IGARAPÉ INSTITUTE
a think and do tank

MAPPING DIGITAL RISKS:

A MULTISTAKEHOLDER CALL TO ACTION FOR DIGITAL SECURITY IN BRAZIL

APRIL 2021

Index

Cover art: Raphael Durão

MAPPING DIGITAL RISKS:

A MULTISTAKEHOLDER CALL TO ACTION FOR DIGITAL SECURITY IN BRAZIL

INTRODUCTION

Over the past two decades, digitization has advanced considerably in Brazil. Even though there is still a long way to go to increase Internet access in the country, 70% of the Brazilian population is already connected. What is more, the Covid-19 pandemic has accelerated the digitization process in Brazil, turning into a necessity what was only a trend. The adopted measures to reduce the virus contagion after the outbreak, such as social distancing lockdown and social isolation, have further highlighted the importance and centrality of the Internet for the society and the economy. Several organizations have changed their operations to provide online services, adopting home office regimes, for example. In addition, more people are using the Internet for entertainment, shopping and keeping in touch with family and friends.

In a context of increasing access and dependence on the Internet, the challenges for digital security have become urgent and ever more widespread. Cities rely on stable networks to maintain their routine activities. As individuals and institutions relocate parts of their operations and lives to the digital environment, they tend to be more exposed and vulnerable to digital threats. Both, public and private sectors, including civil society organizations, need to identify as well as design new strategies in order to strengthen the security and resilience of digital operations.

Although all sectors face risks associated with digitization, the national digital security agenda remains considerably fragmented. Each sector, from banking to academia, experiences digital threats in different ways and has a specific understanding about 'what is a priority' or a 'shared risk'. In the same way, they have their own definitions about what "information security", "digital security", "cybersecurity" and "data security" means. While all sectors have been seeking to improve their digital resilience, they remain fragmented both in terms of vocabulary and actions amidst a growing digital interdependence that continues to amplify the transversal impacts of digital risks.

As a consequence, it is impossible to think about guaranteeing and maintaining digital security without a joint action among all relevant actors - which includes but are not restricted to: governmental agencies, private companies, civil society organizations, academic institutions and experts and the technical community representatives. Cooperation is what will help pave the way for systemic changes with transversal outcomes, reaching (and making safer) the majority of social and economic activities that today depend on the digital environment. To achieve this, we have elaborated this document that presents a framework that is capable of integrating knowledge around digital security risks and propose strategies for mitigating risks.

This work responds to this complex diagnosis: (I) the growing interdependence between sectors (private sector, public sector, armed forces, academia, technical communities, among others;) (II) the shared responsibility among them; (III) and finally, the need to build up a common agenda for digital security in Brazil. We understand that, in order to advance in the development of this agenda with more effective, sustainable and lasting actions for digital security, it is necessary to create a space to integrate knowledge, perspectives and practices about risk mitigation. That is why, throughout 2020, we worked with specialists from different sectors to identify the wide range of assets that need to be protected, as well as to elaborate a digital risk map and propose mitigation strategies that could be a push towards building an inclusive and holistic perspective for national digital security in Brazil.

While we understand that there is still a long way to go in order to promote structural changes and to reconcile digital security agendas, this document is the first step towards a collective action. We hope that it can inspire new initiatives that will respond to this call to action and deepen the framework proposed here.

BUILDING AN HOLISTIC APPROACH FOR DIGITAL SECURITY

The rising number of news related to data leaks, cyber attacks or disinformation campaigns are but the latest expression of the multiple dimensions of digital risks that continuously impact the economy, the society and politics in Brazil [1]. In this paper, **digital risks are a specific risk category related to the use, development and/or management of the digital environment for the conduction of any activity.[2]**

While some organizations have the resources and capacities to identify and monitor their own digital risks, most fall short of identifying the risks shared with other sectors. The immediate demands and pressures to respond to threats within organizations also result in responses and experiences that are strictly sectoral and do not answer challenges that are (and sometimes originate) outside its organizational limits. Nevertheless, other actors lack resources and/or capacities to identify and respond to cyber threats, such as civil society organizations and/or private sector entities that, due to the pandemic, had to digitize quickly to meet a context of virtual services and are left to catch up with security, privacy and data protection best practices.

[1] Examples of recent news on the topic: **TECNOBLOG.** Antivirus and Security. Leak that exposed 220 million Brazilians is worse than what was previously thought. Available at: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Access: mar. 2021. **G1.** Politics. STJ says that the court computer system was targeted by hacker attack and calls for a PF investigation. Available at: https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml. Access: mar. 2021. **CORREIO BRAZILIENSE.** Hackers. Investigation points out that a cyber attack on TSE has leaked recent data. Available at: https://www.correiobraziliense.com.br/politica/2020/11/4890026-investigacao-aponta-que-ataque-cibernetico-ao-tse-vazou-dados-recentes.html. Access: mar. 2021.

[2] Based on “Digital Security Risk Management for Economic and Social Prosperity” (2015), OECD’s Report. Available at: https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf.

So, it is essential to combine intra-organizational responses with strategies to prevent and identify risks and threats that are inter-organizational. Also, it is fundamental to consider a broader panorama of experiences and multistakeholder expertise that can support the construction of coordinated actions and channels (formal and informal) for cooperation as well as information sharing to build trust among sectors to overcome digital risks.

In order to address the **fragmentation challenge present in the national digital security agenda,** we collaboratively built (through multistakeholder meetings and the application of a questionnaire with digital security specialists): (1) a map that identifies all key assets that must be protected and the risks that most affect each one of them; (2) a typology to analyze the main digital risks; and (3) strategies for mitigating these risks. This process involved an effort of aligning different **vocabularies and concepts to address the different challenges associated with digital security,** mainly taking into account the specificities of each sector, as well as the transversality of risks.

This document presents the consolidation of this work, which has culminated in an agenda for mitigating digital risks that focuses on the **five main shared risks to all sectors (public sector, private sector, civil society, banking and financial sector, armed forces and others)** and designs mitigation strategies to support and incentivize a an actionable and collective agenda for digital security.

WHAT TO PROTECT?

To prepare this agenda, we started with the recognition of **six priority pillars for digital protection.** The pillars reflect, beyond the infrastructures and the information and communications systems (assets directly related to technologies), the centrality of assets such as rights, processes and people. Such understanding is fundamental to build a national digital security agenda that includes the individual as a central part of the mitigation strategies designed and implemented. This view is important as it broadens national security definitions for "cybersecurity" and information security that overemphasize systems, networks and infrastructures and introduces new dimensions of "what" and "how" something must be protected in a context of high digitization, interconnectivity and growing vulnerabilities by considering the human dimension of security.

Figure1: Digital Security Assets in Brazil

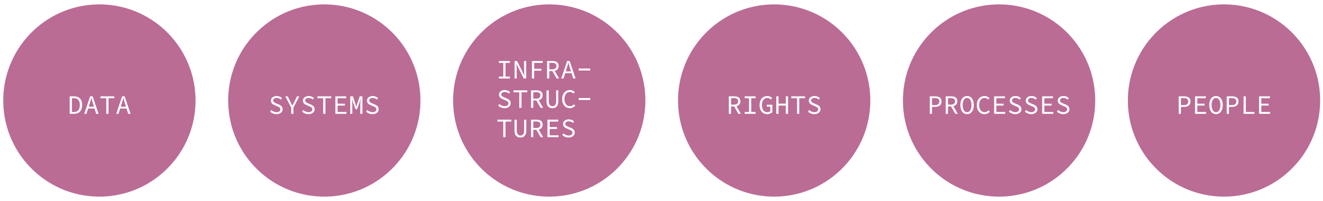


Table 1: Asset Definitions

	DATA	SYSTEMS	INFRASTRUCTURE
Definition of Assets	This asset refers to the units in which information and knowledge are created. Data make it possible to represent the world through units such as numbers, characters, symbols, images, bits, among others[3]. In this case, they include categories such as personal, sensitive and confidential data[4], as well as data related to the functioning of any organization.	The collection of computational and/or communicational components that support more than one objective of an organization, group or State.[5]	Broader category that encompasses both critical infrastructures and critical information infrastructures. [6] It includes priority areas such as: Energy, Water, Telecommunications, Transport, Biosafety and Bioprotection.

	RIGHTS	PROCESS	PEOPLE
Asset Definitions	Category that includes fundamental and human rights such as freedom of expression, reputation and image. This category introduces the intangible perspective of digital security governance assets.	All practices associated with ensuring the confidentiality, integrity and availability of an organization, group or public entity activities.	All kinds of assets related to physical threats to an individual's integrity associated with technological and/or digital tools, such as the impairment of an elevator or a cyberattack in a hospital.

The growth of digitalization not only enables the development of new horizons for the provision of services and information, but also consolidates the presence of these technologies as an increasingly fundamental layer for society, the economy and politics. However, risk analysis methodologies, especially those associated with digital risks and cybersecurity, remain focused on the intra-organizational environment.[7]

[3] Kitchin, R. The Data Revolution. SAGE Publications, 2014, p.3.

[4] It is possible to see the definitions for "personal data" e "sensitive personal data" in Brazilian General Data Protection Law(Law nº 13.709, 2018), in its 5th paragraph, sub paragraphs I e II. Regarding "sensitive information" it is possible to see the definition in Brazilian Freedom of Information Law (Law nº 12.527, 2011), in its 4th paragraph, sub paragraph III. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

[5] Adapted translation from NIST SP 800-16/1998.

[6] It is important to state that there is no common consensus regarding the understanding of infrastructure. However, related to the Brazilian context, the Information Security Glossary, for example, includes three components associated with this asset: cyber infrastructure, critical infrastructure and critical information infrastructure, as described below: **CYBER INFRASTRUCTURE** - "Information and communications systems as well as services composed of all the hardware and software necessary to process, store and transmit information, or any combination of these elements. Processing includes the creation, access, modification and destruction of an information. Storage/data warehousing encompasses any type of media on which the information is stored. Transmission is made up of both the distribution and sharing of information, by any means "; **CRITICAL INFRASTRUCTURE** - "Facilities, services, goods and systems, virtual or physical, which, if disabled, destroyed or have extremely degraded performance, will cause serious social, economic, political, international or security impact";
CRITICAL INFORMATION INFRASTRUCTURE - "ICT systems that support key assets and services of the Critical National Infrastructure."

[7] Based on the article "Cyber risk measurement and the holistic cybersecurity approach" (BOEHM; MERRATH, POPPENSIEKER; RIEMENSCHNITTER; STÄHLE, 2018). Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cyber%20risk%20measurement%20and%20the%20holistic%20cybersecurity%20approach/Cyber-risk-measurement-and-the-holistic-cybersecurity-approach-vf.pdf .

That is why it is important that risk methodologies and approaches incorporate not only the inter-organizational aspect in risk mitigation strategies but also a human-centric perspective to both risk identification and response. This work involves establishing a shared risk map that integrates new methodologies and risk perceptions so as to foster spaces for collaboration and dialogue that can both mitigate shared and specific digital risks through better coordinated strategies. Together, these and other efforts focused on the assets outlined above (Figure 1) can contribute to greater resilience of the digital environment, as they allow the construction of a holistic perspective of digital security, with an understanding of the transversality of the theme and encouraging collective actions.

THE RISKS PROSPECT

With those assets in mind, we identified the top **10 digital security risks in Brazil,**[8] described in Table 2. These risks were incorporated into a questionnaire that was sent to digital security experts from different areas. The questionnaire asked them to point which of the risks outlined in Table 2 have had the greatest impact on their sector.

Table 2: Definitions of Risks to Digital Security

	Absence / Inadequacy of Regulatory Frameworks	Absence of Protocols	Cybercrime	Disinformation and Manipulation	Threats to Critical Infrastructure
Risk Description	Absence of a legal framework (legal environment) suitable for data, systems, infrastructure protection. It can also be related to the existence of a law that can harm the protection of rights.	Absence of protocols for information sharing, for ensuring accountability in processes of technological integration (often, accountability protocols focus only on individual process components or on independent services); May also include other aspects such as the absence of an incident response plan that takes into account the direct and indirect damage that can affect the physical, psychological and patrimonial integrity of individuals. Absence of protocols can also be related to poor systems configuration.	Criminal acts, performed with the use of one or more computers, that violate personality rights - such as crimes against honor and discrimination. Other examples can be the practice of pedophilia and child exploitation as well as theft of credential and improper access to other types of data.	Dissemination of fake information, or even the manipulation of people through the use of information, which may affect the physical, psychological and patrimonial integrity of individuals, such as the manipulation of "feelings" using artificial intelligence tools and misinformation on health-related issues, or other information and communication technologies and their algorithms.	Include but are not restricted to: power outages and other essential services failure; Temperature control breakdown; Failure to control humidity; Inadequate maintenance; Lack of staff; Failures in the control of material disposal; Cyber attacks.

[8] See Appendix 1 to access the extensive list of vulnerabilities and threats that informed the 10 risks included in the questionnaire widely shared with professionals in the cyber security field.

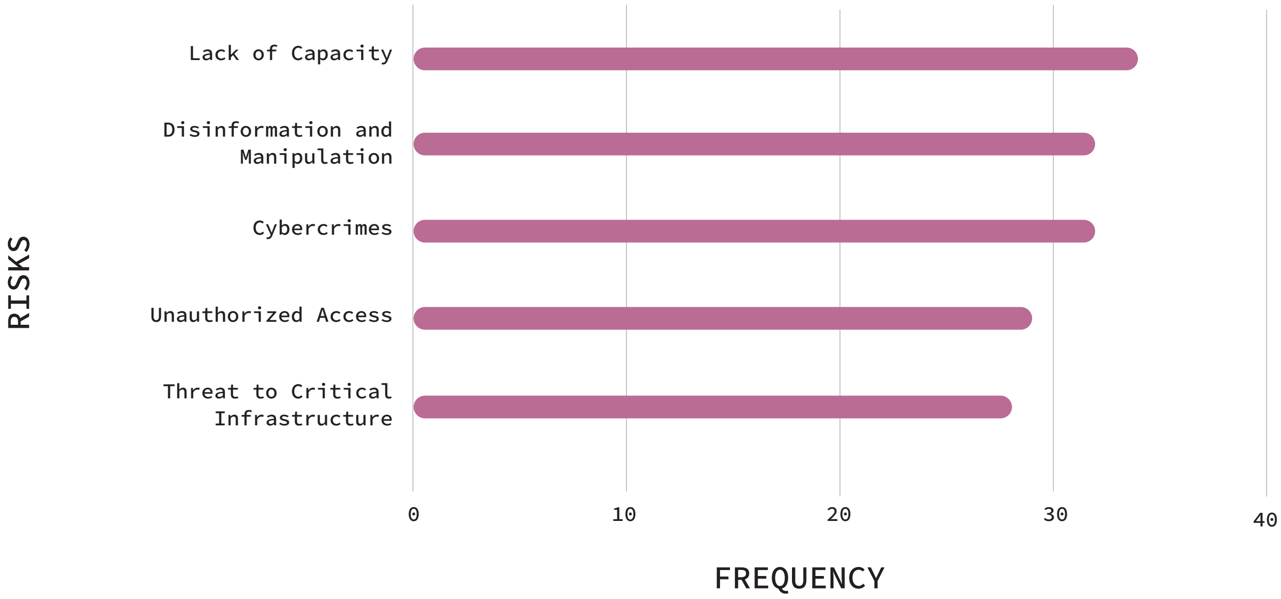
continued Table 2

	Unauthorized Access	Environmental Threats	Threats to Intellectual Property Rights	Threats to Human Rights	Lack of Capacity
Risk Description	Unauthorized access to information systems, obtained through social engineering or theft of credentials which can impair the processes of interaction between the different components of a system or organization.	Natural phenomena that can affect the environment and can also impact the availability and integrity of systems, such as: unfavorable weather conditions, floods, storms,lightning and electromagnetic interference.	Actions perpetrated by groups, individuals or organizations with the aim of damaging an organization's image and/ or reputation, or violating any Intellectual asset such as an industrial patent.	Actions that can harm or hinder the exercise of human rights (such as freedom of expression and press, as well as privacy and data protections), through technological means (surveillance, for example) by state actors - non-democratic and/ or autocratic governments - or the private sector - including practices that range from non-compliance with legislation to massive data collection practices, to name a few.	Lack of knowledge about basic data protection practices for computer systems; lack of technical capacity building for personnel in charge of a certain infrastructure; lack of transparency about responsibilities and competencies to ensure the protection of the system/ infrastructure/database inside some organization; unplanned or poorly system planning processes (designed in a very simplified or excessively complex way); processes that are not implemented (although planned) or poorly implemented; absence of policies and protocols for data processing and systems protection; lack of institutional integration; lack of training on new information and communication technology tools.

Using a **frequency** criteria[9] we defined the five main digital risks in Brazil (Graphic Chart 1): Lack of capacity, had the largest number of responses (34), followed by disinformation and manipulation (32) as well as cybercrime (32), unauthorized access (29) on the fourth place and, finally, threats to critical infrastructure (28).

[9] The "Questionnaire about Digital Risks in Brazil" was divided into four major stages: in the first one, the respondents informed their action sector (public, private, civil society, armed forces, financial and banking sector or other), as well as their gender and job position. In the second part, the respondents needed to indicate from which of the ten risks presented by our team would be the five with the greatest impact in their sector. In a third stage, the respondents were informed about the temporal horizon of occurrence for each risk, being asked to categorize them into short (from 0 to 2 years), medium (from 3 to 5 years) and long term (from 5 to 10 years) . Finally, the participants indicated which mitigation strategies their sectors adopt for each risk presented. The Graphic Chart "Five biggest digital risks in Brazil" were produced according to the answers of the second part of the questionnaire, in which each respondent indicated the five most serious risks according to their perspective. Once the questionnaire obtained 45 valid responses and each respondent informed us the 5 main risks in their perspective, we could get an amount of 225 responses. From this amount, the five most frequent ones appear on the graphic chart being understood as the digital risks of major proportion, common to all sectors/participants of the research. The frequency criterion refers, therefore, to the number of times the term appeared in the participants' responses.

Graphic Chart 1: Five Main Digital Risks in Brazil



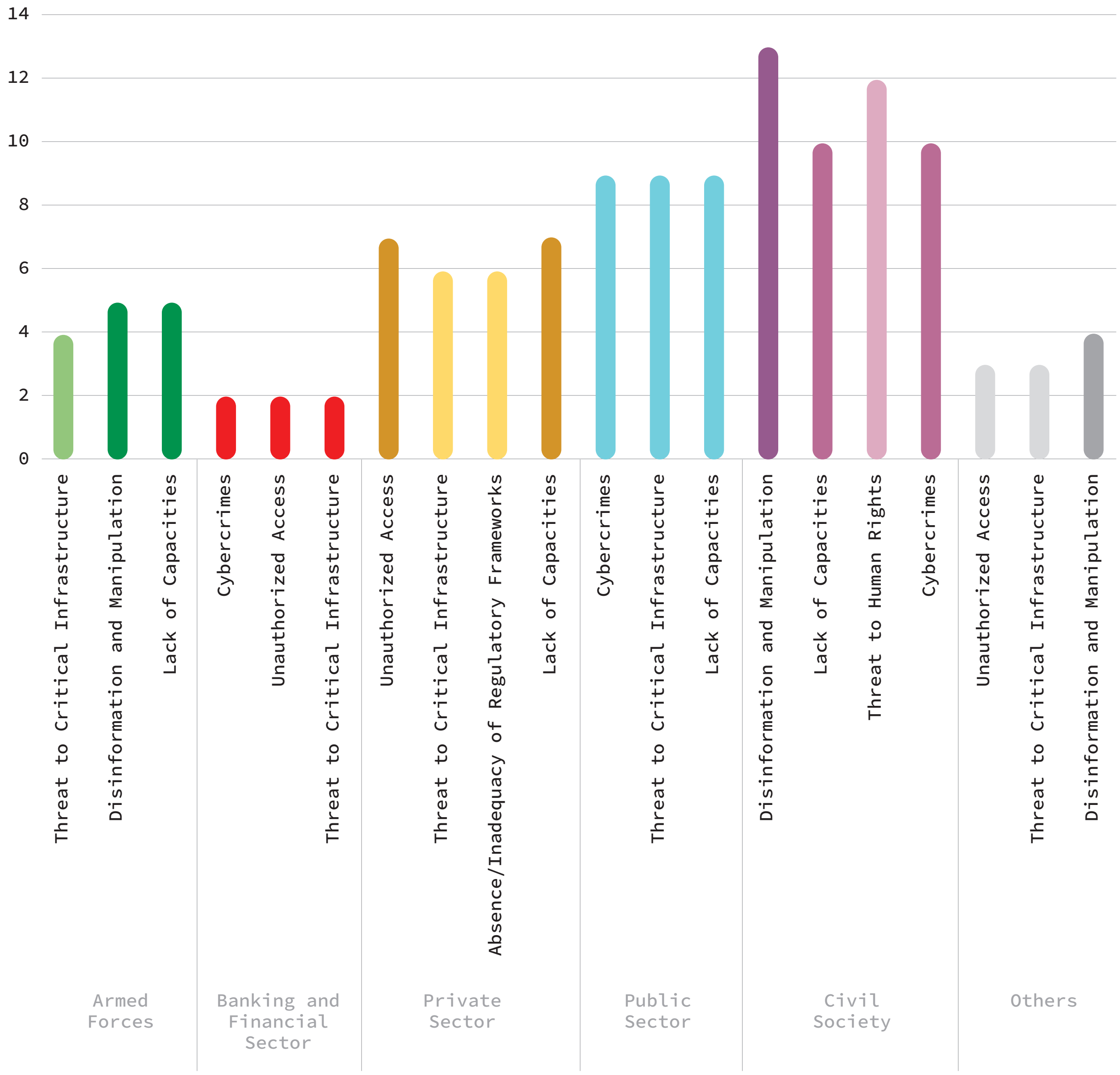
Risks have different impacts, depending on what each sector understands as a priority in cybersecurity. The graphic chart below shows the **three most important risks** for each sector that have taken part in the survey[10] . **Lack of capacity** and **threats to critical infrastructure** are present in the majority of responses, thus can be understood as a shared concern. For **civil society**, the greatest threat is related to disinformation and **manipulation** processes.

The **public sector** understands that **cybercrime, threats to critical infrastructure and lack of training** are risks of equal relevance, and the same happens for the **financial and banking sector** in relation to **cybercrime, unauthorized access and threats to critical infrastructure.** Unlike other sectors, **the absence and/or inadequacy of regulatory framework** emerges as one of the **private sector** concerns.[11]

[10] The Graphic chart "Three Greatest Digital Risks in Brazil according to Sector" was built according to the responses collected in the second part of the questionnaire, in which the respondents informed what were the five biggest digital risks according to their perspective of action. The three most frequent risks among these responses were understood to have the greatest impact on the respective sectors, once all five possibilities indicated by each respondent were considered. The sectoral distribution of all questionnaire's responses is present in the "Responses overview" section.

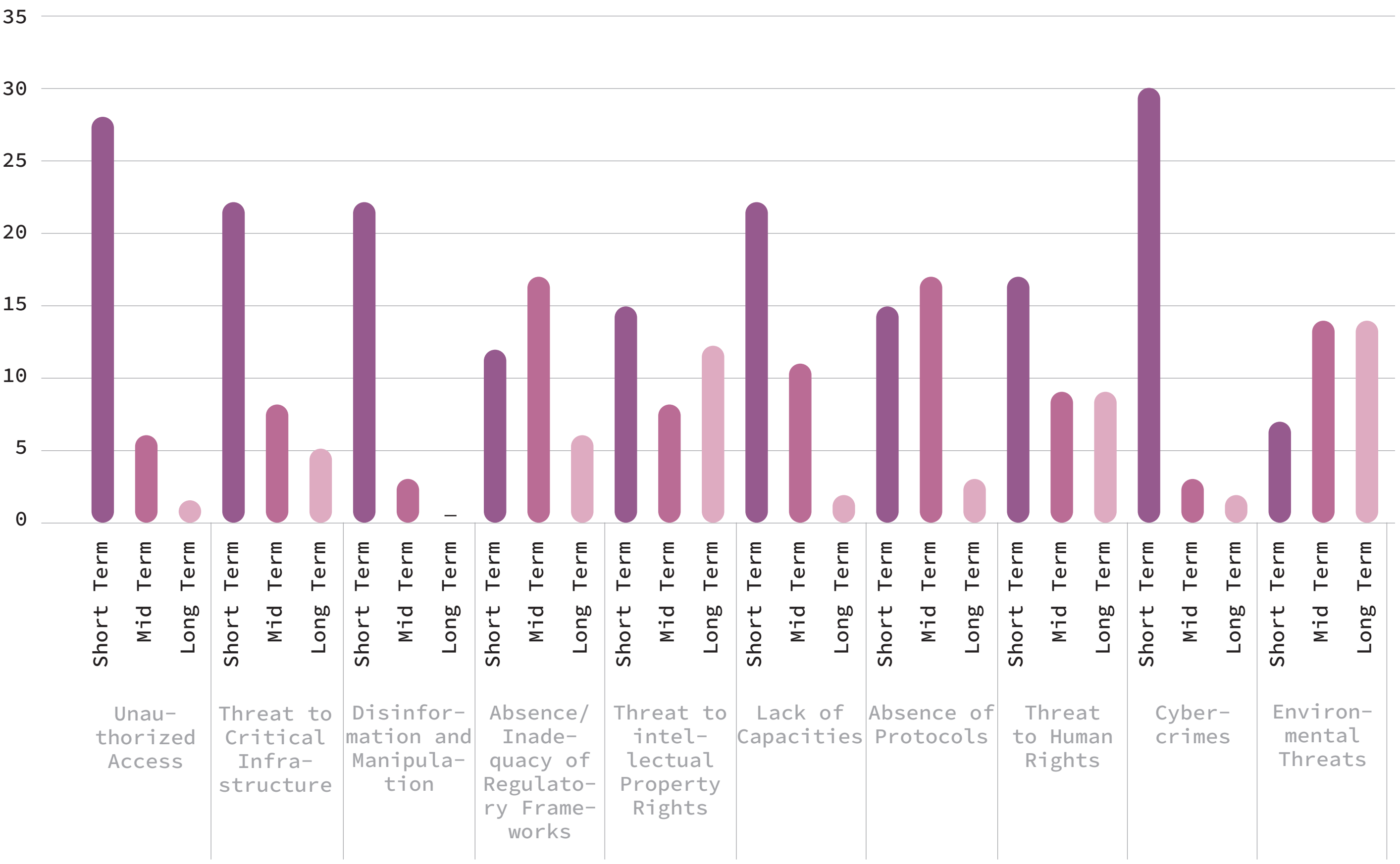
[11] For the private sector and civil society, the ranking of the three greatest risks was level between two different categories, understanding that these sectors consider them of equal relevance. For the private sector, "unauthorized access" and "lack of capacities" are present in seven of the responses, and "Absence/Inadequacy of Regulatory Frameworks" as well as "threat to critical infrastructure" are equally presented in six responses. For civil society, the ranking was: "disinformation and manipulation", with 13 responses, "threat to human rights", with 12, "lack of training" and "cybercrimes", equally with ten responses.

Graphic Chart 2: Three Main Digital Risks in Brazil



Graphic Chart 3: Respondents' Perception of the Digital Risks Time Horizon in Brazil

THE NEXT DECADE OF DIGITAL RISKS



In another part of the survey, the respondents were asked about their perception of the time horizon for the occurrence of each risk presented in the questionnaire.[12] The **short term** refers to the risks that might occur i**n 0 to 2 years, medium term, in 3 to 5 years, and long term, in 5 to 10 years.** All the five **main risks (lack of capacity, disinformation and manipulation, cybercrime, unauthorized access and threat to critical infrastructure) were understood as threats likely to occur in the short term,** expressing the urgency for implementing efficient mitigation strategies to avoid them. In the **medium term,** there are challenges related to adequacy, insufficiency or the emergence of **regulatory frameworks,** as well as concerns about the **absence of protocols.** Finally, one of the **long-term** risks identified was those pertaining to **environmental threats.**

We understand that this is an initial risk mapping effort that needs to be reiterated, expanded and carried out in new collaborative ways so as to achieve an integrated view of the digital risk landscape. Despite the challenges, this first effort allows us to identify not only the perceptions of risks in a multistakeholder way, but also convergences of perspectives and priorities across sectors that can inform the design of an effective horizon for collective action.

[12] For this data compilation, the universe of analysis was 35 valid responses, since not all participants in the questionnaire answered this section.

CHALLENGES AND MITIGATION STRATEGIES

Amidst the diverse set of digital assets and risks, it is equally important to establish key criteria for selecting priorities that can support not only **the creation of a national digital security agenda,** but also **immediate strategic actions to strengthen multistakeholder cooperation for overcoming the main risks.** As a result of the mapping exercise carried out with experts, we present a series of risk-mitigation strategies for the 5 main digital risks identified:

1 - Lack of Capacities;
2 - Disinformation and Manipulation;
3 - Cibercrimes;
4 - Unauthorized Access;
5 - Threats to Critical Infrastructure;

The risks above cut across different sectors (private sector, public sector, armed forces, civil society, financial and banking organizations, among others) and collectively identifying and facing them will not only make the digital environment safer but also will **enhance collaboration among these different actors, building a shared security agenda.**

In this sense, the mitigation strategies presented for each of the five challenges require effective guidelines for collective action between sectors. The following section presents actions that speak both to (i) the need to strengthen response capacities sectorially and (ii) enhance digital security resilience nationally.

1st Challenge
Broad effort for multistakeholder capacity building

There is a consensus among the distinct cybersecurity sectors that the lack of basic knowledge about data protection, technical best practices for infrastructures protection, and planning and implementing capacities are relevant threats to digital security. Although capacity building efforts are being carried out by some sectors, it is necessary to encourage the emergence of multistakeholder awareness and training initiatives to respond to digital risks.

In face of a fragmented digital security agenda, cross-sector training will encourage the sharing of concepts, perceptions and experiences. This will enable different sectors to build up a notion of risks that is better situated and, in this way, contribute to a more agile and sustainable development of a **security culture** in the country - understood here as an essential element for strengthening the resilience of the Brazilian digital environment.

Mitigation Strategies:

- **Provision of incentives for the creation of capacity building for public servants and company employees.** These programs should have clear indicators to measure effectiveness of action, as well as rewards to stimulate participation among organizations' staff. These training courses must be carried out periodically - so as to (i) keep up with the upgrades and changes in the technologies and systems used by both public and private organizations and (ii) to provide professionals with up to date knowledge on the evolving threat landscape. These and other actions reinforce capacity building as a continuous process rather than an ad hoc initiative. Establishing a continuous training across the public sector entities could effectively help address the challenges related to the high rotation of public servants and professionals. It would ensure that cybersecurity and data protection skills and awareness are a precondition rather than an exceptionality, especially within the public service. Capacity building activities and programmes could combine both expert training for cybersecurity professionals and broader security training for general staff.

- **Development of a list with key points of contact specialised in or working with digital security in the public administration.** Although some actors, such as CTIR.gov (Government Response Team for Computer Security Incidents) and others, have been already recognized as central players for technical cooperation within the Federal Public Administration (APF), the high level of rotation of public servants poses challenges for the continuity of communication and coordination activities. Thus, the adoption of practices such as having regular updates on a list of points of contact in different government bodies can help create more sustainable efforts in two ways: It will make it easier to contact key specialists as well as to better plan capacity building efforts for these points of contact and other security experts throughout the public sector.

- **Development of national awareness campaigns, with the involvement of all sectors.** These actions must be periodic, in order to keep the general public updated with the digital security agenda. Awareness actions are also key in accessing hard-to-reach communities and audiences that might not be part of the traditional education system. Currently, actions such as Safe Internet Day and the Internet Forum in Brazil (FIB) have combined similar efforts towards this direction.[13] Future activities should seek not only to bring more visibility into existing initiatives, but also to create spaces, forums and campaigns to address the risks dimensions according to affected communities. These and other efforts will also contribute to capacity building beyond the formal education system, making the topic more accessible to a wider audience.[14]

- **Teaching basic notions of digital security at all education levels,** with the addition of this subject in the National Common Curricular Base.

- **Prioritizing digital security topics in technical courses, higher education and postgraduate courses.** The inclusion of these themes should not be restricted to technical aspects inside the STEM curriculum, but should also be taught within Humanities and Social Sciences courses as well.

- **Inclusion of digital rights issues in all capacity building efforts,** so that incidents can be further understood through rights-centered lenses and according to their legal severity. The various regulatory agencies will have an important role in capacity building efforts.

[13] SAFERNET. Sid2021. Programação. Available at: https://www.safernet.org.br/site/sid2021/programacao. Access in: march. 2021.

[14] An interesting example of this kind of action is the OAS Cybersecurity Symposium, which is specifically dedicated to the cybersecurity topic, but offers thematic trails that address other specific security issues such as national security, human rights and CSIRT training, among others. See: OAS. OAS Cyber Symposium 2019. Available at: https://oeacybersimposio19.gob.cl/eng/wp-content/uploads/2019/09/AgendaSimposioOEA19ENG.pdf. Access in: march. 2021.

- **Conducting simulations and table-top exercises both as capacity building strategies for students and professionals, but also as mechanisms for building cross-sector integration.** Trainings like these have become a priority for many countries, such as UK[15], US, Germany, Switzerland and others that take part in the so-called Cyber 9/12 Challenge - an exercise that gathers students from different universities nationwide to respond to cybersecurity crises. The Organization of American States (OAS), in partnership with Trend Micro, have organized the CyberWomen Challenge, specific for women experts in the field.[16] In Brazil, the Armed Forces have launched the Cyber Guardian Exercise.[17] However, it is necessary to broaden this kind of initiative in order to include civil society organizations. These efforts will enable greater awareness of how digital risks impact different sectors and potentially indicate areas where different sectors can work together in responding to crises.

2nd Challenge Engaging all sectors in tackling disinformation and online manipulation

The use of the Internet, especially social networks, as a tool for spreading disinformation and promoting online manipulation can be considered as one of the main current digital risks. This risk stands out as the second most important threat, according to experts from different sectors in Brazil. The dissemination of false information, or the manipulation of people through its spreading, can affect the physical, psychological and patrimonial integrity of individuals, through dissemination strategies and the use of artificial intelligence tools.

As disinformation campaigns gain strength and volume, the tendency is that information reliability on networks will be largely affected and will result in the weakening of public and private institutions. Thus, it is necessary to understand that the problem of disinformation and manipulation not only affects all sectors but, as a shared responsibility, it also requires actions from institutions beyond traditional media, social media companies, fact checkers, big tech and so forth - it includes the government, cybersecurity experts, policymakers, schools and others.

Fragmented mitigation strategies will not be sufficient to face this risk. The Armed Forces, for example, have played a central role in mitigating external influences, but it is necessary to create collaborative efforts between the public sector, academia, civil society and the private companies to ensure a balanced and collective strategy for tackling the complex activities involved in disinformation and/or influence operations. These efforts should include the sharing of trustworthy information and the development of research that enables sectors to understand this phenomenon of disinformation and manipulation within specific informational environments; raising awareness about its harms in conjunction with building informational resilience through targeted training (i.e. investigative journalists).

Mitigation Strategies:

- **Development of crisis communication strategies.** As could be observed throughout the data leaks episode from the Superior Electoral Court (TSE), during the 2020 elections, a well-articulated communication strategy could have prevented the damage as well as the friction caused by the incident.

[15] Here an “Cyber Strategy Challenge” example (February, 2021). Available at: https://www.cyber912uk.org/en/

[16] TRENDMICRO. Cyber Women Challenge. 2018. Available at: https://resources.trendmicro.com/2018-LAR-CyberWomen-Challenge-ES-About.html. Access in: march, 2021.

[17] EXÉRCITO BRASILEIRO. Exercício Guardião Cibernético 2.0. July. 2019. Available at: https://www.eb.mil.br/web/imprensa/aviso-de-pauta/-/asset_publisher/0004ie79MBVM/content/exercicio-guardiao-cibernetico-2-0. Access in: march, 2021.

- **Creation of Multisectoral or Independent Task Forces to assist democratic processes.** An international example is the USA's "Election Integrity Partnership",[18] formed by academic institutions and think tanks, focused on collaboration between government and civil society, with the purpose to strengthen standards in order to fight disinformation on digital platforms and share related information to a wider public. In Brazil, during the 2020 elections, TSE created the Program to Fight Disinformation with a Focus on the 2020 Elections to leverage the expertise of a wider network of experts in fighting disinformation.[19] However, it is necessary that these multistakeholder efforts have a longer duration, so that they can be able to develop medium and long-term actions.

- **Allocation of resources for digital literacy training, at all educational levels.** Training tracks can be built in partnership with journalists and fact-checking professionals/organizations. The training should aim not only to raise awareness about disinformation techniques, but also to clarify what are the fundamental rights that can be potentially violated in campaigns of this kind.

- **Promotion of research and awareness campaigns about the modalities and techniques used in disinformation campaigns as well as in influence operations.**[20] Several academic and civil society groups are already carrying out research on the topic. Multistakehoder commissions and working groups can be formed to produce material in order to achieve a wider circulation and context-based research on techniques and tactics used by groups spreading and coordinating disinformation campaigns.

3rd Challenge Improving the strategies to prevent cyber crime

The cyber crime category encompasses a wide variety of criminal acts, performed using one or more computers. Such acts range from the violation of personality rights - such as crimes against honor and discrimination in the digital environment - to the practice of pedophilia and child exploitation online.

Other types of cybercrime are related to other challenges listed here, such as unauthorized access to systems and data. A good example are the notorious data leaks from the Superior Electoral Court (TSE)[21] in the 2020 elections, and the recent data leak of personal data from more than 220 million Brazilians citizens. [22] According to an MIT survey, published in the Journal of Data and Information Quality, Brazil had a 493% increase in data theft between the 2018 and 2019. [23]

[18] ELECTION INTEGRITY PARTNERSHIP. The Long Fuse: Misinformation and the 2020 Election. Relatório. 2021, 282p. Disponível em: https://www.eipartnership.net/. Access in: march, 2021.

[19] TSE. Programa de Enfrentamento à Desinformação com foco nas Eleições 2020 mobiliza instituições. Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2020/Maio/programa-de-enfrentamento-a-desinformacao-com-foco-nas-eleicoes-2020-mobiliza-instituicoes Access in: march, 2021.

[20] As operações de influência têm como alvo a formação de opinião através do uso de meios, ferramentas e técnicas ilegítimas, ainda que não necessariamente ilegais. Tradicionalmente, a literatura da área argumenta que operações de influência são realizadas por atores estrangeiros ou atores internos que atuam em nome destes (WANLESS; PAMMENT, 2019). Disponível em: https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf.

[21] UOL. Segurança. Bugs do TSE colocam eleição em risco. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/11/16/bugs-do-tse-nao-colocam-eleicao-em-risco-entenda-4-pontos-do-vazamento.htm. Access in: march, 2021.

[22] TSE. Segurança. Vazamento expõe dados de 2020 milhões de pessoas. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/01/28/vazamento-expoe-dados-de-220-mi-de-brasileiros-origem-pode-ser-cruzada.htm. Access in: march, 2021.

[23] NETO, N.; MADNICK, S.; DE PAULA, A.; BORGES, N. Developing a Global Data Breach Database and the Challenges Encountered. Journal of Data Information Quality, Jan. 2021, Art. 3. Available at: https://dl.acm.org/doi/abs/10.1145/3439873. Access in: march. 2021.

Improving the prevention and fight against cyber crimes must count on multi sector initiatives. On the one hand, it is necessary to strengthen the investigative capacities of the competent bodies. On the other, it is equally important to encourage knowledge sharing between the various sectors and deploy efforts to raise awareness among the population through initiatives that can shed light on vulnerabilities and tactics, but also support the development and adoption of safe and accessible technologies.

Mitigation Strategies:

- **Establishment of inspection and maintenance routines for systems used by public and private entities.** Some agencies and companies have already consolidated this practice, so it is possible to create best practice guidelines and lessons learned that can be further shared across institutions.

- **Investment to strengthen the technological capacities and training for the Federal Police and Civil Police specialized in cyber crimes.** There are currently 18 police departments specialized in cyber crimes in Brazil. However, it is necessary to enhance their capacities so that it is possible to strengthen their investigative skills and tools.

- **Emphasis on the importance of international cooperation in fighting cybercrime, mainly within the framework of Interpol, Ameripol and the United Nations Office on Drugs and Crime (UNODC).** Brazil is already a signatory of international agreements focusing on cybercrime within the scope of the BRICS countries and it is in the process of signing the Budapest Convention. New bilateral agreements can be an important tool to strenghten institutions in the fight against cyber crime.

- **Development of public and open source tools for detecting, filtering and preventing attacks.** Such measures can facilitate access to basic crime prevention resources for all types of users. Open source tools also allow constant improvement and scrutiny by the technical community.

- **Sharing information on detection, filtering and attack prevention systems with the wider public.** There are tools for sharing information on incidents that are already used by institutions in the banking and financial sector that can be adopted by other sectors. Organizations across sectors should encourage a three-way sharing model: within their respective sector (including intra-organizational), cross-sector sharing (with another sector or multiple sectors) and with the general public (so as to build awareness around risks, mitigation strategies and lessons learned).

- **Encouraging the development and use of “secure by design” systems.** As users become more aware of the need to adopt secure systems, there is a tendency for competing systems to improve investments in security in order to attract and gain consumer trust and, thus contributing to increasing the security of the digital environment as a whole.

4th Challenge
Ensuring security for systems access

The unauthorized access to information systems, obtained through social engineering, digital or physical security breaches, or credentials theft, can be considered as one of the main security risks, as they impair the interaction processes between different system components as well as results in significant costs and damages to both organizations and individuals.

Ensuring digital security of systems must be a multisectorial responsibility. Due to the increasing interdependence among organizations, the presence of any vulnerability can affect a whole chain of activities. Unauthorized Access is another challenge that must be faced with multi-sectoral training, awareness and the availability of tools for a wider range of actors and institutions.

Mitigation Strategies:

- **Greater awareness and availability of basic protection tools and mechanisms,** such as the use of devices and platforms with end-to-end encryption, Virtual Private Networks (VPNs), multiple authentication factors and the creation of strong passwords.

- **Encouraging the development and use of "secure by design" systems.** As mentioned in the mitigation strategies for cyber crime, the use of tools, computers, programs and systems that consider digital security as a priority since the moment of its development also contributes to the creation of a more secure digital environment with less exposure to systems's vulnerabilities.

- **Creation of open source and public tools for individual users.** Public and open source tools tend to be more secure, since their source code can be analysed and tested by the technical community. In addition, once they are available to a wider public, they allow easy access for all society's users. However, that does not mean that they are necessarily intuitive or easy to use. To leverage the existing open tools, it is important that capacity building efforts train organizations and individuals in threat modelling combined with an introduction to basic cyber hygiene measures/tools at their disposal.

- **Encouraging the publication of accountability and transparency reports or other measures by public and private organizations, disclosing any unauthorized access to their systems.** Once unauthorized access are identified, they must be reported to the general public. Such transparency measures are important for civil society, as it allows them to monitor the potential impacts that these attacks might have to human rights. [24]

[24] Some research, such as the paper produced by Maschmeyer et al (2020), states out that the majority of intelligence reports do not inform the impacts or incidents related to civil society groups. Some examples include the APT28, a nickname given by the Russian hacking group associated with the Russian intelligence agency GRU, that became known after the attacks against the U.S. Democratic Party in 2016 (MASCHMEYER; DEIBERT; LINDSAY). Available at: 6 (MASCHMEYER; DEIBERT; LINDSAY). Available at: https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658.

5th Challenge
Enhancing critical infrastructure protection

Critical infrastructures are essential assets and services for the full functioning of the society. In Brazil, energy, water, transportation, telecommunications and the financial systems are considered critical infrastructures. These are services that increasingly depend on connectivity, furthermore the energy and telecommunications systems guarantee the Internet provision for the whole country. It is important to emphasize that the protection of critical infrastructures depends not only on the effective prevention against digital threats, but also against physical threats that can compromise networks.

Because of the interdependence that all sectors have with the country's critical infrastructure, strategies for mitigating their risks should also become a shared responsibility. The Armed Forces are already undertaking efforts to train the infrastructure sector through the Cyber Guardian exercise, but it is necessary to expand the number of initiatives and cooperation networks between public agencies and the private sector. The exchange of knowledge and the development of joint initiatives will allow the creation of a security culture and a common understanding of the existing vulnerabilities.

Mitigation Strategies:

- **Establishment of rigorous policies for accessing systems related to critical infrastructures, with security profiles, control checkpoints and other security measures to ensure the confidentiality, integrity and availability of the systems**. Many organizations already have policies for accessing systems, but it is necessary to create and/or also encourage baseline data and cybersecurity standards across critical infrastructure sectors, based on best practices from the private sector and public agencies.

- **Encouraging policies for monthly maintenance for essential hardwares.** Hardwares are often less monitored against vulnerabilities than softwares. Thus, a policy of regular hardware maintenance and inspection is crucial for infrastructure incidents prevention.

- **Establishing a culture of regular external audits.** Independent audits, focused in assessing security systems used in critical infrastructure activities can be an efficient tool to identify vulnerabilities that might have gone unnoticed by self monitoring practices and protocols. These audits can also have an accountability role for all other sectors that depend on the full functioning of critical infrastructure.

- **Creation of a network of progressive cooperation between critical infrastructure institutions and the Federal Police,** for monitoring cyber crimes that may compromise the functioning of their services.

- **Establishing and maintaining detailed mapping of vulnerabilities and specific risks within the infrastructure sector.** It is possible to establish partnerships with academia for the development of methodologies that are aligned with technological development, in order to allow the constant updating of current risks and their mitigation strategies.

CONCLUSION

Throughout the multistakeholder meetings organized in the last 6 months and during the analysis of the multiple mitigation strategies mentioned in the questionnaires, it was possible to identify that the challenges shared by the different sectors reflect a central aspect: the absence of a more inclusive, transparent and sustainable digital security culture. Thus, if this document started with a diagnosis that highlights the transversal problem of the digital security agenda fragmentation, its conclusion comes with the perception that it is necessary to work for the establishment of a culture that overcomes this issue.

Digital security culture is understood as a set of concepts, paradigms and practices that can shape different perceptions and actions about security. The creation of a digital security culture involves taking forward awareness efforts on the subject, but also creating institutional norms, standards and practices that can ensure continuity, predictability and sustainability in achieving this cultural change.

The National Cybersecurity Strategy (E-Ciber) mentions the need to establish a culture of digital security, but we need to take a step further in deepening and transforming this imperative into concrete actions. Each actor involved in digital security governance demonstrates awareness on the importance of building a security culture. This process involves popularizing tools, protocols and techniques for risk prevention and systems' protection, as well as strengthening training efforts from different sectors. However, there are still no parameters for defining responsibilities in establishing a digital security culture.

In order to create a digital security culture, each sector must go beyond managing the risks that affect its own activities. Governments and companies need to empower users of their services so that they will acquire the essential knowledge and tools to ensure their security. Therefore it will be possible not only to protect themselves, but to enhance digital education and literacy among society.

Academic institutions and the technical community can collaborate in strengthening this culture by providing the necessary knowledge for the development of new techniques and practices. However, both sectors also need public investment for research in order to create cutting-edge technologies. Civil society organizations will also benefit from these investments and training efforts, while providing the expertise needed to reach vulnerable groups and a human rights-centered perspective on cybersecurity.

We hope that this work, and its future iterations, can assist in the enhancement of a digital security culture. We expect that (I) all sectors become fully aware of the overall landscape and all assets that must be protected. We also expect to (II) inform processes such as updating the Brazilian Digital Transformation Strategy (E-Digital); (III) assist the design of concrete implementation plans for strengthening trust in the Digital Environment in a multisectoral and multidimensional way; and (IV) reconcile defense and security in the digital environment in a broader panorama of strengthening data protection and privacy in Brazilian society.

ANNEX 1: DIGITAL SECURITY RISKS GLOSSARY

Below is a complete list of the assets and vulnerabilities highlighted in the digital security risk mapping process. As previously mentioned, this list is not exhaustive, but it presents a more detailed view of the challenges present in the current national panorama. It is worth mentioning that some threats and vulnerabilities may be mentioned more than once, since they represent different aspects in each asset.

ASSETS	THREATS & VULNERABILITIES	
Data	Data leaks	The unauthorized data transmission and sharing from an organization to an external destination, carried out electronically or physically, accidentally or intentionally.
	Credential Theft	Unauthorized obtaining security credentials that grant access to data, including identification, authentication, passwords, and profiles.
	Lack/Inadequate Regulatory Framework	Absence of a legal framework (or legal environment) suitable for data, systems, infrastructure and obligation protection. This concept can also be related to the existence of a law that can harm the protection of rights.
	Absence of Information Sharing Protocols	The absence of internal and external parameters that define how data can be shared and/or transferred between different departments of a single organization and/or between different organizations.
	Ransomware	Unavailability of data access through the implementation of malicious code until an amount is paid for the ransom.
	Lack of Capacities in the Use of Resources and Information Systems	The lack of knowledge about basic data protection practices for securing and protecting computer systems.
Systems	Environmental Threats	Natural phenomena, which affect the environment and can also impact the availability and integrity of systems, such as: unfavorable weather conditions, floods, storms,lightning and electromagnetic interference.
	Physical Threats	Theft; Vandalism; Sabotage; Terrorism; Inadequate transport.

Infrastructures	Unauthorized Access	Unauthorized access to information systems, obtained through social engineering or credentials theft which can impair the processes of interaction between the different components of a system or organization
	Threats to Critical Infrastructure	Power outages and other essential services failure; Temperature control breakdown; Bankruptcy to control humidity; Inadequate maintenance; Lack of staff; Failures in the control of material disposal; Cyber attacks.
	Environmental Threats	Natural disasters that compromise the integrity and availability of infrastructures.
	Espionage	Cyber attack carried against the infrastructure's information confidentiality.
	Power outages	Failures in the supply of energy that may compromise the integrity and availability of the infrastructures.
	Lack of Specialized Technical Staff	The absence of technical knowledge of the personnel responsible for the maintenance, administration and operation of some infrastructure system.
	Fires	Accidental or intentional fires that may compromise the integrity and availability of some infrastructure.
	Physical Invasions	Security incident in which the attack was made successfully, resulting in access, manipulation and/or destruction of information and/or system installation that compromises the integrity or availability of some infrastructure. Physical intrusions can be accompanied by malicious cyber attack strategies.
	Precarious System Configurations	Systems improperly configured and which may compromise the integrity and availability of the infrastructure provider.

Rights	Threats to Immaterial Property Rights	Actions perpetrated by groups, individuals or organizations with the aim of damaging an organization's image and/or reputation, or violating any Intellectual/immaterial asset such as an industrial patent.
	Control and censorship	Actions that can harm the exercise of freedom of expression, freedom of the press, the right to privacy and data protection, through the use of technological and non-technological means by state agents, non-democratic and/or autocratic governments.
	Cyber Crimes	Criminal acts, performed with the use of one or more computers, that violate personality rights - such as crimes against honor and discrimination. Other examples can be the practice of pedophilia and child exploitation as well as credential theft and improper access to other types of data.
	Disinformation and Manipulation	Dissemination of fake information, or even the manipulation of people through the use of information, which may affect the physical, psychological and patrimonial integrity of individuals, such as the manipulation of "feelings" using artificial intelligence tools and misinformation on health-related issues, or other information and communication technologies and their algorithms.
	Threat to Critical Infrastructure	Cyber attacks against critical infrastructures that once affect their availability and integrity, can impair the exercise of rights.
	Disproportionate or Inappropriate Use of ICTs	The use of new technologies without the appropriate knowledge of their operators, as well as the lack of regulation for them and failures intrinsic to its functioning. This scenario can lead to rights violations, such as: surveillance technologies and individual behavior changes due to platform algorithms.

Process	Unauthorized Access	Unauthorized access to information systems, obtained through social engineering or credentials theft which can impair the processes of interaction between the different components of a system or organization.
	Lack of responsibility attribution	The absence of full accountability protocols regarding technology integration processes. Lack of transparency about responsibilities and competencies to ensure the protection of the system/infrastructure/database.
	Unavailability	Communication failures between the different components of the process, service interruption (man-in-the-middle / DDoS); loss of connectivity and interference in the communication processes between systems.
People	Neglect the role of individuals in Incident Response Plans	Incident response plans, whether public or corporate, do not take into account the direct and indirect damage that can affect the physical, psychological and property of individuals.
	Disinformation and Manipulation	Dissemination of fake information, or even the manipulation of people through the use of information, which may affect the physical, psychological and patrimonial integrity of individuals, such as the manipulation of “feelings” using artificial intelligence tools and misinformation on health-related issues, or other information and communication technologies and their algorithms.
	Threats to Physical Integrity	Failures, attacks or misuse of systems that affect life controls (such as ransomware attacks in an hospital system), attacks that cause disruption of essential services, exploitation of vulnerabilities in technologies vital to an individual’s health (for example, cardiac pacemakers) and take -over of surveillance systems (in public security, aviation, among others).

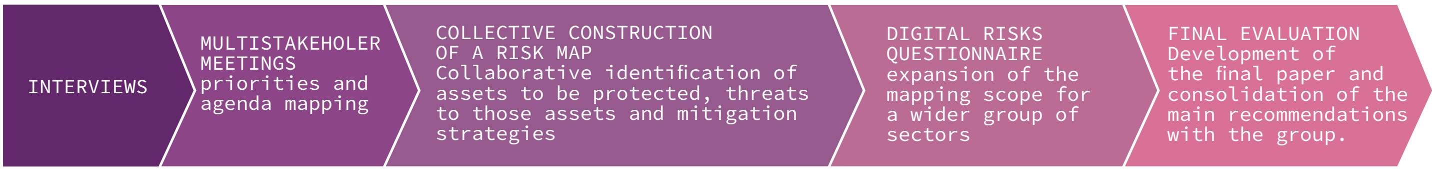
ANNEX 2: METHODOLOGY

This document is the outcome of a year of dialogue with representatives from different sectors in Brazil. We began the process with a multistakeholder meeting in April 2020, right after the outbreak of the pandemic. The objective of the first meeting was to understand the impacts of the pandemic in the reconfiguration of risks and priorities for digital security in Brazil. As a result of this first meeting, we identified that different sectors also have different views about security: which assets need to be protected, how to protect them and what are the gaps to achieve effective mitigation. In spite of the multiple questions regarding roles, responsibilities and understandings identified as a result of this session, the diagnosis in itself is not a negative one. It reflects the diversity of risks, experiences and priorities that compound Brazil's digital security. Even so, while a good understanding of its own sectoral risks has helped specific actors to be prepared to protect its data, systems, infrastructures, information and rights, the lack of dialogue between sectors is perhaps one of the main challenges for advancing a more strategic vision for digital security in the country.

Based on this diagnosis, we understand that, more than bringing these sectors into a dialogue, it was necessary to integrate different knowledges about digital risks, seeking to work together in a vocabulary capable of reflecting both the specific and transversal impacts of these risks.

THE RESEARCH PROCESS

Throughout the year (2020-2021), we developed a collaborative risk mapping with representatives from different sectors. The document is supported by a robust methodology that included interviews (semi-structured and unstructured), multisectoral meetings with the application of design thinking techniques and a questionnaire.



INTERVIEWS

MULTISTAKEHOLER MEETINGS
priorities and agenda mapping

COLLECTIVE CONSTRUCTION OF A RISK MAP
Collaborative identification of assets to be protected, threats to those assets and mitigation strategies

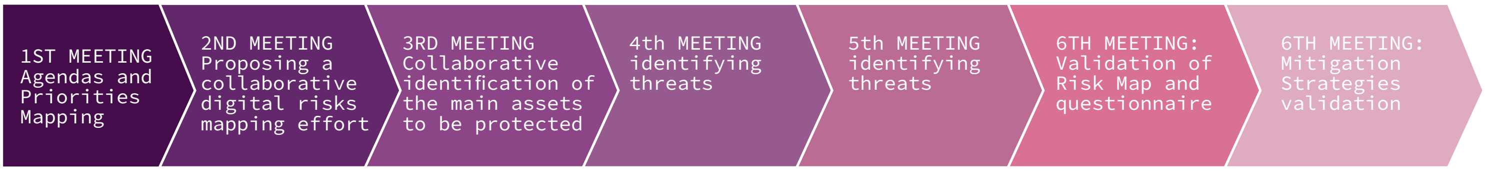
DIGITAL RISKS QUESTIONNAIRE
expansion of the mapping scope for a wider group of sectors

FINAL EVALUATION
Development of the final paper and consolidation of the main recommendations with the group.

MULTISTAKEHOLDERS MEETINGS

This paper collective construction process included seven virtual multi-sectoral meetings. We started with a scenario prospecting meeting to understand the main agendas and concerns about digital security in Brazil and which were the mains transformations caused by the pandemic. A lack of common vocabulary and understandings for addressing digital security challenges in an increasingly interconnected scenario was identified. Although the meetings participants presented some shared concepts definition (such as information, cyber security and digital security), on the other hand, it was diagnosed a need to delimit what were the specific concerns about each sector main risks.

In the second phase, we brought together a larger group of experts from different sectors to start a collaborative risk mapping process for digital security. The process, which lasted six months, went through the identification of the main assets to be protected, the main threats and, finally, the main mitigation strategies and responses.



1ST MEETING Agendas and Priorities Mapping

2ND MEETING Proposing a collaborative digital risks mapping effort

3RD MEETING Collaborative identification of the main assets to be protected

4th MEETING identifying threats

5th MEETING identifying threats

6TH MEETING: Validation of Risk Map and questionnaire

6TH MEETING: Mitigation Strategies validation

Regarding the mitigation strategies identification, we combined this collaborative work with a questionnaire application aimed at digital security professionals.

THE QUESTIONNAIRE

We shared the questionnaire with specialists and professionals from different sectors with impact on digital rights, technology and security issues. In total, we obtained 45 valid responses. The questionnaire was divided in two parts: the first section presented multiple choice questions to assist in the process of mapping the main risks according to each sector's priorities. The second section presented questions about the mitigation strategies suggested by the respondents.

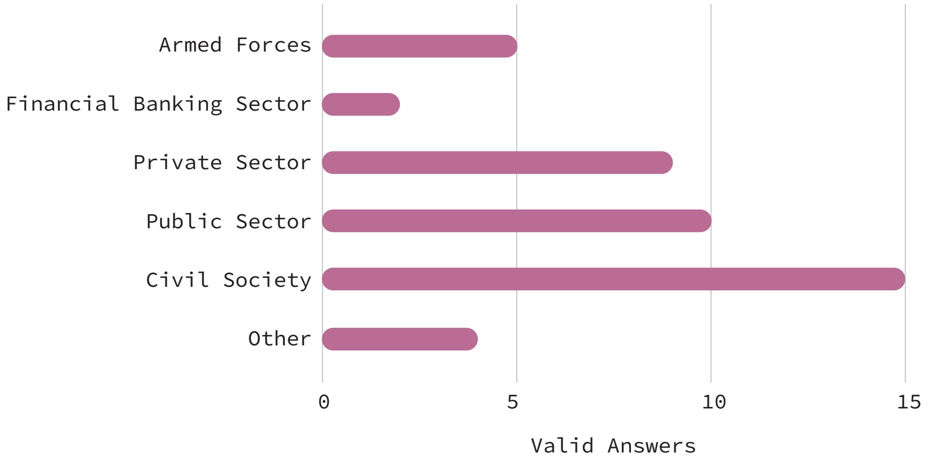
The results of the questionnaire were coded and classified according to Hierarchical Analysis methodology (Analytic Hierarchy Process) to carry out a thematic analysis. After the analysis, we developed an initial list of main recommendations for strengthening mitigation strategies in the country. Once listed, we worked with the multisector group of experts to consolidate and validate the strategies collaboratively.

SUMMARY OF RESPONSES

Sectoral distribution

The questionnaire was sent to 69 institutions representing the following sectors: (I) public, (II) private, (III) Armed Forces, (IV) civil society organizations, (V) financial and banking sector entities and (VI) others. The questionnaire counted on the contribution of 89 responses. From this amount, 45 were valid responses, based on the following sectoral division:

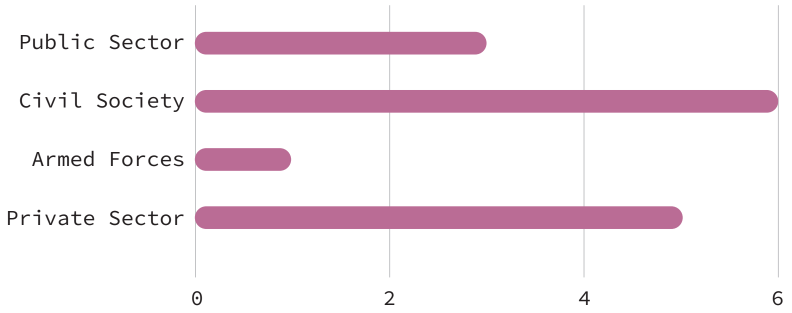
Sector of respondents to the questiomnaire about digital risks in Brazil



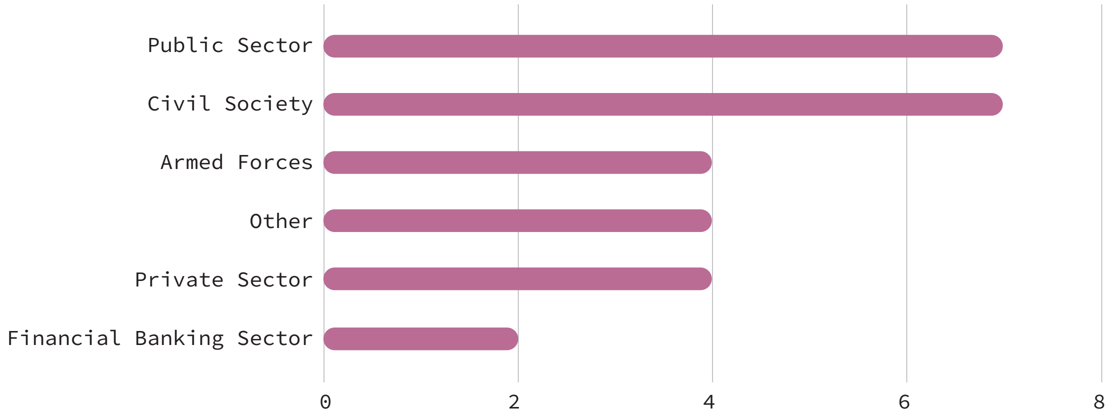
Gender Distribution

Out of the 45 valid responses, 28 were answered by men and 15 by women. The other participants preferred not to inform their gender. These respondents are distributed in the following fields of activity:

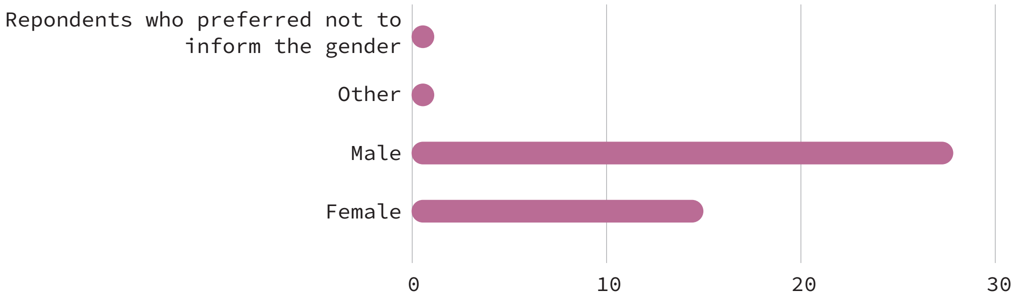
Sector of female respondents of the questionnaire



Sector of male respondents of the questionnaire



Distribution of questionnaire respondents by gender



IGARAPÉ INSTITUTE
a think and do tank

The Igarapé Institute is an independent think and do tank, dedicated to integrating security, development, and climate agendas. The Institute's goal is to propose data-driven solutions and partnerships to global challenges through research, new technologies, and strategic communication. The Institute is a nonprofit, independent and non-partisan institution based in Rio de Janeiro, active in Brazil and across Latin America and Africa. The Institute was ranked the world's best social policy think tank in 2019 by Prospect Magazine, and has been listed among the top 100 Brazilians NGOs since 2018.

Supported by:

British Embassy
Brasilia

Igarapé Institute

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Translation	**Layout**
Daisy Teles	Stephanie Gonçalves

Creative direction
Raphael Durão - STORMdesign.com.br

www.igarape.org.br

IGARAPÉ INSTITUTE
a think and do tank