T20 INDONESIA 2022 THINK

Policy Brief

ENHANCING INTERNATIONAL COOPERATION, DATA GOVERNANCE AND PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL INFRASTRUCTURES AGAINST CYBER THREATS

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Paulo Sergio Melo de Carvalho, Brazilian Center for International Relations (CEBRI)
Hugo Bras Martins da Costa, Sciences Po Paris & State University of Rio de Janeiro

Abstract

This Policy Brief offers three recommendations to the G20 to implement a comprehensive framework for protecting smart critical infrastructures. It highlights the driver role played by inclusive partnerships between the public and private sectors and institutionalized levels of international cooperation, and underline the potential capacity of the G20 Digital Economy Task Force on cybersecurity cooperation to propose to the G20 leaders: 1) promoting public-private partnerships to protect smart critical infrastructures; 2) enhancing institutionalized levels of international cooperation to safeguard smart critical infrastructures; 3) expanding the Digital Economy Task Force focus to include the protection of smart critical infrastructures.

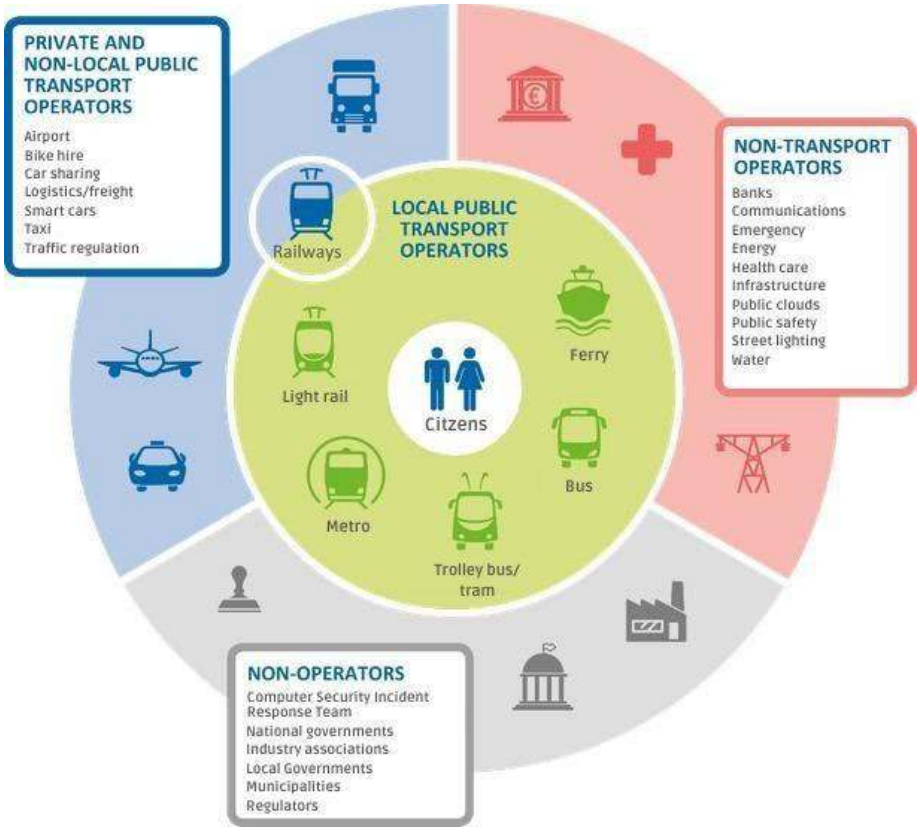
Challenges

The fast-paced digital revolution brought about by integrated technologies and devices in smart cities has generated remarkable improvements in operational efficiency in public services and governance and transparency, as well as has provided a better quality of government service and citizen welfare. However, it has also expanded the cybersecurity landscape to protect smart cities' critical infrastructures.

Critical infrastructures describe the physical and cyber systems, assets, and networks with a strategic dimension that the incapacity or destruction would have a debilitating impact on the economy, society, and environment. According to the Brazilian National Critical Infrastructure Security Strategy, critical infrastructures play a vital role in national security and sovereignty, and sustainable economic development including: communications, energy, public safety, transport, health, finance, and water infrastructures.

Due to the widespread use of intelligent-autonomous technologies in critical infrastructure and the increase in their interconnection and integration with technologies and devices across intelligent cities, recent trends see critical infrastructures migrating toward smart critical infrastructures. In other words, critical infrastructures are even more data-controlled infrastructures based on intelligent-autonomous technologies and devices. They operate even more in cyber-physical systems and exchange data under several schemes with the cyber layer of other critical infrastructures and integrated systems technologies and devices within and across urban cities (Figure 1).

Figure 1: Smart Critical Infrastructures



Source: ENISA, 2017

As a result, cybersecurity experts identify a phenomenal increase in their security surfaces. In traditional cities, cyberattacks could undermine critical infrastructures by either exploiting vulnerabilities or creating the perception that such vulnerabilities exist by exploiting technical or human vulnerabilities. Cyberattacks in smart cities can cause severe damage to critical infrastructures by directly attacking their data-controlled cyber-physical systems based on intelligent-autonomous technologies and devices. They can also cause severe damage by attacking technologies and devices interconnected to them within and across urban cities or exploiting vulnerabilities in the cities' Integrated Command and Control Centre.

Therefore, protecting national critical infrastructures against cyberattacks is a common challenge for most G20 nations who are at the forefront of a fundamental and wholesale transition in intelligent-autonomous and interconnected technologies and devices in operating facilities, services, and assets considered essential for a functioning society and economy.

Proposals for G20

This Policy Brief offers three recommendations to the G20 to implement a comprehensive framework for protecting smart critical infrastructures in both the national and the international spheres by mobilizing the driver role played by inclusive partnerships between the public and private sectors and institutionalized levels of international cooperation, as well as the potential capacity of the G20 Digital Economy Task Force.

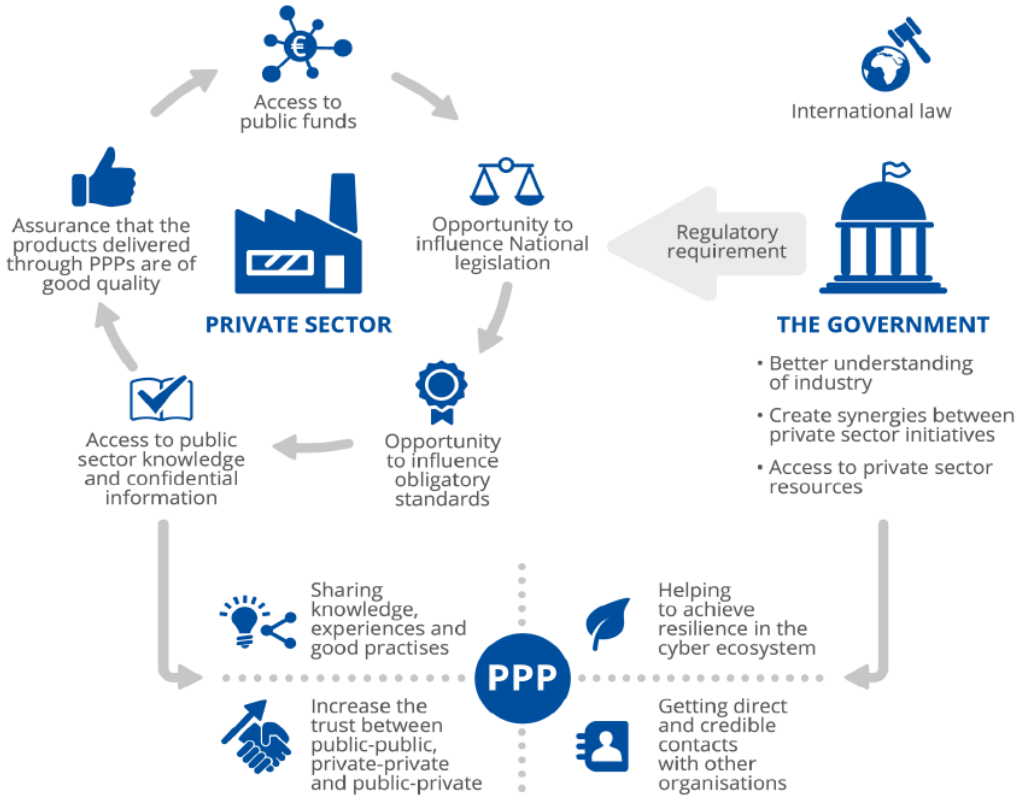
Proposal 1. Promote Public-private partnerships to protect smart critical infrastructures

Protecting smart critical infrastructures is a shared responsibility among multiple stakeholders because neither the government nor the private sector has the knowledge, authority, or resources to do it alone. This tendency has evolved due to the economic liberalization that increased the share of the private sector control over these vital assets, systems, and networks and the private sector's role in developing cutting-edge operational or security technologies used in critical infrastructures, whether public or private.

A public-private partnership is a long-term agreement, cooperation, and collaboration between two or more public and private sectors about private-public teamwork and it includes private-private and public-public relations. In addition to public-private initiatives, this kind of partnership can, thus, foster the agreement, cooperation, and collaboration between either private entities of different economic sectors and within the same industry or state agencies and organizations.

There are multiple reasons for the government and the private companies to create or join the public-private partnership in cybersecurity that ranges from economic interests to regulatory requirements, public relations, and social interests. More specifically, it offers the public sector a better understanding of intelligent critical infrastructures protection, the opportunity to create synergies between different private sector initiatives, and access to private sector resources, which makes it easier to set up standards and good practices. On the other hand, it offers the private sector access to public funds, public sector knowledge, confidential information, and an opportunity to influence general legislation and mandatory standards. Finally, it offers both the public and the private sectors an opportunity to share knowledge, experiences, and good practices, helping entities achieve resilience in the cyber ecosystem and increasing trust by getting direct and credible contacts with other organizations (Figure 2).

Figure 2: Public-Private Partnership on cybersecurity



Source: ENISA, 2017

As a result, public-private partnership in cybersecurity offers considerable contributions to the security and resilience of intelligent critical infrastructure. It delivers effective incident handling, crisis management information exchange, strength, and emergency planning, awareness-raising, and early warnings. It also provides access to research and risks analysis, developing good practices, defining standards and guidelines, and a framework for strategic planning, joint exercises, technical evaluation, help desk, triage, resilience, benchmarking, statistics archiving, and security audit. In a nutshell, public-private partnership in cybersecurity enables both the public and the private sector organizations to meet their particular goals while still benefiting from a high-level cybersecurity network.

Implementing proposal 1

To properly implement the proposal of promoting public-private partnerships to protect smart critical infrastructures, the G20 leaders should:

- First, implement cybersecurity governance of crucial smart infrastructure through the interaction between the public and private sectors and technological research institutes to bridge the gap between cybersecurity experts and decision-makers.
- Increase public and private investment in Science and Technology and promote greater strategic alignment of funding agencies with national cybersecurity policies to address the shortage of cybersecurity professionals and talents in both the public and private sectors.
- Third, promote a collaborative network between the different entities of society so that coordination at multiple levels and sectors could be carried out more intrinsically, taking into account data governance and cybersecurity principles.
- Create regulatory strategies and incentives for greater coordination between companies in the critical infrastructure sector and intersectoral coordination.
- Finally, promote a multistakeholder periodic assessment of the existing data governance systems and management to detect cyber vulnerabilities in essential intelligent infrastructure networks.

Proposal 2. Enhance institutionalized levels of international cooperation to protect smart critical infrastructures

As digital boundaries do not coincide with national frontiers and most critical threats related to cybersecurity derive from international cyberattacks and cybercrimes, protecting smart critical infrastructures demands a sort of action that eludes any State's sovereignty. In other words, preserving intelligent vital infrastructure against cyberattacks that are constantly proliferating, shifting in focus, and exploiting opportunities worldwide, implies ensuring solid and institutionalized levels of international cooperation.

Although it may happen often, international cooperation does not only mean mutual aid among governments and institutions from different countries. International cooperation is a fundamental political field of international relations and a polysemic word that refers to several related terms and concepts, such as official international aid and technical cooperation among states. It means governments and institutions develop common standards and create programs that consider benefits and problems extended to more than one nation.

More specifically, international cooperation refers to an institutionalized sphere of action of states' foreign policies to rich shared objectives through a mutually agreed variety of practices, such as: public and private grants, debt-generating loans and financing, international public-private partnerships, and multi-financier funds, training for governmental officials and civil servants of public institutions, development, diffusion, and dissemination of good practices, technical skills and know-how, and transferring of technology. Since its inception, international cooperation incrementally followed domestic social policies and the modernizing reforms of

their public administrations and has extended to all areas from trade and finance to security, environment, education, and health issues. In addition, the proliferation of so-called new actors in this field of international relations broke the States' monopoly in international cooperation.

In cybersecurity, international cooperation contributes to the capacity building of the fundamental regulations, human resources, and technical mechanisms for an appropriate dynamic and coordinated response to cyber incidents and cybercrimes. It also offers access to cutting-edge research, knowledge, and analysis. Furthermore, it facilitates the transfer of advanced technologies on mutually agreed terms, expanding its frontier at the global level rather than holding back its development or controlling such technology for fear of its potential abuse, promoting international asymmetries and inequalities. In addition, international cooperation is also a catalyzer of additional financial resources for capacity building, technology development or acquisition, and policy implementation. Finally, it also fosters a shared global understanding and builds confidence among nations while appreciating their diverse values in terms of cybersecurity.

It is essential to highlight that international cooperation can also significantly contribute to addressing the main gaps between the policy and the political and operational requirements for implementing and developing public-private partnerships in cybersecurity. By facilitating technical know-how and technology development and transfer, and mobilizing the public and private sector and research institutes, civil society organizations, and foreign partners experts, international cooperation can offer additional human resources to public-private partnerships. Catalyzing access to other financial resources, international cooperation can also provide a supplementary budget to guarantee the necessary money for developing public-private partnerships and their continuity in the long term. By ensuring the essential trust and political-legal coordination among domestic actors within states, international cooperation can contribute to overcoming the distrust between public-private, private-private, and public-public entities to create a public-private partnership in cybersecurity and to maintain it. Finally, it can contribute to overcoming the lack of a legal basis to establish the limits of each public and private organization's roles and responsibilities in the partnership.

Implementing proposal 2

To properly implement the proposal of enhancing institutionalized levels of international cooperation to protect smart critical infrastructures, the G20 leaders should:

- Foster trust-building between national governments through transparency on cybersecurity threats, early warnings on cyber risks and cyber incidents, and best practices exchange;
- Express the urgency of the protection of intelligent critical infrastructure against cyberattacks;

- Promote consensus building on the topics of cybersecurity that G20 countries can agree on standard definitions, despite the lack of consensus on what exactly constitutes cyberwarfare or cyberterrorism, as well as on the complete application of existing international laws to cyberspace;
- Commit non-proliferate advanced persistent threats to another state's smart critical infrastructures.

Proposal 3. Expand the focus of the G20 Digital Economy Task Force to include the protection of smart critical infrastructures

The Group of Twenty (G20) assembles the most relevant nations in terms of GDP, trade, and demography at the forefront of the digital transition and the development of national cybersecurity technologies and policies. In this regard, it has a Digital Economy Task Force to propose a common understanding, principles, and critical areas for development and cooperation in the digital space. However, since its creation in 2016, the Digital Economy has focused almost exclusively on the agendas of equitable connectivity, digital innovation, and promotion of investments in information and communication technologies. Hence, the G20 has failed to pay enough attention to cybersecurity cooperation, particularly in the security of smart critical infrastructures.

As a multilateral platform with a strategic role in securing future global economic growth and prosperity, the G20 agenda cannot neglect the critical role of cybersecurity as an enabler of sustainable economic development in the fast-paced transition to a digital economy. Data flow and intelligent-autonomous technologies hold tremendous potential to bolster economic growth in the following decades and improve operational efficiency in public services, governance, and citizens' welfare. However, their adoption and diffusion cannot be accelerated unless cybersecurity concerns are addressed.

Although the G20 is neither a multilateral organization nor a homogeneous grouping of states, as an informal forum that connects the world's major developed and emerging economies, it has some leverage in discussing proposals and reaching commitments for a framework for cybersecurity cooperation. In this regard, the G20, in partnership with regional and universal multilateral organizations, should expand the focus of its Digital Economy Task Force to include the protection of smart critical infrastructures.

Implementing proposal 3

To properly implement the proposal of expanding the focus of the Digital Economy Task Force to include the protection of smart critical infrastructure, the G20 leaders should:

- Add the protection of intelligent critical infrastructure in the priority areas of the G20 Digital Economy Task Force;
- Promote a discussion session on the protection of smart critical infrastructure during the G20 Digital Ministerial Meeting;

- Establish a collaborative dialogue of the G20 Digital Economy Task Force with the sherpa forums of the G20 (i.e., the Infrastructure, Trade, Investment and Industry, Health and Agriculture Working Groups), and key engagement groups of the G20 (i.e., the Business 20, Urban 20, Think Tank 20, Science 20, Civil 20 and Parliament 20);
- Prioritize the promotion of international cybersecurity cooperation and public-private partnerships on the working agenda of this new priority area of the G20 Digital Economy Task Force.

Conclusion

The G20 assembles the major global economies and societies that are at the forefront of digital transition and in which intelligent-autonomous technology plays an increasingly vital role. It also plays a leading role in international development cooperation in the domain of intelligent-autonomous technologies. However, G20 countries are confronted with considerable challenges to increase international cooperation in order to mobilize and redirect the much-needed transformative power of reviewing and monitoring frameworks, regulations, and incentive structures to strengthen cybersecurity in national critical infrastructures in this new era of indispensable coexistence with intelligent-autonomous technologies.

This Policy Brief offers three recommendations to the G20 to implement a comprehensive framework for protecting smart critical infrastructures. It highlights the driver role played by inclusive partnerships between the public and private sector and institutionalized levels of international cooperation, and underline the potential capacity of the G20 Digital Economy Task Force on cybersecurity cooperation to propose to the G20 leaders: 1) promoting public-private partnerships to protect smart critical infrastructures; 2) enhancing institutionalized levels of international cooperation to safeguard smart critical infrastructures; 3) expanding the Digital Economy Task Force focus to include the protection of smart critical infrastructures.

References

Carvalho, P. (2020). *Os constantes desafios em segurança cibernética nas organizações como parte da estratégia dos negócios*. CEBRI Report. Available at: https://www.cebri.org/br/doc/30/seguranca-cibernetica-nas-organizacoes-como-parte-da-estrategia-dos-negocios

Carvalho, P. (2020). Segurança Cibernética e Redes Privadas 5G no Brasil. CEBRI Report. Available at: https://www.cebri.org/br/doc/29/seguranca-cibernetica-e-redes-privadas-5g-no-brasil

Carvalho, P. (2020). *A segurança cibernética e a tecnologia 5G no cenário brasileiro*. CEBRI Policy Paper. Available at: https://www.cebri.org/br/doc/28/a-seguranca-cibernetica-e-a-tecnologia-5g-no-cenario-brasileiro

BRASIL (2020). DECRETO Nº 10.569, DE 9 DE DEZEMBRO DE 2020: Estratégia Nacional de Segurança de Infraestruturas Críticas. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm

ENISA. (2017). *Public Private Partnerships (PPP): Cooperative models*. Available at: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

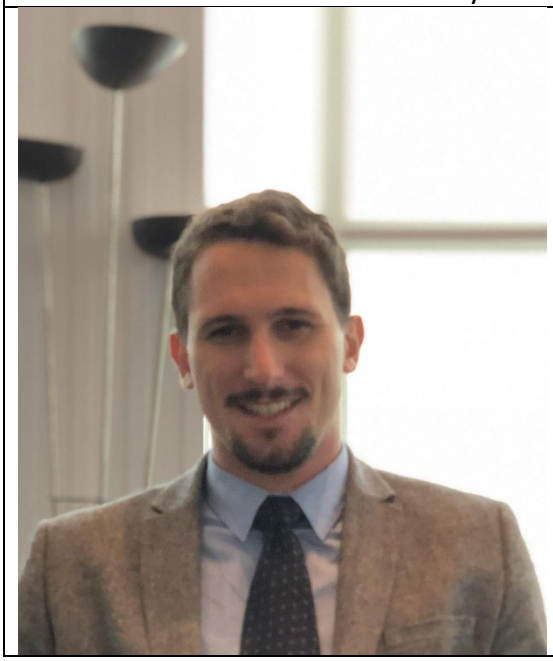
ENISA. (2013). *Cybersecurity cooperation: Defending the digital frontline*. Available at: https://www.enisa.europa.eu/news/enisa-news/securing-the-cyber-frontline-enisa-report-highlights-need-for-cooperation

About the Authors

Paulo Sergio Melo de Carvalho
Brazilian Center for International Relations (CEBRI)

Paulo Sérgio Melo de Carvalho is a reserve Lieutenant General for the Brazilian Army. He is a specialist in Information Technology and Communications and has acted in the cybernetics area at the political/strategic and operational/technical levels, having headed the Cybernetic Defense Center between 2014 and 2016 and becoming the first commander of the Cybernetic Defense Command, created in 2016. Currently, he is a consultant for the cybernetic sector and participates in human resources capacitation, in Brazil and abroad.

Hugo Bras Martins da Costa
Sciences Po Paris & State University of Rio de Janeiro



Hugo Bras Martins da Costa is a PhD in Political Science in a joint thesis program between the Institute of Social and Political Studies at the Rio de Janeiro State University (IESP-UERJ) and Sciences Po Paris. He is also Enseignant Vacataire de Sciences Po Paris and Associate Researcher at the Laboratory of World Political Analysis (Labmundo) of IESP-UERJ. Between 2020 and 2022, he was Project Coordinator of the Brazilian Center for International Relations (CEBRI). His contact e-mail is: hugobrasmartinsdacosta@gmail.com