialized companies. These alerts, in general, are produced by the CTIR-Gov itself, based on the notifications received or on incidents dealt with, or are redistributions of alerts issued by other centers with national responsibility. The CTIR-Gov, upon redistributing alerts, can add specific recommendations for its audience and assign different degrees of severity.

f. Cooperation with other teams: The CTIR-Gov, through general coordination, acts in the implementation of cooperation agreements with other APF incident response teams, as well as with other CSIRTs, public and private, national and international, with the purpose of technical cooperation and mutual assistance in the treatment of security incidents.

Through Regulatory Guideline No. 1, the GSI-PR advises the bodies and entities of the APF, directly and indirectly, discerning all necessary actions to implement information and communications security management.[18] Among these are appointment of the SIC manager; assignment and implementation of the *Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais* (Computer Network Incident Response Team, ETIR); and approval of SIC policy and other information and communications security regulations.

With regards to the creation of the ETIR in APF organizations and entities, directly and indirectly, the GSI-PR published Complementary Guideline No. 5, which regulates the creation of these teams.[19] This complementary guideline, in addition to offering several models to implement the ETIRs, presents many different ways that these teams can be structured, depending on the implementation model to be adopted; the size of the organization, the number of geographic locations and where the functions are located, the number of supported systems and platforms, the number of services to be offered, and the technical knowledge of the existing staff. Like the above, the GSI-PR published other complementary guidelines that are helping all APF organizations to structure and operationalize the protection of their computer networks.

Taking advantage of the successful experience of the APF, it is proposed that all the entities that make up the ICNs adopt this same structure for the treatment of computer network incidents, that is: implementation of CTIR and ETIR in all the entities that deal with the security of the people and CIs of the country. One way to implement this framework would be:

a. The creation of a CTIR in each regulatory agency in priority areas, such as: communications (ANATEL), energy (ANEEL), water (ANA), and transportation (ANTT).

b. The creation of the ETIRs in the various organizations that make up the ICN, for example, electric power: an ETIR in each of the operators, distributors, transmitters, and generators of electric power, linked to the CTIR of the ANEEL.

c. The connection of all CTIRs, including ComDCiber, to act as the CTIR of the MD, through the CTIR-Gov or another organization created for this

purpose, in which case, the CTIR-Gov would also be linked to that organization.

With the creation of these CTIRs and ETIRs, the doors would be open for greater interaction among all the entities linked to the security and cyberdefense of the ICN. In addition, the basis for the creation and effectiveness of a Brazilian Cyber Security and Defense System would be launched.

Creation of the Brazilian Cybersecurity and Defense System

From what has been presented, Brazil already has a significant basic framework in the areas of cybersecurity (including information security and communications and security of critical infrastructure) and cyberdefense. In the area of cybersecurity, the current framework confers a fundamental advantage by concentrating the coordination of main tasks in the presidency of the republic, as in the case of the GSI-PR. The work of the GSI-PR in this area is facilitated by its organizational structure, which allows the concentration of efforts in the main areas of interest, bringing together technical and military fields, and intelligence activities, for the prevention and management of crises.

Another relevant factor is the GSI-PR's responsibility to execute the actions necessary to carry out the exercise of the competencies of the CDN and CREDEN; organizations that have essential cyber prerogatives in the field of strategic decisions, as in the case of the CDN, and the formulation of public policy norms and guidelines, as well as the articulation of actions involving more than one ministry, as in this case of the CREDEN. Therefore, it is desirable that all those responsibilities linked to an organization that is part of the presidency of the republic be retained, as is the current case with the GSI-PR, to act as the central body of the system. This also applies to cyberdefense activities, which although more directly linked to the MD and the armed forces, need to be linked to the CDN for strategic decisions, and to the CREDEN, mainly for the articulation of actions with other public and private organizations. Taking as a starting point the proposals presented by OLIVEIRA, the strengthening of existing frameworks and the adoption of mechanisms that provide for systemic action, such as the formulation of corresponding public policies and guidelines, and the issuance of legal provisions that protect and regulate the actions of the participating organizations in the system, is proposed.[20]

In a simplified way, figure 3 presents an overview of the Institutional Model of the Brazilian Cyber Security and Defense System, adapted from BARROS.[21]

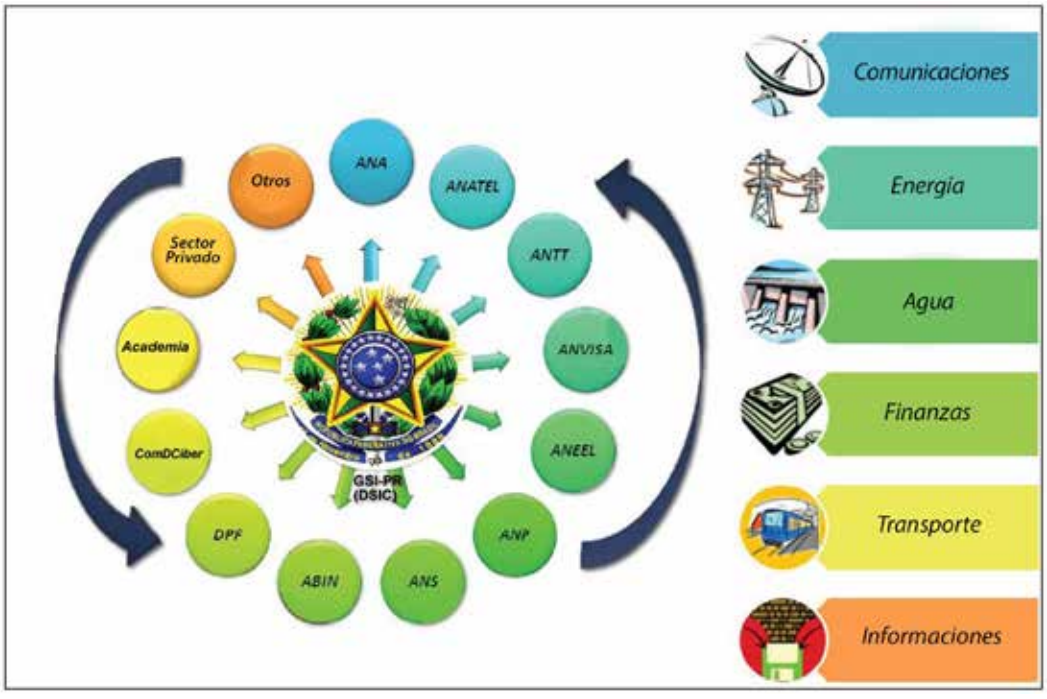

Figure 3. Institutional Model of the Brazilian Cyber Security and Defense System (adapted from BARROS)

As for cyberdefense, the strategic objectives and the corresponding strategic tasks are already established, as explained above. Now it's about implementing them. To make viable the creation of this system and facilitate understanding its application, it is necessary to establish a high-level interministerial GT within the framework of the CREDEN to study and propose the organization of this new system and the expansion, adaptation, and improvement of existing frameworks. Another important point to be highlighted is the system's imperative need for the permanent participation and interaction with intelligence activities.

Integration of Intelligence Activities to Security and Cyber Defense

The intelligence activity plays a fundamental role in the security and cyberdefense environment. It is essential in the search for information, using all available sources, to identify and prevent cyberthreats and provide adequate, timely responses. In addition, professionals working in the cyber sector must develop an intrinsic attitude of counterintelligence, to protect the knowledge and information inherent to their activities.

In this instance, it is important to expand signal intelligence activities to cover cyber needs, as is happening in other countries. One could take advantage of the experience of the armed forces and SISBIN. Therefore, the intelligence organizations in SISBIN must fulfill important activities within the Brazilian Cyber Security and Defense System.

Final Considerations

If, on the one hand, the advances obtained in the area of information and communications technology facilitate our lives and bring important benefits for humanity, on the other hand, they also bring harmful side effects with which we must learn to deal with. As cyberspace evolves, it is to be expected that the threats and challenges emanating from it will also evolve. The cyberthreat is patent and real. It reveals itself in the routines of people and institutions, whether in the individual, collective, or professional environments, and is stamped in the news media almost every day.

In the strategic environment of the state, combating this threat must be part of its priorities, to prevent damage to society and the state itself, which can reach considerable proportions. In Brazil, despite the relatively recent concern with the issue, actions have intensified in recent years. In the field of cybersecurity, the actions gained greater momentum after the creation of the DSIC in the GSI-PR in 2006. In cyberdefense, greater emphasis came to be observed with the publication of END in 2008.

In any case, the current moment is propitious to accelerate measures, to improve the interaction and integration of all the actors that deal with the security of ICNs, and that would make up the Brazilian Cybersecurity and Defense System. Thus, some actions were proposed to contribute to the achievement of these objectives:

a. Systemic evaluation and management of risks and business continuity, as the first step for the protection of critical information assets.

b. Creation of CTIRs and ETIRs to facilitate the interaction and exchange of information among all the entities involved in the protection of the ICNs.

c. Creation of the Brazilian Cyber Security and Defense System to systematize, integrate, and allow information to flow quickly, so that the responsible actors can make the right decisions in a timely manner and to establish a permanent collaborative environment.

d. Integration of intelligence activities with security and cyberdefense to predict, anticipate, and even prevent attacks from occurring.

In general, this article sought to focus on improving the interactions and integration of the organizations that make up the ICN, in relation to cybersecurity and cyberdefense. Likewise, for the structuring and strengthening of the cyber-protection of ICNs. Several other factors, in addition to the proposals presented here, should be considered and analyzed by the interministerial GT, proposed above, as it is outside the scope of this article. ❑.

Notes

1. MANDARINO JR., Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro (Security and Defense of Cyber Space). Brasília. 2010. p. 38.

2. International Critical Information Infrastructures Protection Handbook 2008/2009. Center for Security Studies, ETH Zurich, p. 36-37. Apud CANONGIA, Claudia, marzo de 2009.

3. Boston Consulting Group, World Economic Forum in "Our critical infraestructure is more vulnerable than ever" (*Foro Económico Mundial en "Nuestra infraestructura crítica es más vulnerable que nunca"*). Available in: <https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/>, consulted 12 August, 2018.

4. ENISA, Protecting Industrial Control Systems. Recommendations for Europe and Member States. (*Protegiendo los sistemas de control industrial. Recomendaciones para Europa y los estados miembros*), 2011. Available in: < https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states>. Consulted 12 August, 2018.

5. BRASIL. Presidência da República. Decreto nº 6.703. Aprova a Estratégia Nacional de Defesa, e dá outras providêICNas. (Presidency of the Republic. Decree Number 6.703. Approves the National Defense Strategy and other measures). Brasília. Diário Oficial da União, Poder Executivo. Brasília. 19 December, 2008. Available in: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Consulted 12 August, 2018.

6. BRASIL. Presidência da República. Lei nº 8.153. Dispõe sobre a organização e o fuICNonamento do Conselho de Defesa Nacional e dá outras providêICNas (Presidency of the Republic, Law No. 8.153, Establishes the organization and functioning of the National Defense CouICNl and other measures). Brasília. 11 April, 1991. Available in: <http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm>. Consulted 12 August, 2018.

7. BRASIL. Constituição da República Federativa do Brasil (Constitution of the Federal Republic of Brazil). Brasília. 1988. Available in: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Consulted 12 August, 2018.

8. BRASIL. Presidência da República. Lei nº 8.183. Organização e fuICNonamento do Conselho de Defesa Nacional - CDN. (Presidency of the Republic, Law Number 8.183. Organization and functioning of the National Defense CouICNl–CDN). Brasília. 11 April, 1991. Available in: <http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm>. Consulted 12 August, 2018.

9. BRASIL. Presidência da República. Decreto nº 4.801. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo (Presidency of the Republic. Decree Number 4.801. Creates the Ministry of Foreign Relations and the Government´s National Defense CouICNl). Brasília. 6 August, 2003. Available in: <http://www.planalto.gov.br/ccivil_03/Decreto/2003/D4801.htm>. Consulted 12 August, 2018.

10. BRASIL. Lei nº 13.502, de 1º de novembro de 2017. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios (Law Number 13.502 of 1 November, 2017. Establishes the basic organizations of the bodies of the presidency of the republic and the Ministries). Available in: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Lei/L13502.htm>. Consulted 12 August, 2018.

11. BRASIL. Decreto nº 9.031, de 12 de abril de 2017. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República (Decree Number 9.031 of 12 April, 2017. Approves the regimental structure of positions in commission and trusted functions of the Cabinet of Institutional Security of the Presidency of the Republic). Available in: <http://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Consulted 12 August, 2018.

12. BRASIL. Presidência da República. Decreto nº 3.505. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (Presidency of Republic. Decree Number 3.505. Establishes the information security policy in the bodies and entities of the Federal Public Administration). Brasília. 13 June, 2000. Available in: <http://www2.camara.leg.br/legin/fed/decret/2000/decreto-3505-13-junho-2000-368759-publicacaooriginal-1-pe.html>. Consulted 12 August, 2018.

13. BRASIL. Presidência da República. Decreto nº 9.031. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República. (Presidency of the Republic. Decree Number 9.031. Approves Regulatory Structure and Chart of Positions in Commission and trusted functions of the Cabinet of Institutional Security of the Presidency of the Republic). Brasília. 12 April, 2017. Available in: <http://planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Consulted 12 August, 2018.

14. BRASIL. Ministério da Defesa. Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos de Defesa (Ministry of Defense. Ministry Directive Number 14. Integration and Coordination of the Defense Strategic Sectors). Brasília. 9 November, 2009. Available in: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/0014_2009.pdf>. Consulted 18 August, 2018.

15. BRASIL. Ministério da Defesa. Portaria Normativa nº 2.621. Aprova a Estratégia Setorial de Defesa (Ministry of Defense. Normative Instruction Number 2.621. Approves the Sector Defense Strategy). Brasília. 7 December, 2015. Available in: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/12/2015&jornal=1&pagina=32&totalArquivos=136>. Consulted 18 August, 2018.

16. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Guia de ReferêICNa para a Segurança das Infraestruturas Críticas da Informação. Versão 1 (Presidency of the Republic. Reference Guide for the Security of Critical Information Infrastructures. Version 1). Brasília. November 2010. Available in: <http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf>. Consulted 12 August, 2018.

17. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 13 (Presidency of the Republic. Cabinet of Institutional Security of the Presidency of the Republic. Instruction Number 13). Brasília. 4 August, 2006.

18. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa nº 1 (Presidency of the Republic. Cabinet of Institutional Security of the Presidency of the Republic. Regulatory Instruction Number 1). Brasília. 13 June,

2008. Available in: <https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/14_IN_01_gsidsic.pdf>. Consulted 19 August, 2018.

19. BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Norma Complementar nº 5 (Presidency of the Republic. Cabinet of Institutional Security of the Presidency of the Republic. Complimentary Instruction Number 5). Brasília. 14 August, 2009. Available in: <http://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf>. Consulted 19 August, 2018.

20. OLIVEIRA, J.R. *Sistema de Segurança e Defesa Cibernética Nacional: Abordagem Com Foco nas Atividades Relacionadas à Defesa Nacional. In: Desafios Estratégicos Para a Segurança e Defesa Cibernética. 1ª Edição* (System of National Security and Cyber Defense: Focus on Activities Related to Nacional Defense. In: Strategic Challenges for Cyber Security and Defense. First Edition). 2011. Brasília. Anais... Brasília: Imprensa Nacional, 2011.

21. BARROS, O.S.R.; GOMES, U.M. *Conclusão. In: Desafios Estratégicos Para a Segurança e Defesa Cibernética. 1ª Edição*. (Conclusion. In: Strategic Challenges for Security and Cyber Defense. 1st edition) 2011. Brasília. Anais... Brasília: Imprensa Nacional, 2011. p. 213.

Brig Gen (Reserve) Pedro Arthur Linhares Lima, PhD,
Brazilian Air Force

Graduate from the Brazilian Air Force Academy. Continuance in Systems Analysis in the Pontifical Catholic University of Rio de Janeiro. Master's Degree in Computer Science from the USAF Institute of Technology. Doctor of Science in Production Engineering from The Alberto Luiz Coimbra Institute for Graduate Studies and Research in Engineering. Master's Degree in Business Administration in Politics and Strategy from COPPEAD-UFRJ Institute of Administration. He was Head of the Aeronautics Computing Center of São José dos Campos; Deputy Director of Systems and IT Infrastructure, Deputy Director of IT Projects, Advisor-Head of IT Governance and Director of Information Technology of Aeronautics. He is currently a researcher and professor of the Postgraduate Program in Aerospace Sciences of the University of the Air Force (UNIFA).