Mapping the World's Critical Infrastructure Sectors

Weber, Valentin; Pericàs Riera, Maria; Laumann, Emma

Veröffentlichungsversion / Published Version
Stellungnahme / comment

No. 35
November 2023

DGAP POLICY BRIEF

Mapping the World's Critical Infrastructure Sectors

Valentin Weber
Senior Research Fellow, Center for Geopolitics, Geoeconomics, and Technology

Emma Laumann
Student Research Master Social Sciences, University of Amsterdam

Maria Pericàs Riera
Project Assistant, Center for Geopolitics, Geoeconomics, and Technology

This paper examines the policy documents of 193 United Nations member states and Taiwan. It analyzes what countries perceive as critical infrastructure (CI). While it may at first appear clear what CI sectors are, e.g., energy, education, water, and food, this view varies by member state. By mapping what countries designate as their critical infrastructure sectors, we hope to propel UN cyber discussions, which have so far been slow to result in agreement on a global common denominator for critical infrastructure sectors.

– 100 of 194 countries have published what they perceive as CI sectors. The CI sectors that countries most frequently mention are energy (96%), information and communications technology (ICT) (95%), transport (93%), economy and finance (89%), public services (84%), and health (83%).

– By far the least-mentioned categories worldwide are research and education (15%), national security (45%), food (51%), and water (76%).

– If it were only a numbers game, the most common CI could be included in a global definition. A more inclusive approach would name all the above sectors as CI at the UN.

– Many countries need further support in defining CI (see Appendix C). While almost all countries in Europe and North America define CI sectors, Asia, Latin America, and Oceania are far behind.

INTRODUCTION

No common definition of critical infrastructure (CI) exists among the 193 UN member states and Taiwan. In fact, there are at least 100 different national positions on the subject. Many countries lack lists of their CI or critical information infrastructure (CII) sectors, including two in Europe (Monaco and San Marino). Because 94 countries have still not defined their CI, the 2023 annual progress report of the Open-Ended Working Group on information and communication technologies (OEWG II) notes that "[s]tates also proposed to support developing countries and small States, in their identification of national CI and CII, where requested."[1]

It is crucial to establish a common global denominator as to what is or is not CI. States are bound under international law not to attack CI (in and outside cyberspace) and have also agreed on a voluntary, non-binding norm on refraining from malicious information and communications technology (ICT) activity against CI in cyberspace during peacetime.[2] Thus, knowing what other states perceive as CI is important to reduce the likelihood of misperception and escalation. So how can countries agree on a global denominator?

While all CI is off-limits for both cyber- and conventional attacks in peacetime according to international law, CI in cyberspace needs additional protection. In a previous paper, one author argued that specific CI sectors (electrical grid, early warning satellites, and nuclear command and control systems) need to be protected from all cyber operations. This means that not only attacks should be banned, but also espionage and the placement of logic bombs – malicious code in software triggered by certain conditions. These special protections are needed because those three sectors are the most important CI of all. Cyber operations against such entities could lead to disastrous misperceptions, i.e., countries (mis)perceiving that other countries are preparing for war.[3]

This paper takes a complementary and broader approach to the previous paper, which focused exclusively on the cyber context and on deepening the UN norm on not attacking critical infrastructure. In contrast, this paper creates a global database with countries' different definitions of sectors they perceive as CI. While not all countries have an official document laying out their CI sectors, 100 countries do. This allows us to analyze which sectors appear quite often and which do not. It also permits us to compare which sectors are perceived as CI in various regions of the world and, finally, to find similarities across countries.

While this paper does speak to the cyber diplomacy community, which aims to protect CI from cyberattacks, it is not limited to this community. Having a global and common definition of CI is valuable for policy makers outside the cyber field, since the offline and online worlds have merged in recent years. There is no CI sector that is not connected in one way or another to the internet. The protection of CI from both cyber and conventional attacks must be tackled together. There has not yet been a serious attempt at UN cyber negotiations to agree on a comprehensive definition of CI. Current definitions at the UN OEWG on international cybersecurity have been quite arbitrary and have changed over time.[4] They have also not striven to be comprehensive. So no process is in place yet that would try to assemble countries' definitions of CI sectors. This may be because some countries fear that anything that falls outside their CI definition could become a target for cyber operations.

However, this is misguided. This paper does not suggest that the Bahamas, Bolivia, or Madagascar should publish detailed lists of where critical water supply networks or industry facilities lie. This paper rather aims to nudge countries toward publicly naming broad lists of CI sectors that would be abstract and would not provide concrete targets.

Furthermore, countries publicly listing their CI sectors have not been more frequently attacked than those that have not yet defined CI. To the contrary, countries that have codified CI sectors have been better at establishing measures to protect CI. The European Union's NIS and NIS2 directives are examples of such regulations that improve CI protection. Without a definition of CI, protection is not possible.

1 p. 6.

2 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "UNGGE Report," 2015: https:// documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf? OpenElement; Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, "OEWG I Final Substantive Report," 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290- 2021-CRP.2.pdf (both accessed November 03, 2023).

3 Valentin Weber, "Political Declaration Between EU Member States, the United States of America, and the People's Republic of China on Protecting Select Critical Infrastructure from Cyber Threats During Peacetime," German Council on Foreign Relations (September 2023) https://dgap.org/sites/default/files/Fictional_Draft_Declaration_on_CI_DGAP_26092023.pdf (accessed November 03, 2023).

4 Ibid.

Past and current UN processes usually aim to find consensus on a certain topic by encouraging countries to submit their national views – e.g., on international law or progress in securing CI – to a UN platform or to voice them when diplomats gather for substantial sessions of UN working groups. In this vein, it took more than a decade to define a norm calling for countries to refrain from attacking CI via cyber means. This paper aims to speed up the process of arriving at a global and common understanding of critical infrastructure.

METHODOLOGY

The study examines the CI sectors of 193 United Nations member states[5] and Taiwan. These states are regionally categorized in accordance with the guidelines set forth by the United Nations Statistics Division.[6][7]

The worldwide categorization of CI is based on extensive research. The authors analyzed official documents, including national security strategies, laws and ministry websites. The study draws exclusively on open-source data. Despite the considerable research effort, country classifications may have been overlooked or published after the authors concluded their evidence-gathering in November 2023. It is the authors' aim to add missing data in future iterations of the dataset.

There is a lack of standardized terminology in designating CI and the sectors that fall into it. While the term critical infrastructure is commonly used, countries also use variations, such as "activities of vital importance" in France or "crucially important facilities" in Belarus. And there is a diverse spectrum of classifications for CI sectors such as public services, based on how individual countries define them. This encompasses everything from emergency services to administration, waste disposal, government, cultural heritage, and tourism.[8] Other CI sectors are more straightforward. Energy and ICT are relatively easy to classify due to the extensive overlap of terminology in the countries examined.

While compiling the dataset, the authors conducted a thorough analysis to identify the most frequently recurring categories of CI. They identified ten categories: energy, ICT, transport, health, food, water, public services, economy and finance, research and education, and national security.

Additionally, the authors listed some sectors several times. For example, Poland lists "health transport rescue" as a sector. They classified this both as transport and health. Another example is food and water, which appears in both food and water categories in this study, despite being considered a single category in some countries.

What is more, numerous countries lack English versions of their public documents. In these cases, the translations were made by the researchers themselves or by using online translation tools.

While this dataset is the first to provide an up-to-date and global overview, other repositories have been useful in this research. Those are the UNIDIR Cyber Policy Portal,[9] which provides documents including cybersecurity policies and legal frameworks, and the OECD, which presents a list of member countries and their CI sectors.[10]

FINDINGS

The Number of Countries Defining CI Varies Greatly by Region

More than half of the countries worldwide have an official list that defines national CI sectors. However, a closer look shows that the way CI sectors are described varies among regions. In Europe, 95% (42/44) of the countries studied have an established list. In North America, which includes Canada and the United States, 100% have such a list, while only 42% (14/33) of those in Latin America and the Caribbean do. Asia comes in at 49% (23/47) and Oceania at 29% (4/14). The region where the fewest countries have a list of definitions is Africa, with 28% (15/54).

5 United Nations, "Member States," https://www.un.org/en/about-us/member-states

6 https://unstats.un.org/unsd/methodology/m49/ (accessed November 22, 2023)

7 While UNSTATS categorizes Cyprus as an Asian country, this study has chosen to classify it as part of Europe due to its membership in the European Union.

8 The CI Sector, as defined and labeled int official government documents can be found in Appendix B.

9 UNIDIR, "Cyber Policy Portal", https://cyberpolicyportal.org/ (accessed November 22, 2023)

10 OECD, "Reviews of Risk Management Policies: Good Governance for Critical Infrastructure Resilience," 2019: https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en#:~:text=Overall%2C%20six%20sectors%20are%20widely,%2C%20health%2C%20transport%20and%20water (accessed November 3, 2023)

Table 1 – Percentage of countries that publicly define CI sectors

REGIONS	NUMBER OF COUNTRIES WITH LIST OF CI SECTORS	TOTAL NUMBER OF COUNTRIES	PERCENTAGE OF COUNTRIES WITH CI SECTORS IN EACH REGION
Europe	42	44	95%
North America	2	2	100%
Latin America and the Caribbean	14	33	42%
Africa	15	54	28%
Oceania and Australia	4	14	29%
Asia	23	47	49%
Global	100	194	52%

Source: Authors' own compilation

Several African countries have not yet defined their specific critical sectors and are aiming to do so in the coming years. Often these aims are part of the effort to draft and implement a national cybersecurity strategy. Mauritania is one such example.

GLOBAL ALIGNMENT OF SECTORS

Among the countries with specified sectors, the category incorporated by nearly all is energy (96%). This is followed by ICT (95%) and transport (93%), while economy and finance, public services, and health also scored above 80%.

In Europe, all 42 countries listed energy as a critical sector. In Africa, among the fifteen countries that define CI sectors, all include ICT. For Asia, this was the case with energy and economy and finance. In Asia, Jordan did not include a public services sector. ICT and transport were left out by Qatar.

Compared to other regions, Latin America stands out as the only place worldwide where energy holds the third position. As mentioned above, in all other regions, energy consistently occupies the top spot or shares it with another critical sector.

For this study, North America is comprised of only two countries. It is therefore a special case, as both the US and Canada cover 9 sectors, therefore a top three cannot be given. The only sector not considered critical by the US and Canada is research and education. It should be noted that the US does incorporate this category as a sub-sector, but this was not included in the overall analysis.

The least-mentioned category in all regions is research and education, named by only 15% of all countries. On the African continent, 27% of the countries included this category. This is significantly higher than Europe (12%) and Asia (13%). Other categories that scored low globally are national security (45%), food (51%), and water (76%).

Regional Specificity:

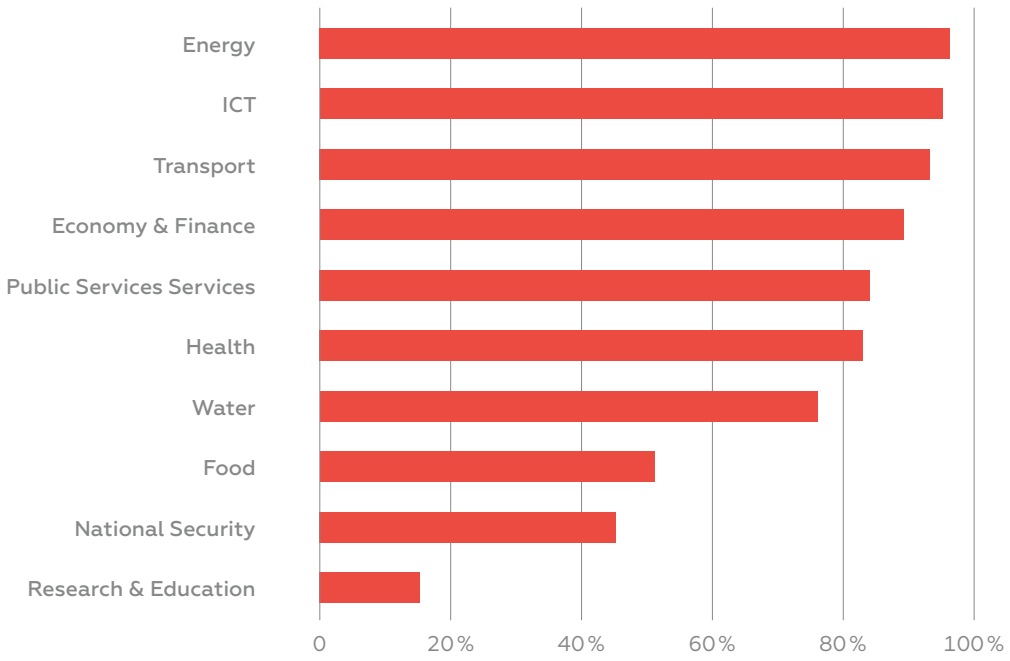
- **Asia:** Globally, 51% of countries include food as a category in their CI lists. In Asia, however, out of the twenty-three countries with CI sectors, only five (22%) feature this category. Those are: Israel, Kyrgyzstan, Malaysia, Oman, and the United Arab Emirates.
- **Africa:** Democratic Republic of the Congo, Ghana, Kenya, and Nigeria were the only African countries to list research and education as a category of CI.
- **Europe:** Russia includes "Russian legal entities and individual entrepreneurs who own information systems" and "Russian legal entities and/or individual entrepreneurs that ensure the interaction of these systems and networks" as critical sectors.

Table 2 – Percentage of countries that officially define energy, ICT, and transport as CI sectors

REGIONS	1. ENERGY	2. ICT	3. TRANSPORT
Europe	100%	90%	95%
North America	100%	100%	100%
Latin America and the Caribbean	86%	100%	93%
Africa	87%	100%	80%
Oceania and Australia	100%	100%	100%
Asia	100%	96%	96%
Global	96%	95%	93%

Source:Authors' own compilation

Chart 1 – Inclusion of specific sectors (in %) among the 100 countries that have published lists of CI sector



Source: Authors' own compilation

- **North America:** The United States lists the defense industrial base as critical, including overseas entities.
- **Latin America and the Caribbean:** Environmental elements are seen as essential components of critical infrastructure. Globally, this CI is mentioned only by very few countries. In the case of Brazil, a focus on biosafety and bioprotection stands out, reflecting a commitment to safeguarding biological resources. Likewise, Ecuador places significant importance on the preservation of its rich biodiversity and genetic patrimony.

CONCLUSIONS

The aim of this article was to shed light on what countries view as CI sectors. There are several main conclusions that can be drawn from this analysis.

First, many countries, particularly in Asia and Africa, are still working on the categorization of their CI sectors (see Appendix C). While this trend shows a growing awareness of the importance of safeguarding vital systems, it also reflects that 94 countries still have not defined their CI sectors nor have response plans to protect them. It is the international community's task to support those member states in defining and protecting their CI.

Second, the efforts of countries that have already defined their CI sectors can help foster a common global alignment. While each nation may have specific needs, the pursuit of a common global understanding of CI could result in significant benefits. Such an approach could lead to improved international cooperation, information sharing, and the development of best practices for protecting CI on a global scale.

This policy brief answered the "what" questions of CI: what countries define CI and what those definitions look like. This is especially useful to gain an understanding of what countries mean by broad terms such as ICT. Some countries say it is submarine cables, others satellite communication; for Russia it is Russian legal entities and individual entrepreneurs who own information systems; for others it is broadcast media or the digital economy. The variety of definitions captured in this paper is even broader when it comes to public services, encompassing everything from sensitive organizations to urban areas, national monuments and values. A key goal in writing this paper was to go beyond assumptions as to what CI is and to provide facts. Countries can use the global overview to add CI sectors they have omitted, but which other countries have on their lists, and exchange information with them as to how to best protect those sectors.

But there is more to studying CI than compiling what countries perceive as CI. There are many more "why and how" questions for future research. Why do countries publish CI lists at a certain point in time? Is it because they have been attacked recently and need to double down on CI protection? Australia, for instance, added telecommunications companies to its existing list of CI in 2023.[11] This was a direct reaction to a large hack telecommunications companies in Australia suffered in 2022. Adding telecommunications companies to the list of CIs not only puts ink on paper, it also creates new rules with stricter security procedures for this CI sector, which will be enforced by the Australian government.

Why some countries and not others? While the authors chose not to study those that have not codified CI, one explanation for the lack of codification may be that many countries simply do not have the resources to establish CI regulation. It might also be that certain regional organizations have not been nudging countries in this direction, as for example the EU has done. Another question for future research is, for example, why certain countries include national security in their strategies and why others omit food or water.

Many of these questions may be answered by further research. But alongside in-depth analyses by researchers, states themselves should also establish their own initiatives. Those that have published their lists of CI sectors should push for global standards regarding CI definitions and CI protection. As they have already set standards by publishing lists, they have a first mover advantage and could decisively shape global discussions on this issue.

11 ABC NEWS, "Telcos Required to Report on Cybersecurity Measures in Bid to Prevent Repeat of 2022 Optus Hack," 2023: https://www.abc.net.au/news/2023-11-13/cyber-law-changes-after-optus-dp-world-hack/103096906 (accessed November 22, 2023)

APPENDIX A:

Table 3 – Regions and their CI sectors

Regions	Europe	North America	Latin America & the Caribbean	Africa	Oceania & Australia	Asia	Global
Number of Countries	44	2	33	54	14	47	194
Number of Countries with lists of CI	42	2	14	15	4	23	100
Energy	42	2	12	13	4	23	96
ICT	38	2	14	15	4	22	95
Transport	40	2	13	12	4	22	93
Health	36	2	12	12	2	19	83
Food	28	2	6	8	2	5	51
Water	33	2	10	11	3	17	76
Public Services	35	2	10	13	2	22	84
Economy & Finance	37	2	11	13	3	23	89
Research & Education	5	0	2	4	1	3	15
National Security	17	2	8	7	1	10	45

Source: Authors' own compilation

APPENDIX B: DESIGNATIONS GIVEN TO CI BY COUNTRIES AND OUR CATEGORIZATION OF THEM

1. Energy: Energy; electricity; electric power; natural gas; gas; oil; petroleum products; oil and gas infrastructure; energy facilities and networks; supply of energy; energy resources and fuels; fuel and energy complex; non-renewable natural resources; electric transmission; energy and utilities; nuclear reactors; materials and waste; electronic power supply; heating; electricity and water.

2. ICT: ICT; telecommunication; electronic communication; communications and information technology; digital infrastructure; information systems; client and patient information systems; audiovisuals and information; IT; communications ICT networks; information and communication networks and systems; satellite communication; Russian legal entities and individual entrepreneurs who own information systems; information society services; digital economy; electromagnetic spectrum and geostationary orbit; radio electric spectrum; telephony; key databases; fiber optic cable; submarine cables; telecommunication transmission hubs; telecommunication lines; posts; data centers; communications; data storage and processing sector; public communication; electronic information; broadcast media; information, communication, science and technology.

3. Transport: Transport; traffic; transportation; postal service; transport infrastructure; transportation and refining of hydrocarbons; public transportation; transportation systems; air transport; civil aviation; aviation; various forms of transportation; transportation sector; land transport; maritime transportation system; freight transport; air and sea transport; three-waters; transport (land, sea, air); port and airport development; health transport rescue; aviation; railway; roads; road, air, land, maritime, port, or railway connection.

4. Health: Health; healthcare; public health; health transport rescue; medical and care services; public health; rescue services; accident control; life-support systems; national public health and safety; healthcare facilities; medical sector; emergency aid and hospitals.

5. Food: Food; agriculture; food supply; food and water; food and agriculture; food products; financial food supply; food security and safety; forestry and water management; food industry; beverage services; grocery sectors; agriculture and plantation.

6. Water: Water; drinking water supply and distribution; water supply and distribution; water management; water supply; food and water; wastewater; electricity and water; water supply and environmental sectors; supply and distribution of potable water; water, forests, and environment; dams; supply and distribution of drinking water; treatment of non-potable water; water and sanitation sector; water and sewerage; water conservancy; waterworks; energy sector and electricity and water.

7. Public services: Public services; social services; postal and courier services; justice, public order, and security; state and social administration; regional development and public works; environment; cultural heritage; disaster protection; sports venues and facilities; production, storage, and transportation of dangerous substances; national monuments and values; security services; emergency services; public administration; state agencies; waste management; civil activities of the state; judicial activities; municipal waste disposals; state and administration; media and culture; law and government; public safety; national security; policing and public safety infrastructure; civil administration; government; public security and law enforcement; state governance; public order and safety; digital government; production storage and use of chemical and radioactive substances; administration; culture and national cultural heritage; mail; environmental protection; municipal technical services; social infrastructure; waste disposal; cultural objects; places of mass agglomeration; state authorities; services of the government; ecology; state bodies; state institutions; Russian legal entities and/or individual entrepreneurs that ensure the interaction of these systems and networks; public goods; authorities; public safety; civil protection of the population and territories; biosafety and bioprotection; national monuments and cultural heritage; administrative entities of all branches of government and of the different levels of government; biodiversity and genetic patrimony; postal and shipping entities; public safety; tourism and heritage sites; postal and shipping entities; civil protection; tourism; and heritage sites; e-government; public regalian administration; logistics; government installations; provincial and municipal governments; public key infrastructure; essential emergency services and criminal law enforcement; law enforcement; e-governance; sensitive organizations; electronic government services; natural resources; social order and safety; urban areas; governments direction and administration.

8. Economy and finance: Economy and finance; financial services; financial market and currency; finance; production, storage and transport of dangerous goods; industry; insurance; banks; stock market infrastructure; industry; banking services; financial market infrastructures, financial market institutions; finance payment operations; finance cash supply; finance operations of the state budget; finance and tax system, chemical industry; finance services; trade and industry; engineering; insurance services; financial; chemical, biological and nuclear industry; property; state registration of rights to real estate and transactions with IT; banking and other areas of the financial market; mining; metallurgical and chemical industry; international trade; trade; manufacturing; catering; commercial facilities; critical industry; custom centers; budgeting; high-tech parks.

9. Research and education: Research; education, science and technology; space; research facilities; academic sector; educational institutions; higher education and research.

10. National security: Space; defense; maritime; military activities of the state; space and research; national defense; nuclear; national security; protection; safety and security; rockets and space; civil nuclear; national or economic security; defense and industrial base; military sector; security, defense or international relations; space technology; defense industry; security and intelligence services; public security.

APPENDIX C:
LIST OF COUNTRIES THAT HAVE NOT YET PUBLISHED LISTS OF CI SECTORS

Afghanistan
Algeria
Angola
Antigua and Barbuda
Armenia
Azerbaijan
Bahamas
Bangladesh
Bhutan
Bolivia (Plurinational State of)
Brunei Darussalam
Burundi
Cambodia
Cameroon
Central African Republic
Chad
Comoros
Congo (Republic)
Costa Rica
Côte D'Ivoire
Cuba
Democratic People's Republic of Korea
Djibouti
Dominica
Dominican Republic
Equatorial Guinea
Eritrea
Eswatini
Ethiopia
Fiji
Gabon
Georgia
Grenada
Guatemala
Guinea
Guinea Bissau
Guyana
Haiti
Honduras
Iran (Islamic Republic of)
Iraq
Lao People's Democratic Republic
Lebanon
Lesotho
Liberia
Libya
Madagascar
Malawi
Maldives
Mali
Marshall Islands
Mauritania
Micronesia (Federated States of)
Monaco
Mongolia
Morocco
Namibia
Nauru
Nepal
New Zealand
Nicaragua
Niger
Palau
Panama
Paraguay
Rwanda
Saint Kitts and Nevis
Saint Vincent and the Grenadines
San Marino
Sao Tome and Principe
Saudi Arabia
Senegal
Seychelles
Solomon Islands
Somalia
SouthSudan
Sri Lanka
Sudan
Suriname
Syrian Arab Republic
Tajikistan
Timor-Leste
Togo
Tonga
Tunisia
Turkmenistan
Tuvalu
United Republic of Tanzania
Uruguay
Uzbekistan
Vanuatu
Yemen
Zambia
Zimbabwe

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Ellen Thalman

Layout Lara Bührer

Design Concept WeDo

Author picture(s) © DGAP