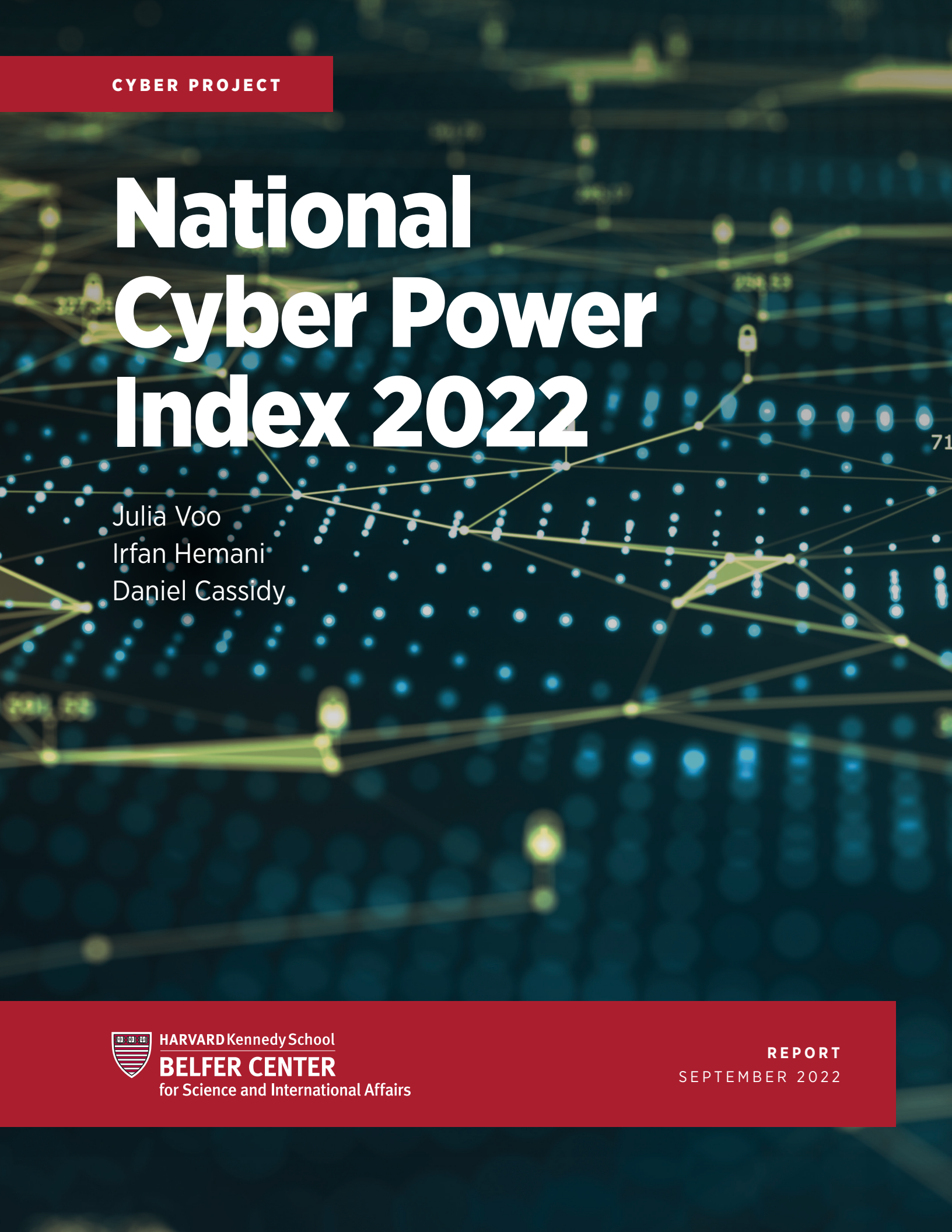

CYBER PROJECT

National Cyber Power Index 2022

Julia Voo
Irfan Hemani
Daniel Cassidy

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
SEPTEMBER 2022

Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/project/cyber-project

CYBER PROJECT

National Cyber Power Index 2022

Julia Voo
Irfan Hemani
Daniel Cassidy

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
SEPTEMBER 2022

About the Authors

Julia Voo is a Cyber Fellow and leads the team behind Belfer's National Cyber Power Index. She was formerly the Research Director for the China Cyber Policy Initiative. Julia previously served at the British Embassy in Beijing where she covered China's cyber and AI policy from a commercial perspective, technical standards, and other trade policy issues.

Irfan Hemani is a Deputy Director for Cyber Policy at the UK's Department for Digital, Culture, Media and Sport, responsible for secure technology policy as part of the UK's new National Cyber Strategy. He previously worked in Deloitte's Technology Risk Advisory team.

Daniel Cassidy is a strategy and security professional who is currently a director at Dartkite, a consultancy firm specializing in using data to support strategy and policy decision making, particularly related to cyber and cyberspace. He previously worked for the UK Government and the EU as an expert in strategy and crisis management, and a wide range of issues including arms control, applied research and migration.

Acknowledgments

We would like to thank the many national governments, academic experts and security organizations that have contributed their time and effort to engage with the Belfer team as the 2022 iteration of the National Cyber Power Index has evolved.

We would also like to thank Anina Schwarzenbach for her support with the calculation of the ranking itself, Andrew Webster and Angela Zhong for their support as Research Assistants extraordinaire. All have made a valuable contribution to the methodology, data gathering and many debates that have been held over the last two years.

In addition, we would like to thank Lauren Zabierek, Bruce Schneier, and Winnona DeSombre for their feedback on earlier drafts of this study.

About the Cyber Project

Forty years ago, an interdisciplinary group of Harvard scholars – professors, researchers and practitioners – came together to tackle the greatest threat of the Cold War: the fear of a nuclear exchange between the Soviet Union and the United States. Today, we seek to recreate that interdisciplinary approach to tackle a new threat: the risk of conflict in cyberspace. The problems that confront today's leaders are substantial and diverse: how to protect a nation's most critical infrastructure from cyberattack; how to organize, train, and equip a military force to prevail in the event of future conflict in cyberspace; how to deter nation-state and terrorist adversaries from conducting attacks in cyberspace; how to control escalation in the event of a conflict in cyberspace; and how to leverage legal and policy instruments to reduce the national attack surface without stifling innovation. These are just a sample of the motivating questions that drive our work. The aim of the Belfer Center's Cyber Project is to become the premier home for rigorous and policy-relevant study of these and related questions.

A Note to Readers

The Belfer Center's mission is to provide leadership to advance critical policy-relevant knowledge of important international security issues. The release of the National Cyber Power Index in 2022 does just that. Over the past two years, the NCPI has catalysed conversations and debate between policymakers, academia, and industry on the concept of cyber power and how states are and can further harness their capabilities to enhance their overall ability to achieve national objectives.

Harnessing a state's cyber power requires a whole-of-nation approach. National governments should not just be concerned about destructive operations, espionage, or enhancing its cyber resilience, but also other state's efforts at surveillance, information control, technology competition, financial motivations, and shaping what is acceptable and possible through norms and standards.

During my time in the US Government, I sought and applied analytical methods to assess cyber threats to US national security. With the challenges in the cyber domain only increasing, it is critical for analytical tools to also be available, presenting the full range of cyber power, and informing critical public debates today. The framework that the NCPI provides is one that allows policy makers to consider a fuller range of challenges and threats from other state actors. The incorporation of both qualitative and quantitative models, with over 1000 existing sources of data and with 29 indicators to measure a state's capability is more comprehensive than any other current measure of cyber power.

NCPI 2022 builds on the foundations outlined in the 2020 paper and it should be understood as a snapshot of the current status of the thirty states and not be considered a linear step from the 2020 index. Due to the team's methodology, downwards movements do not mean that a state's cyber power has diminished in absolute terms. Instead, this movement should be interpreted as relative to the assessment of demonstrated cyber power of other states drawn from publicly available sources only. Importantly, the index does not make value judgements about how states use their cyber power, only that they have demonstrated their capability and intent to use it. Policy decisions around what is responsible and in the best interests of states, international conventions, and the world, should draw on this tool, and others, to make those judgements.

The Belfer Center team's model for cyber power remains the most holistic and best model-to-date for measuring cyber power. I am proud of the team for the work they continue to do to push forward this important conversation shining a light on a previously abstract, constantly evolving and central topic to state power and geopolitics today.

-Eric Rosenbach
Co-Director, Belfer Center
Former Chief of Staff and
Assistant Secretary for the U.S. Department of Defense

Table of Contents

Executive Summary

When we first broached the definition of Cyber Power in 2020 and issued the National Cyber Power Index in the same year, governmental dependency and use of the internet and digital technologies to achieve national objectives was well known but not effectively catalogued. Neither was the relationship to national power well understood. The popularised concept of cyber power at the state level was piecemeal and contested, primarily focusing on destructive capabilities and on a handful of states. At the same time, the COVID-19 pandemic was exacerbating the cyber risks that governments, infrastructure, businesses, and remote dispersed workforces face.

Our holistic definition of cyber power and the accompanying index contributed to the global debate, providing a starting point and structure for future thinking on a broader grouping of who has cyber power and what national objectives they seek to achieve via cyber means. The first National Cyber Power Index in 2020 extended the scope of the conversation from 5 to 30 states, from one or two objectives to eight. Debates on cyber power have influenced some governments to take a more considered approach to measuring their own cyber capabilities and stimulated a deeper exploration of the scope and application of cyber power.

Our intention is to underline the importance of understanding cyber power holistically, that its impacts are more broad reaching than immediate national security concerns, that harnessing it requires a whole-of-nation approach, and that cyber capabilities are but one tool in a state's toolkit. This broader definition is the prism through which governments across the world are channelling their resources to achieve national objectives, and through which a cornerstone of international engagement should be understood and shaped. Understanding the evolution of states and their respective cyber power will remain fundamental for policymakers and geopolitics for the foreseeable future. The National Cyber Power Index team will continue to revisit and measure cyber power as it evolves.

1. Introduction

Since we published the inaugural National Cyber Power Index (NCPI) in Fall 2020 the discussion on cyber power - including its scope and utility - has continued unabated. Its importance is undeniable with governments across the world prioritizing the development of multifaceted capabilities and releasing new cyber strategies outlining how at international, national, and local levels they intend to harness their domestic capabilities to develop their cyber power to achieve the eight objectives we first highlighted two years ago.

Whilst governments have been developing holistic policy on developing and using cyber power over the past two years, we have witnessed a slew of significant cyberattacks including Solarwinds, Microsoft Exchange, Colonial Pipeline, JBS and more recently the use of cyberattacks as one of many tools deployed in Russia's attack on Ukraine. Not only has the number of large-scale ransomware attacks risen in the past two years, but we've also seen an increase in the use of digital supply chains as a vector for cyberattacks. The more connected and integrated we become, the more attractive cyberattacks will be for criminals and states. States need to enhance their cyber power to protect their interests.

To best understand the actions of states and national power today, it is useful to conceptualize cyber power as composed of the eight objectives that states will attempt to achieve in and through cyberspace. States seek to not only destroy and disable an adversary's infrastructure and capabilities (the traditional, but narrow and misleading, perception of cyber power), but also to strengthen and enhance national cyber defences, gather intelligence in other countries, grow national cyber and commercial technology competence, control and manipulate the information environment, and to extend their influence through defining international cyber norms and technical standards. Cyber power should be considered in the context of a state's national objectives and governments should, and increasingly are, taking a whole-of-nation approach when attempting to harness it.

This 2022 Index provides a refreshed measurement of 30 states' cyber power through considering the indicators that contribute to both intent and capabilities. We have used 29 capability indicators across eight objectives to measure capability and assessed national strategies for all states assessed, where available.

The movements in state rankings reflect the data available to measure cyber power. We emphasize that any movements downwards are not a reflection that the state in question's capabilities have decreased in absolute terms, in most cases it is because publicly available data has become available for other states which demonstrates both their capability and intent to pursue the national objectives through cyber means.

Our primary aim is to understand and track cyber power as an evolving interconnected set of policies and capabilities that span the breadth of a state's activity. Our framework and the index are only a tip of the iceberg for understanding states intentions and capabilities in cyberspace. The academic and policy research space on cyber power and geopolitics is growing and we expect this field and the concept of cyber power to continue to evolve in the coming years.

2. **Key Themes**

In this section we briefly highlight two issues that have been of particular interest to readers of the Index since we published in 2020. They are a holistic approach to cyber power and achieving multiple objectives using cyber means.

2.1. **A Holistic Approach to Cyber Power**

Cyber power is multifaceted and requires a whole-of-nation approach in order to harness it. The objective of the NCPI is to provide a more complete measure of cyber power than existing indices, anecdotal studies, or journalistic speculation. We take such an approach to measuring cyber power wherever possible. This approach resonated with many governments, who have increasingly approached cyber power as a broader policy tool. We have seen in the past two years an expansion of strategic documents detailing how governments are trying to harness cyber power through an all of nation approach.

Within the NCPI we measure government strategies, capabilities for defensive and destructive operations, resource allocation, private sector capabilities within a country such as technology companies, workforce, and innovation. Our assessment is both a measurement of demonstrated capability and potential, where the final score assumes that the government can wield these capabilities effectively or the state benefits from them.

Objectives:

Surveilling and Monitoring Domestic Groups:

A state has taken steps to give itself the legal permissions and cyber surveillance capabilities to monitor, detect, and gather intelligence on domestic threats and actors within its own borders. This may range from efforts to conduct surveillance of its citizens, monitor internet traffic, circumvent encryption, or detect and disrupt foreign intelligence services, criminal organisations, and terrorist groups.

Strengthening and Enhancing National Cyber Defenses:

A state has prioritized enhancement of the defense of government and national assets and systems, and improvement of national cyber hygiene and resilience. This includes active defense of government assets, promoting cybersecurity and cyber hygiene to key industries and the general population, and raising national awareness of cyber threats.

Controlling and Manipulating the Information Environment:

Reflecting the duality of information controls, a state has utilized using electronic means to control information and change narratives at home and abroad. The form includes spreading domestic propaganda, creating and amplifying disinformation overseas, and using cyber capabilities to target and disrupt groups otherwise outside of its jurisdiction. The latter includes taking down extremist material from social media and refuting foreign propaganda.

Foreign Intelligence Collection for National Security:

A state has extracted national secrets from a foreign adversary via cyber means. This objective is specifically focused on the collection of information that is not commercially sensitive, but instead the collection of information that informs diplomatic activities, military planning, treaty monitoring, and other situations in which states seek to improve their situational awareness and understanding of a foreign state. This includes hacks and breaches of classified material, such as military plans, but it also includes stealing personnel records, and accessing the communications of senior government figures.

Growing National Cyber and Commercial Technology Competence:

A state has attempted to either grow its domestic technology industry or used cyber means to develop other industries domestically. This could be through legal and illegal means. Illegal means include conducting industrial espionage against foreign companies and states to facilitate technology transfer. Legal means include investment in cybersecurity research and development and prioritizing cybersecurity workforce development.

Destroying or Disabling an Adversary's Infrastructure and Capabilities:

A state has used destructive cyber techniques, tactics, and procedures to deter, erode, or degrade the ability for an adversary to fight in cyber or conventional domains. This includes cyberattacks on critical infrastructure, and Distributed Denial-of-Service attacks on government communications networks. It also includes cyberattacks to demonstrate intent and capability to deter an adversary from acting.

Defining International Cyber Norms and Technical Standards:

A state has actively participated in international legal, policy, and technical debates around cyber norms. This might include signing cyber treaties, participating in technical working groups, and joining cyber partnerships and alliances to combat cybercrime and share technical expertise and capabilities.

Amassing Wealth and/or Extracting Cryptocurrency:

A state has conducted cyber operations to amass wealth. This includes theft by cyber means including ransomware, blackmail using information obtained via data breaches and attacking the digital infrastructure of financial institutions, and blackmail based on information obtained via data breaches.

Figure 1. The 8 Objectives

We measure a state's intent to pursue each objective through an assessment of national strategies, rhetoric, and attributed cyber operations. If a state's intent to pursue an objective is low, we assess that the objective is of less importance to that state.

We measure a state's capability within each objective. The indicators we consider are either direct contributors to cyber power or proxies for difficult to measure capabilities. The cyber community's understanding of what contributes to cyber power is nascent and as this field develops, the cyber community's understanding of what contributes to cyber power capabilities will evolve, and our indicators will need to evolve with that. We recognize that national objectives pursued using cyber means are not composed in isolation. Cyber capabilities are just one of a state's suite of tools, i.e. alongside traditional military means, diplomacy, sanctions, and tariffs, that are available for states to deploy to achieve their national objectives.

"Cyber power is the effective deployment of cyber capabilities by a state to achieve its national objectives"

Cyber power is the effective deployment of cyber capabilities by a state to achieve its national objectives. To differentiate between levels of intent and capability between states across all objectives we assign the term "comprehensiveness" to describe a state's use of cyber power to achieve multiple objectives as opposed to a few.

Through combining both the intent and capability score across all eight objectives, we are able to reflect a "Comprehensive Cyber Power Ranking" where the most comprehensive cyber power is the state that:

- Has the intent to pursue multiple objectives using cyber means
- Has the capabilities to pursue and achieve said objectives

The most comprehensive cyber power has the highest intent and highest capability to achieve the most objectives using cyber means and the lowest scoring state is pursuing the least objectives using cyber means with the lowest level of intent and capability.

2.2. **Achieving Multiple Objectives Using Cyber Means**

In NCPI 2022 we explore the extent to which certain states seek to pursue multiple objectives using cyber means. To clarify, this is not a measure of technical capability or the 'sophistication of a cyberattack'. In our feedback workshops, experts noted that sophistication of attacks was not reflected in our 2020 index. Where a state perpetrating a low-level attack was counted in a binary manner and given the same 'scoring' as a highly sophisticated attack. We acknowledge the weakness and judge that we cannot measure the technical complexity of attributed attacks using publicly available data. Furthermore, even if measuring the technical complexity of cyber operations was included, this would not provide a definitive assessment of an actor's capability. The complexity of the operation is necessarily linked to the demands of the objective. Information collection, spreading disinformation or the theft of intellectual property could all use differing levels of technical complexity. Indeed, the most sophisticated cyber operations are not always made public. This could be because either the victim is unaware or unwilling to confirm that they were subject to an attack or the attacker's actions were not detected, or cannot be attributed to them.

In 2020, we relied on the Council on Foreign Relations (CFR)'s Cyber Operations Tracker. Following feedback, we have drawn on an additional resource, the Center for Strategic and International Studies (CSIS) Significant Cyber Incidents database, which measures incidents with a financial impact of more than $1M, in addition to the CFR database, which in theory does not make this distinction.

We previously measured the attacks perpetrated by states with various objectives as a measure of a country's demonstrated ability to operationalize particular types of attacks. This indicator is important because it is one of the concrete indicators of a state's ability to leverage their cyber power to achieve a given objective, although we recognise that the sources do not have access to all cyber operations that have been undertaken. This year, we have enhanced this indicator by drawing on another source and applying the NCPI framework for considering a comprehensive cyber power, that is, which states are pursuing multiple objectives in a cyber operation.

3. National Cyber Power Index 2022

3.1. Overall Ranking for 2022[1]

As seen in Table 1, the top ten most comprehensive states with the highest level of intent and capabilities across all eight objectives are as follows. Table 2 breaks the ranking down by objectives.

Table 1. NCPI 2022: Top 10 Most Comprehensive Cyber Powers

Rank	2022
1	US
2	China
3	Russia
4	UK
5	Australia
6	Netherlands
7	ROK
8	Vietnam
9	France
10	Iran

3.2. Interpreting the Index

Researchers, practitioners and policy makers can use the NCPI's aggregated measure of cyber power across all eight objectives to understand which states are the most comprehensive cyber powers based on publicly available data. We assess that top ranking states are the most effective in using cyber means to achieve objectives in multiple areas.

1 Please see Annex A for the NCPI conceptual framework and definitions of objectives.

State Movements:

Table 2. A Comparison of the Top 10 Cyber Powers in 2020 and 2022

Rank	2020	2022
1	US	US
2	China	China
3	UK	Russia
4	Russia	UK
5	Netherlands	Australia
6	France	Netherlands
7	Germany	ROK
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

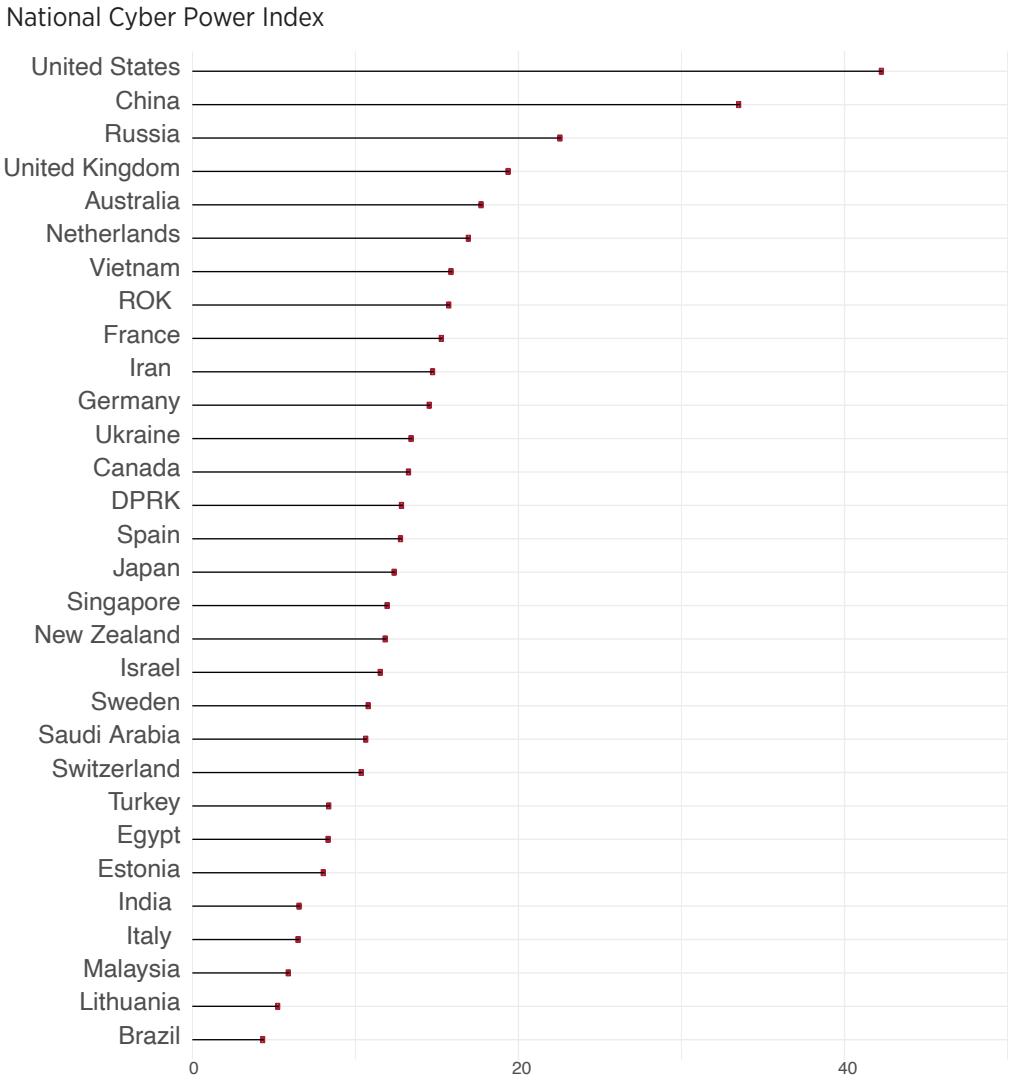

Figure 2. Overall Ranking 1-30

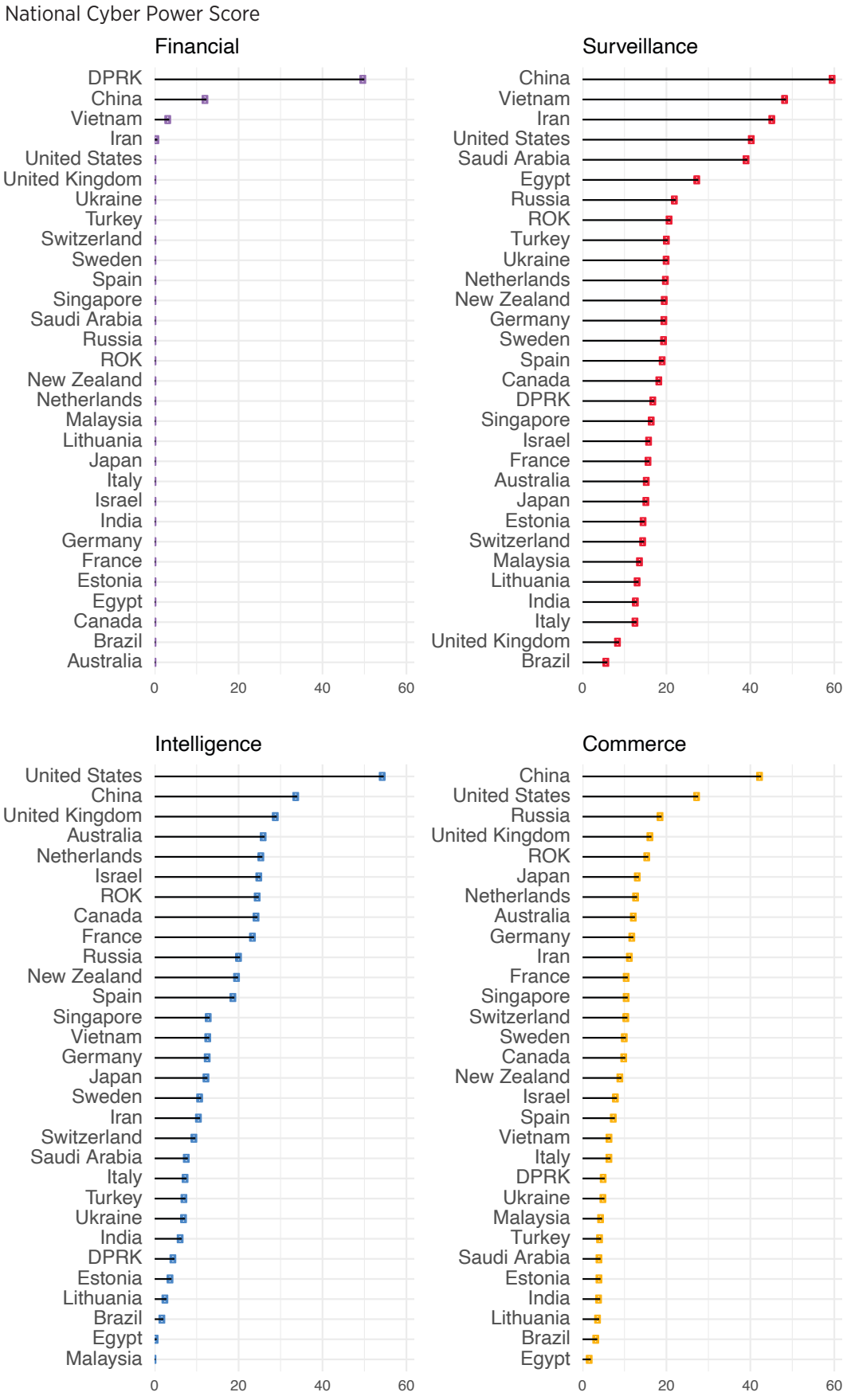

Figure 3.a. Ranking of States by Objective

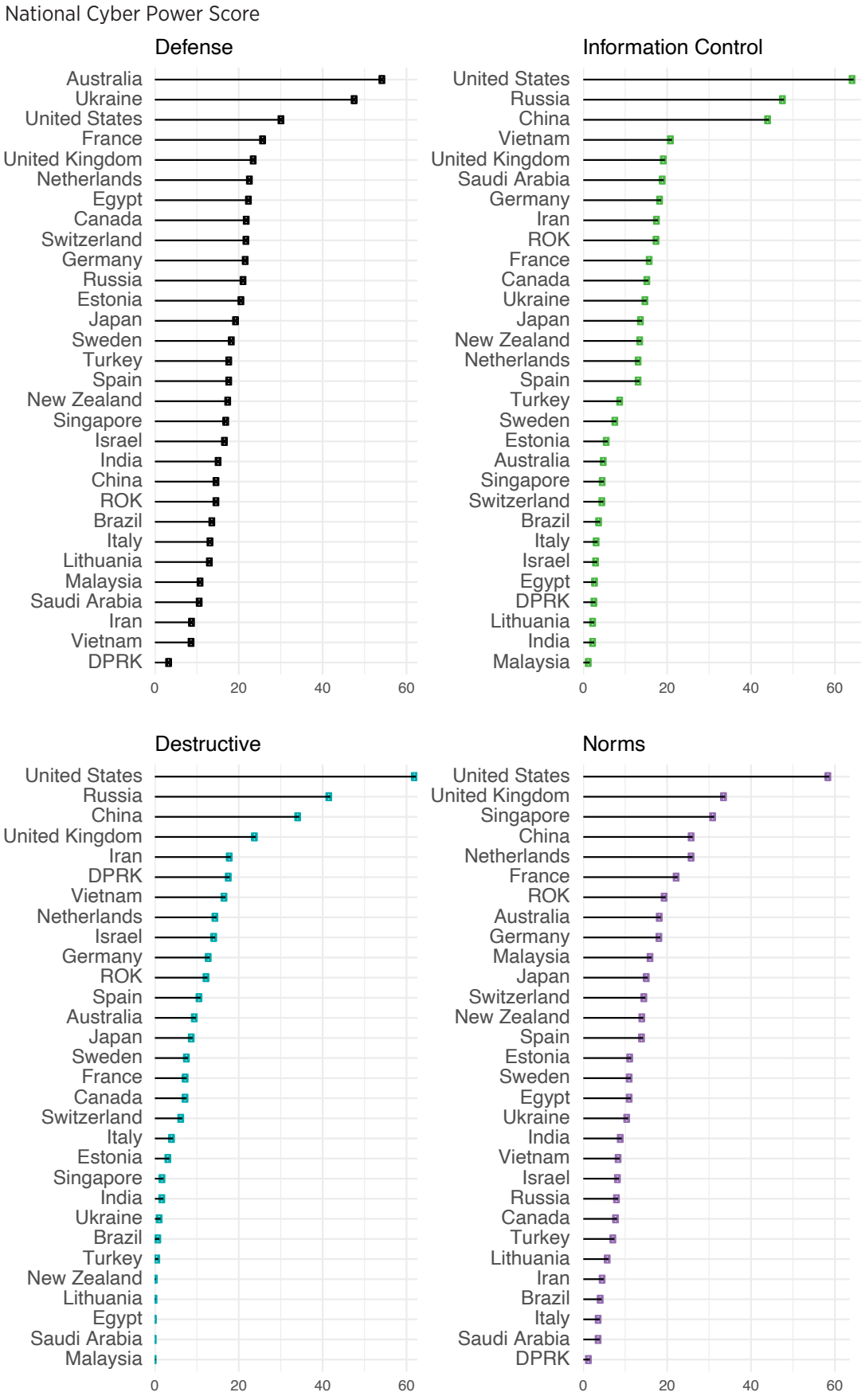

Figure 3.b. Ranking of States by Objective

There are some movements in our Top 10 ranking of cyber powers. Most notably Russia moved from 4th place to 3rd and the UK moved down one spot. Within two objectives, commercial gain and destructive capability, Russian cyber power has increased relative to that of the UK, largely because of their undertaking of more cyber operations that have been publicly reported in these areas.

Other interesting movements in our rankings have been Iran and Ukraine. Iran has climbed the index from 22nd to 10th. Its capability ranking went from 28th to 15th due to increases in its destructive and surveillance scores, as well as the newly scored objective - financial, where it scored 3rd overall. Ukraine has gone up from 29th to 12th, with it's capability ranking increasing two places, and its intent ranking moving from 21st to 6th, driven largely by increases in defence, intelligence and destructive rankings, but having seen increases across the board.

Two of China's regional neighbours have seen significant gains in the index. The Republic of Korea has gone from 16th to 7th having seen its capability remain level but its intent rising from 18th to 9th because of increases across the board but particularly in surveillance, information control, intelligence, commercial and norms.

Vietnam's ranking has gone up from 20th to 8th having seen its capability remain steady but its intent rising from 16th to 3rd due to increases in defense, commercial, destructive and norms.

Given the nature of the data we collect, these movements in rankings do not point to an absolute increase or decline in cyber power in comparison to 2020, but a relative change in cyber power based on publicly available information in comparison to others.

3.3. **Limitations**

The NCPI's objective oriented analysis of national cyber power suffers from some limitations, which are mostly connected with the evolving and contested nature of "Cyber Power" and the limited data available in the public domain about state cyber capabilities and intentions. The limitations that we outlined in the methodology of the 2020 index remain, in brief:

Lack of Publicly Available Data on Cyber Capabilities and Intent:

The data that we have collected is available for the majority, but not all the states that we assessed. One of the challenges of building this index is that components that contribute to a state's cyber power are sensitive and therefore classified, for e.g. its number of military personnel, or intelligence capabilities. There are areas where the data is less sensitive, such as efforts to increase the skilled workforce and industry related data. However, this data tends to be less easily available for states with less transparent and accountable governance structures, or with fewer resources.

Due to the sensitivities of some aspects of cyber power, particularly destructive, defensive and espionage capabilities and their reliance on domestic national security structures, states may deliberately be shielding their intent and capabilities from public knowledge for strategic purposes. We suspect this is the case for most states in relation to covert or military capabilities, but specifically for China, Israel, Iran, and North Korea. In recent years, we have seen western democracies share more information about their military cyber capabilities, be this as a deterrent to adversaries, as a result of national policies on transparency, or to signal leadership and to shape the global debate. This lack of transparency is particularly the case in those three stated objectives, but also in other areas as geopolitical tensions rise. We recognize that a state deliberately choosing to be opaque will be under-ranked in respective areas in the NCPI. For example, no state will openly state that they are using cyber means such as ransomware to amass wealth and to counter this absence in information the NCPI includes attributed cyberattacks within this objective as we consider a state carrying out a cyber operation also demonstrates intent. Similarly, few states will publish the numbers of personnel working, or operations being undertaken, on destructive cyber operations, making it extremely difficult to measure a state's capability, particularly if those operations are successful enough that they are not detected and not reported on publicly.

4. **Conclusion**

States continue to expand their capabilities to achieve multiple objectives in cyberspace. To better understand the actions of states and national power it is important to conceptualize cyber power as multidimensional and to expand the scope of analysis to include the breadth of objectives states are attempting to achieve through cyber means. From our analysis, it is clear that states seek to not only destroy and disable an adversary's infrastructure and capabilities, but also to strengthen and enhance national cyber defenses, gather intelligence in other states, grow national cyber and commercial technology competence, control and manipulate the information environment, and extend their influence through defining international cyber norms and technical standards. Cyber power should be considered in the context of a state's national objectives and states should and increasingly are taking a whole-of-nation approach when attempting to harness it.

Taking a step back from the Index, the governance and infrastructure underpinning the internet is increasingly fragmented. Expedited by power shifts and geopolitical events, and the rise of China's influence, particularly in the cyber domain, states are, now more than ever, reaching out to build coalitions on cyber-related issues to shape the cyber domain in their interest. Whether it is seeking consensus on the acceptable conduct of states and norms in cyberspace at the UN, the governance of technology through technical standards to either drive or prevent interoperability, or plans to diversify supply chains creating new ecosystems in friendlier states, the nexus of technology and values is a growing fault line in global affairs.

Exacerbating this fault line in global affairs has been the devastating, unilateral invasion of Ukraine by Russia in which the full spectrum of cyber power has been explored. The prospect of Russian cyberattacks either unintentionally spilling outside of the conflict zones, or being used as a targeted weapon against those that declared themselves to be Ukrainian allies sent the cyber community into overdrive; offering support to defend Ukraine's digital estate, with capacity building and with providing equipment. States ramped up their own cyber defences to prepare for both scenarios.[2] At the point that this paper has been published, Russia appears to have been targeted in its use of its destructive cyber

2 https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/.

power as part of the conflict - attacking Ukrainian infrastructure, services, and businesses. Reports suggest that whilst military and cyberattacks have operated in tandem, the scale has been smaller than expected and appear to have had overlapping objectives.[3] The control of the domestic information environment has been a key part of its war effort, ensuring that Russians are seeing only a limited perspective of the events, and attempting to use its power to discredit both Ukrainian and western narratives internationally. The conflict has highlighted the interconnected nature of global supply chains, and will no doubt add a significant case to the debate on the bifurcation of technologies - with an exodus of foreign companies from Russia due to western sanctions and domestic Russian companies, or non-western companies, stepping in to fill the void[4] whilst also relying on western components for its military capability.[5] States have already started re-examining their own supply chains and domestic commercial power in this area. We can expect Russia to continue to flex its domestic surveillance and intelligence gathering in other states, the capabilities for which can easily support other objectives, particularly destroying adversary infrastructure.

It is clearly evident in today's geopolitical environment that states are pursuing a more comprehensive set of cyber power capabilities. The comparison and understanding of a broader range of actors is more important than ever. We anticipate the twin challenge of keeping up with the evolving concept of cyber power and simultaneously measuring cyber power across 30 or more states with publicly available data will continue to inspire debate and require flexibility. But finding a way to draw a comparison and a common understanding is critical as national governments strive to build dialogue and coalitions within national ecosystems and between states to enhance their own cyber power relative to, or in concert with, others. We hope that other researchers continue to build on this work, and we look forward to the inevitable and enriching debates on the evolution of cyber power and geopolitics going forwards.

3 The economist (online), Russia seems to be co-ordinating cyber-attacks with its military campaign, London, May 10, 2022 and https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

4 https://www.reuters.com/world/europe/foreign-digital-firms-leave-russias-domestic-providers-pounce-2022-04-01/

5 https://www.nytimes.com/2022/06/02/business/economy/russia-weapons-american-technology.html

Annex A: Methodology

Between the 2020 and 2022 index, the team went through a rigorous process of challenging the indicators that had been used to understand if there was better data now available or whether there were better indicators that could help measure various capabilities. We hosted several workshops and conducted in depth interviews with intelligence, defense, and cyber specialists to test the assumptions behind NCPI 2020 and for suggestions on how to refine our methodology with what is openly available. As such, there have been a number of adjustments to the indicators used.

A.1 Conceptual Framework

Table 3. Objectives Pursued

Objective	Description
Amassing & Protecting Wealth	A state has conducted cyber operations to amass wealth. This includes theft by cyber means including ransomware, blackmail using information obtained via data breaches and attacking the digital infrastructure of financial institutions, and blackmail based on information obtained via data breaches.
Controlling & Manipulating the Information Environment	Reflecting the duality of information controls, a state has utilized using electronic means to control information and change narratives at home and abroad. The form includes spreading domestic propaganda, creating and amplifying disinformation overseas, and using cyber capabilities to target and disrupt groups otherwise outside of its jurisdiction. The latter includes taking down extremist material from social media and refuting foreign propaganda.
Defining International Cyber Norms and Technical Standards	A state has actively participated in international legal, policy, and technical debates around cyber norms. This might include signing cyber treaties, participating in technical working groups, and joining cyber partnerships and alliances to combat cybercrime and share technical expertise and capabilities.
Destroying or Disabling an Adversary's Infrastructure and Capabilities	A state has used destructive cyber techniques, tactics, and procedures to deter, erode, or degrade the ability for an adversary to fight in cyber or conventional domains. This includes cyberattacks on critical infrastructure, and Distributed Denial-of-Service attacks on government communications networks. It also includes cyberattacks to demonstrate intent and capability to deter an adversary from acting.

Foreign intelligence Collection for National Security	A state has extracted national secrets from a foreign adversary via cyber means. This objective is specifically focused on the collection of information that is not commercially sensitive, but instead the collection of information that informs diplomatic activities, military planning, treaty monitoring, and other situations in which states seek to improve their situational awareness and understanding of a foreign state. This includes hacks and breaches of classified material, such as military plans, but it also includes stealing personnel records, and accessing the communications of senior government figures.
Growing National Cyber and Commercial Technology Competence	A state has attempted to either grow its domestic technology industry or used cyber means to develop other industries domestically. This could be through legal and illegal means. Illegal means include conducting industrial espionage against foreign companies and states to facilitate technology transfer. Legal means include investment in cybersecurity research and development and prioritizing cybersecurity workforce development.
Strengthening and Enhancing Cyber Defenses	A state has prioritized enhancement of the defense of government and national assets and systems, and improved national cyber hygiene and resilience. This includes active defense of government assets, promoting cybersecurity and cyber hygiene to key industries and the general population, and raising national awareness of cyber threats.
Surveilling and Monitoring Domestic Groups	A state has taken steps to give itself the legal permissions and cyber surveillance capabilities to monitor, detect, and gather intelligence on domestic threats and actors within its own borders. This may range from efforts to conduct surveillance of its citizens, monitor internet traffic, circumvent encryption, or detect and disrupt foreign intelligence services, criminal organisations, and terrorist groups.

A.2 **National Cyber Power Index Formula**

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{8}\sum_{x=1}^{8} Capability_x \times Intent_x$$

Figure 4. Formula NCPI 2022

A.3 **Construction Of The Aggregated NCPI**

Missing Data and Normalization of Indicators:

We were not able to find data for all 30 states included in NCPI 2022 for each of our indicators. All indicators in the Index reflect the available of data for at least 21 (70%) of the 30 states and where we had reasonable proxies for the missing data points. Estimates were calculated based on states that share similar characteristics (population size, economic strength, geography) or based on other indicators that

were close to what we measure. Indicators that did not meet this threshold were not included. We sourced multiple indicators in house and followed a rigorous coding scheme and procedure.

The data set does not contain any missing values. For all indicators and states, where information was missing, we provide an estimated value. Specifically, some values have been estimated for the following indicators:

Table 4. State Capability Indicators that used Estimates

Indicator	Estimated for the following states
Cyber Risk Literacy and Education Index	DPRK, Egypt, Iran, Malaysia, Ukraine, Vietnam
Cyber Military Staffing	DPRK, Egypt, India, Lithuania, Malaysia, New Zealand, Saudi Arabia, Ukraine, Vietnam
Data Privacy Laws	DPRK
Freedom on the Net	DPRK, Israel, Lithuania, Netherlands, New Zealand, Spain, Sweden, Switzerland
Global Soft Power Index	DPRK, Lithuania
Mobile/ Computer Infection Rate	DPRK, Estonia, Lithuania, New Zealand
National Standards Body	DPRK, Brazil, China, Egypt, Israel, Lithuania, Malaysia, Russia, ROK, Saudia Arabia
Population on the Internet	DPRK
Social Media Usage	DPRK
Surveillance	DPRK, Egypt, South Korea, Saudi Arabia, Turkey, Ukraine, Vietnam

Before aggregating the data, we made directional adjustments to our indicators so that higher values correspond to better cyber power performance in all indicators. We have performed pairwise correlation analysis over all indicators.

Before aggregating we normalized the indicators to bring them on a common scale. We have used the Min-Max technique as our normalization technique because it: (1) best reflects our conceptual framework; (2) is most appropriate for the data properties; and (3) can be easily interpreted by users.

NCPI Aggregation and Weighting:

To measure the score for each objective, we took the average of the normalized capability scores for that objective. We then multiplied the averaged normalized capability scores of a specific objective with the intent score of said objective to get the NCPI score for a single objective. To calculate the NCPI across all objectives we summed the single-objective scores together to create an aggregate score.

The objective-oriented approach has important consequences for the construction of the NCPI as it introduces a weight, and some indicators are counted multiple times (see Table 14). Multiple counting is based on careful theoretical reflection on how different cyber capabilities map to multiple cyber objectives.

Any indicator counted multiple times will, by default, boost the score in both the NCPI and the Cyber Capability Index for a state that scores highly on that capability indicator.

We compute the NCPI intent scores by multiplying - for each objective - a state's capabilities with its intent to achieve said objectives. For each state, through the intent measure we are effectively putting a weight on its capabilities. The intent part of our NCPI Index can be considered equivalent to a weight. The NCPI intent score reflects the different prioritisation that some states place on leveraging specific cyber capabilities. This assumes that a state will only invest in and deploy its cyber capabilities in a domain, such as national surveillance, if it shows a relatively high intent to do so.

A.4 **Changes To NCPI 2022 Methodology**

This year, we have used 29 capability indicators that are then averaged into the Cyber Capability Index. As with 2020, some metrics contribute to more than one objective. If new information was available for indicators used in 2020 they have been updated. We have also included new indicators to incorporate the eighth objective.

Inclusion Of The Eighth Objective: Amassing And Protecting Wealth

The NCPI has outlined eight objectives that states seek to achieve using cyber means. In our 2020 index we did not provide a measure for the eighth objective: Amassing and Protecting Wealth. This omission was due in part to the difficulty in collecting data on this objective. This year, whilst useful data for this objective remains difficult to come by, we have used a single indicator to measure a state's capability in this objective, which while imperfect provides an enhanced dimension to this index.

We have defined Amassing & Protecting Wealth as the use of cyber operations to amass wealth. This includes theft by cyber means including ransomware, ransoms demanded for not publicising information obtained via data breaches and attacking the digital infrastructure of financial institutions.

The four states that recorded a score in this area were China, DPRK, Vietnam, and Iran. The anomaly in this ranking is the absence of Russia in a high-ranking position. Whilst a number of high-profile ransomware groups have been reported to be based in Russia and Russian speaking states, the overt, published, or stated intent by the Russian Government does not include the generation of cash from cyberattacks. This index has also not taken into account, for the purpose of scoring, the close relationship between cybercriminal groups, or proxies, and the state. The collaboration between the Russian state and criminal groups is a strategic and tactical approach to its own cyber power and global policy ambitions.

For this objective, the index looked at the number of attacks identified in open-source databases that had a financial gain objective.

Annex B: National Cyber Power Index - Results Charts

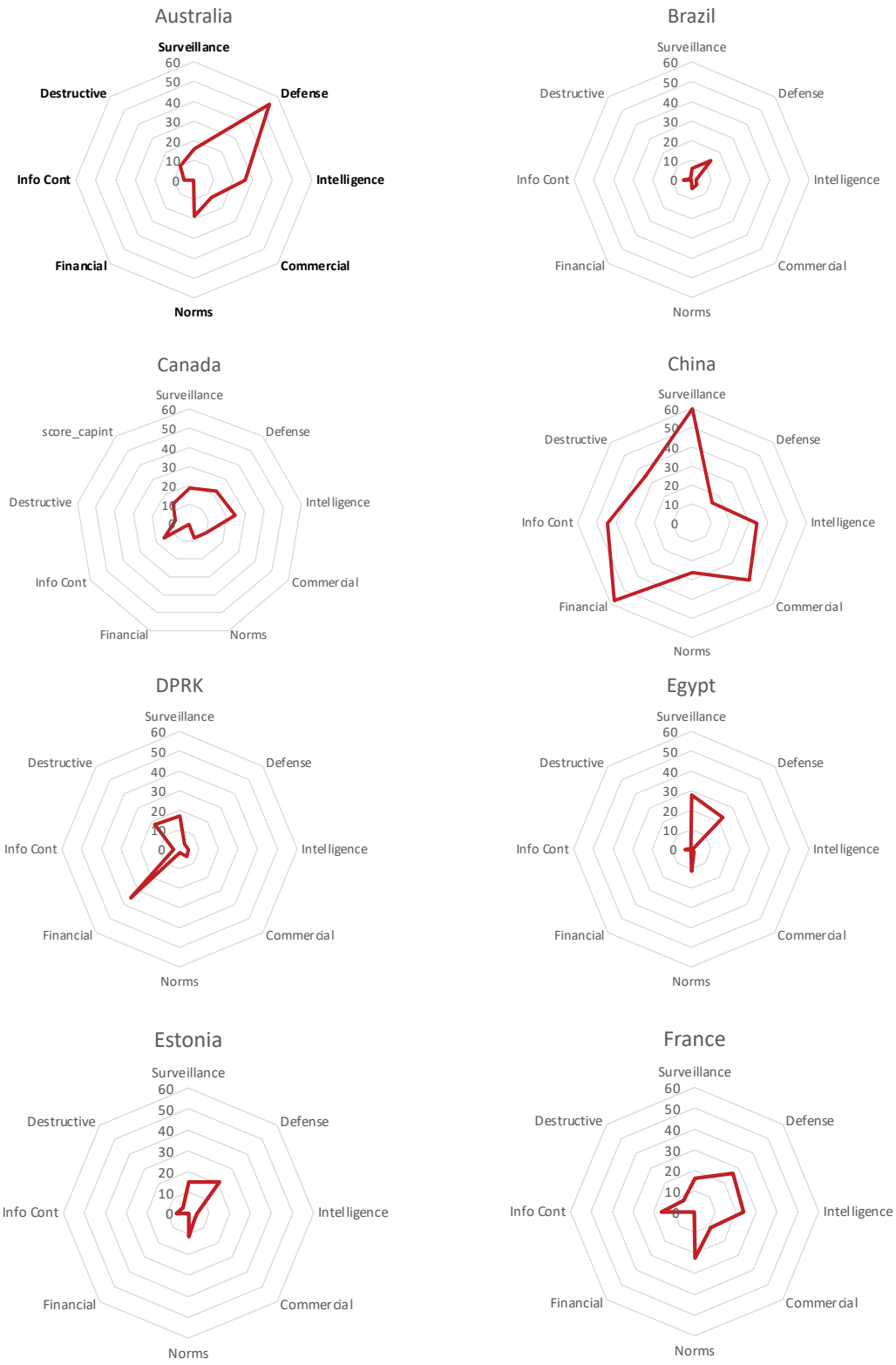

Figure 5.a. National Cyber Power Radar Charts by Objective

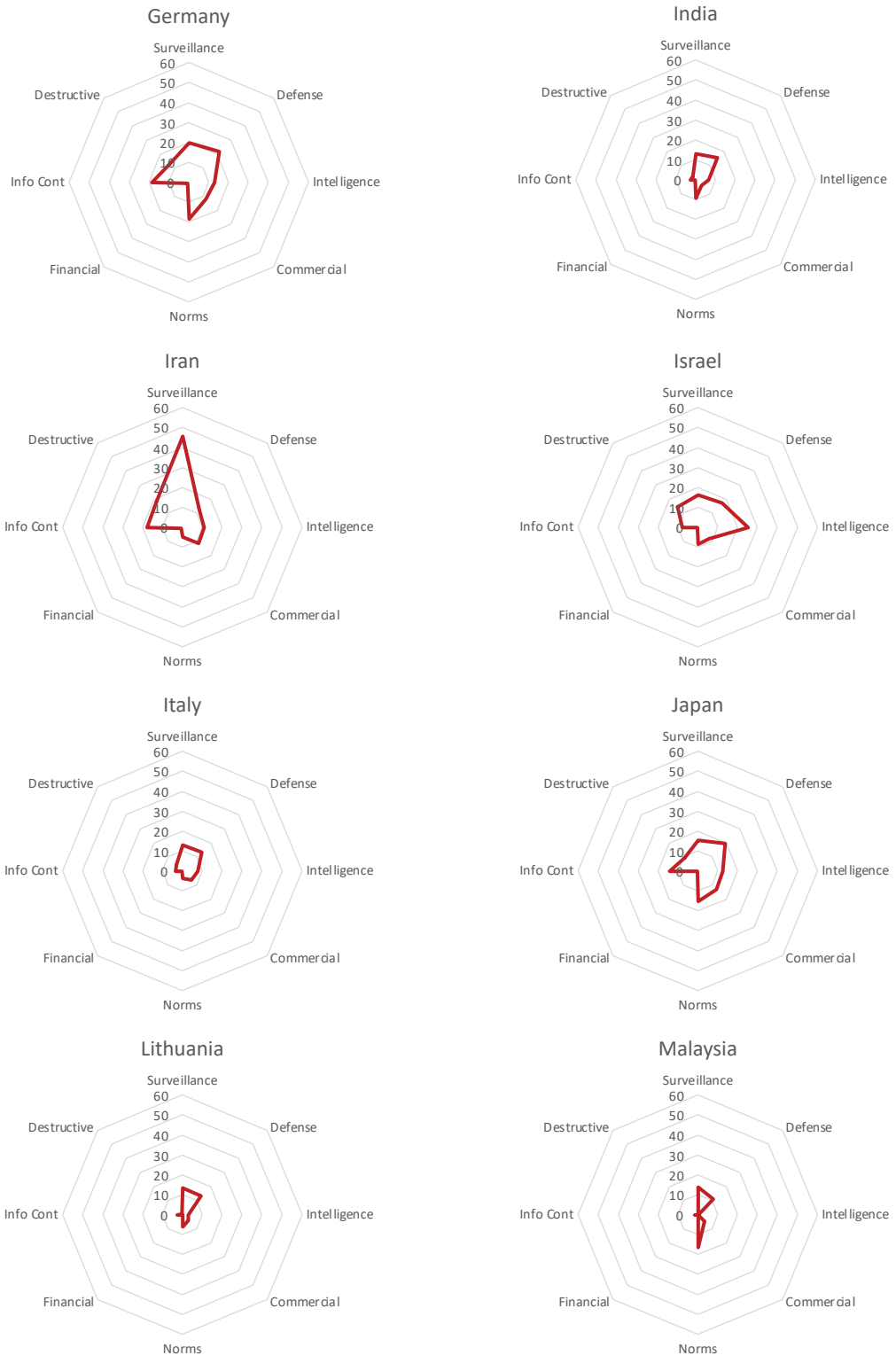

Figure 5.b. National Cyber Power Radar Charts by Objective

Figure 5.c. National Cyber Power Radar Charts by Objective

Figure 5.d. National Cyber Power Radar Charts by Objective

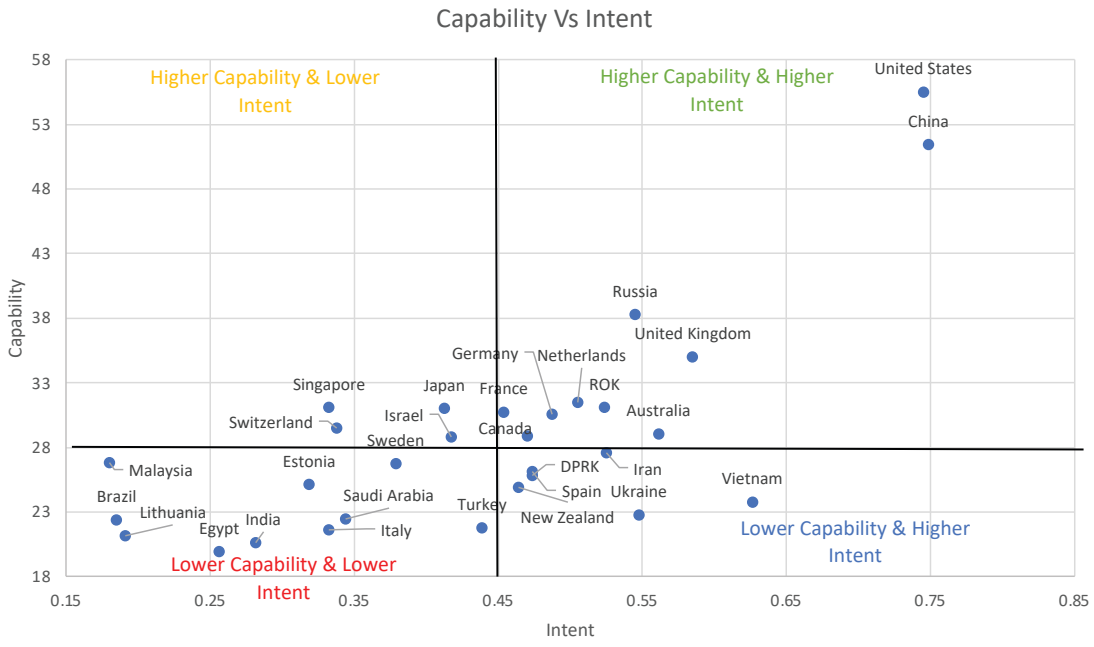

Figure 6. Capability vs Intent Scatter chart

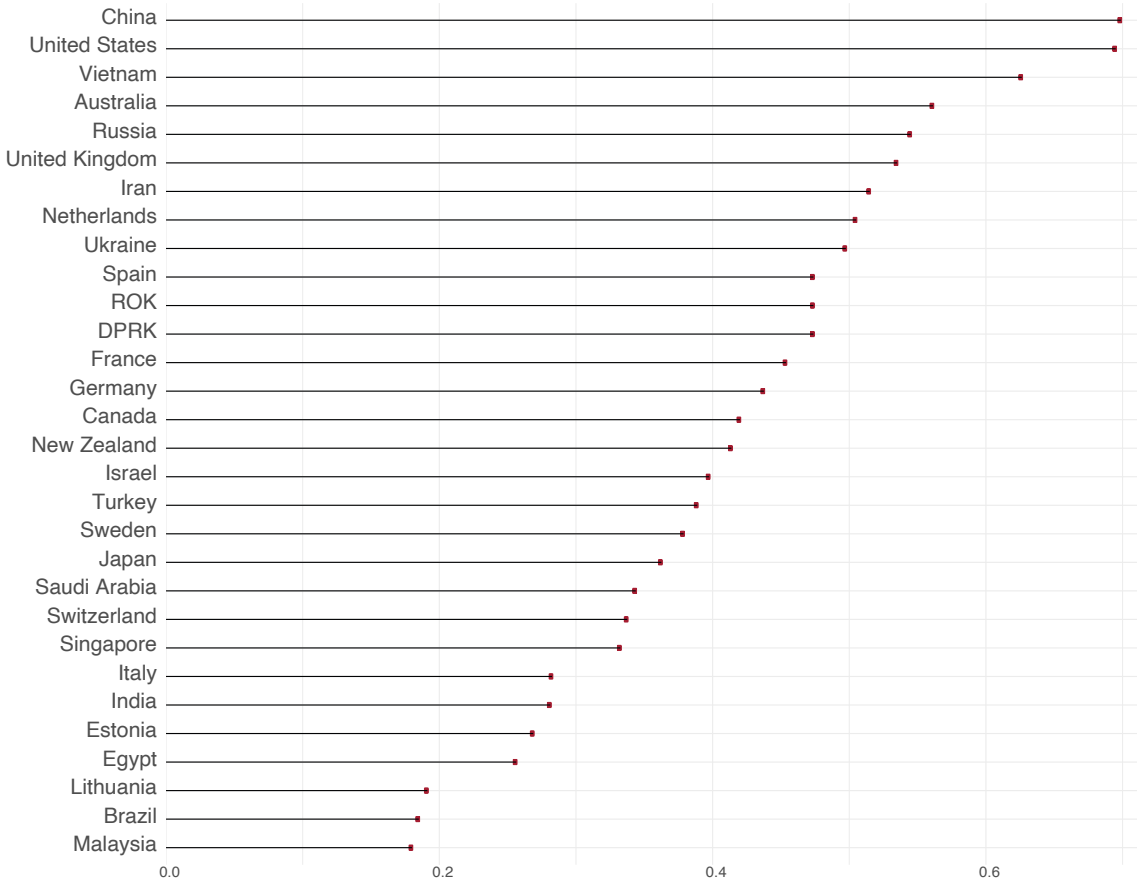

Figure 7. Cyber Intent Index Ranking

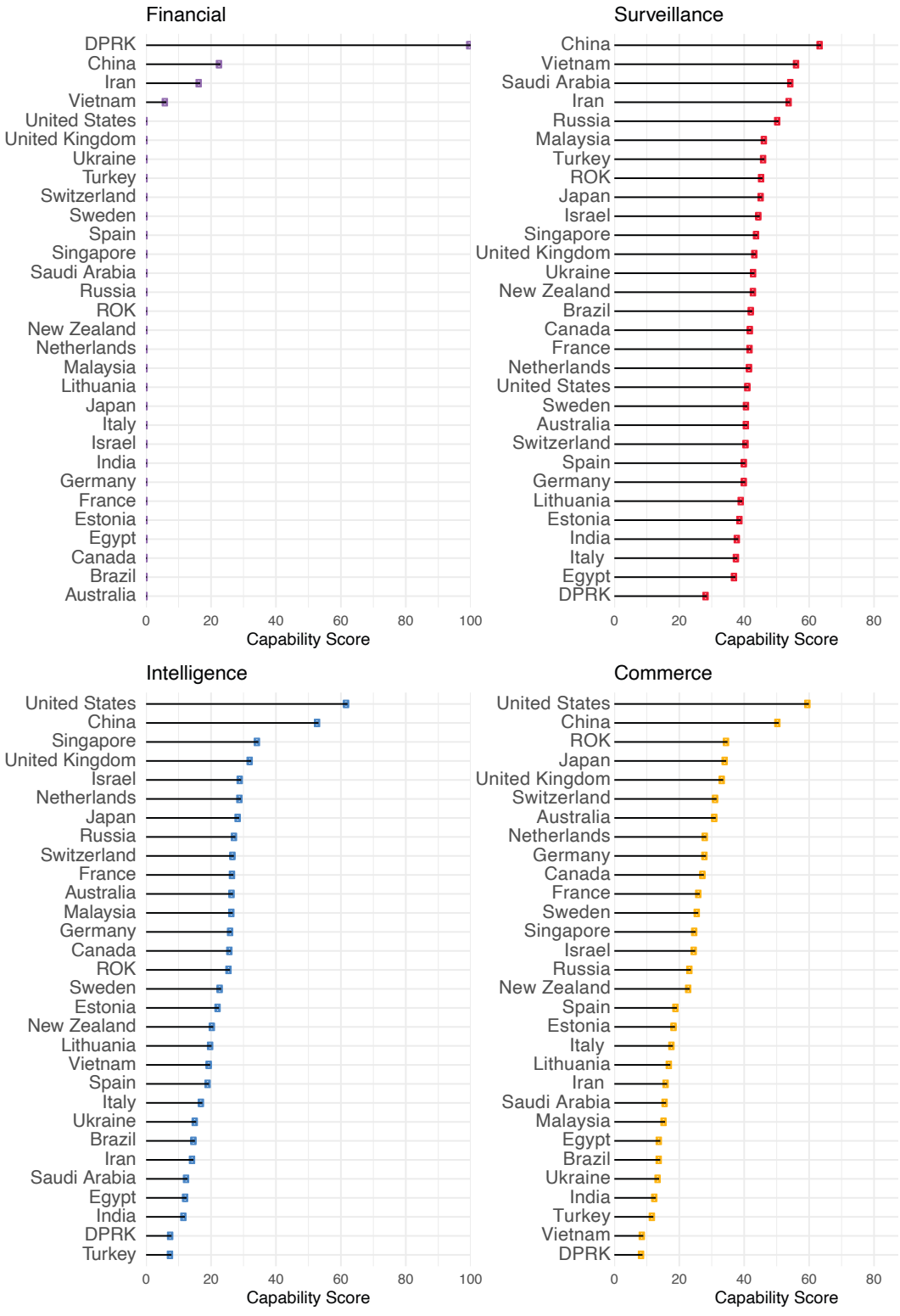

Figure 8.a. Results by Objective (Capability)

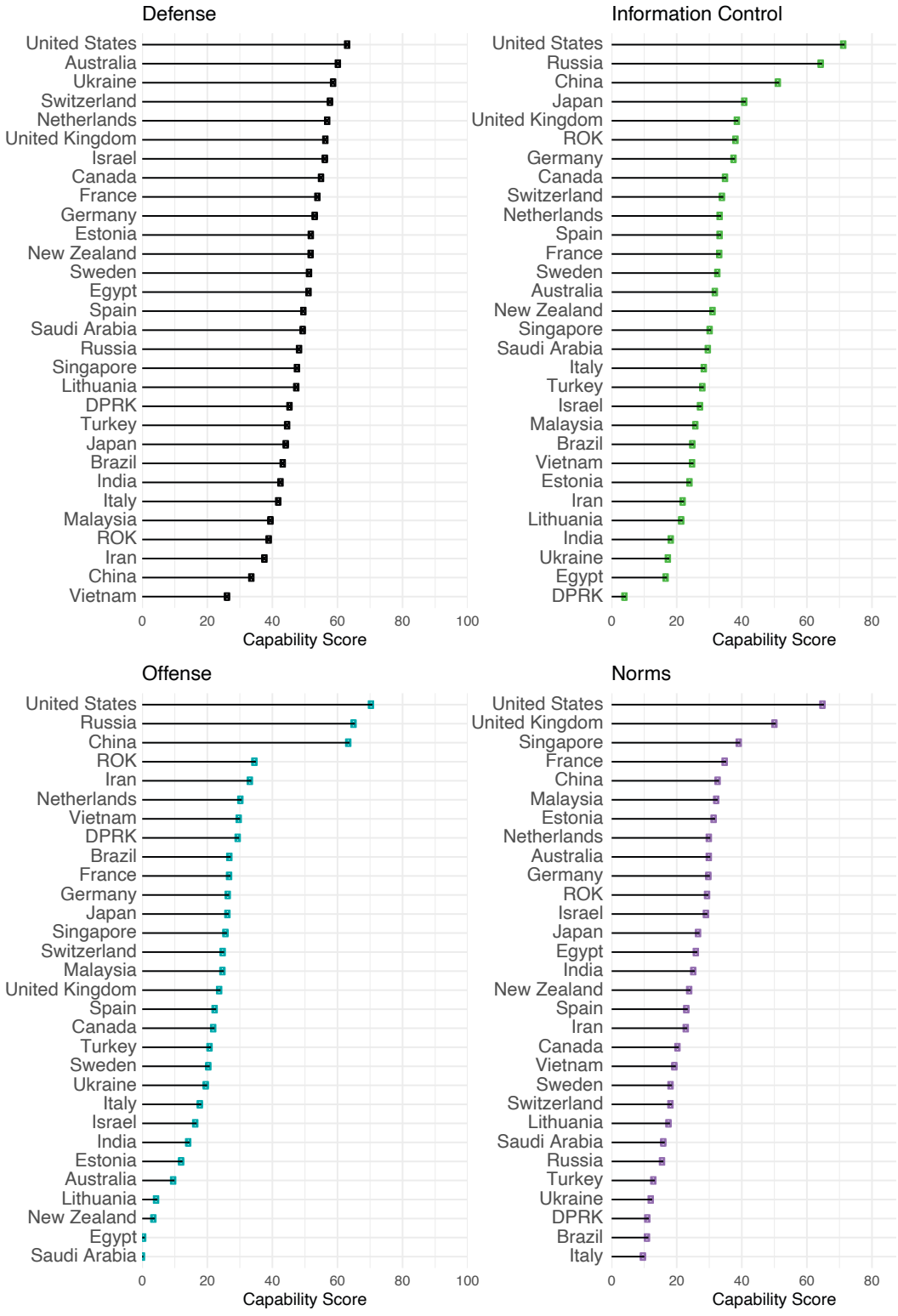

Figure 8.b. Results by Objective (Capability)

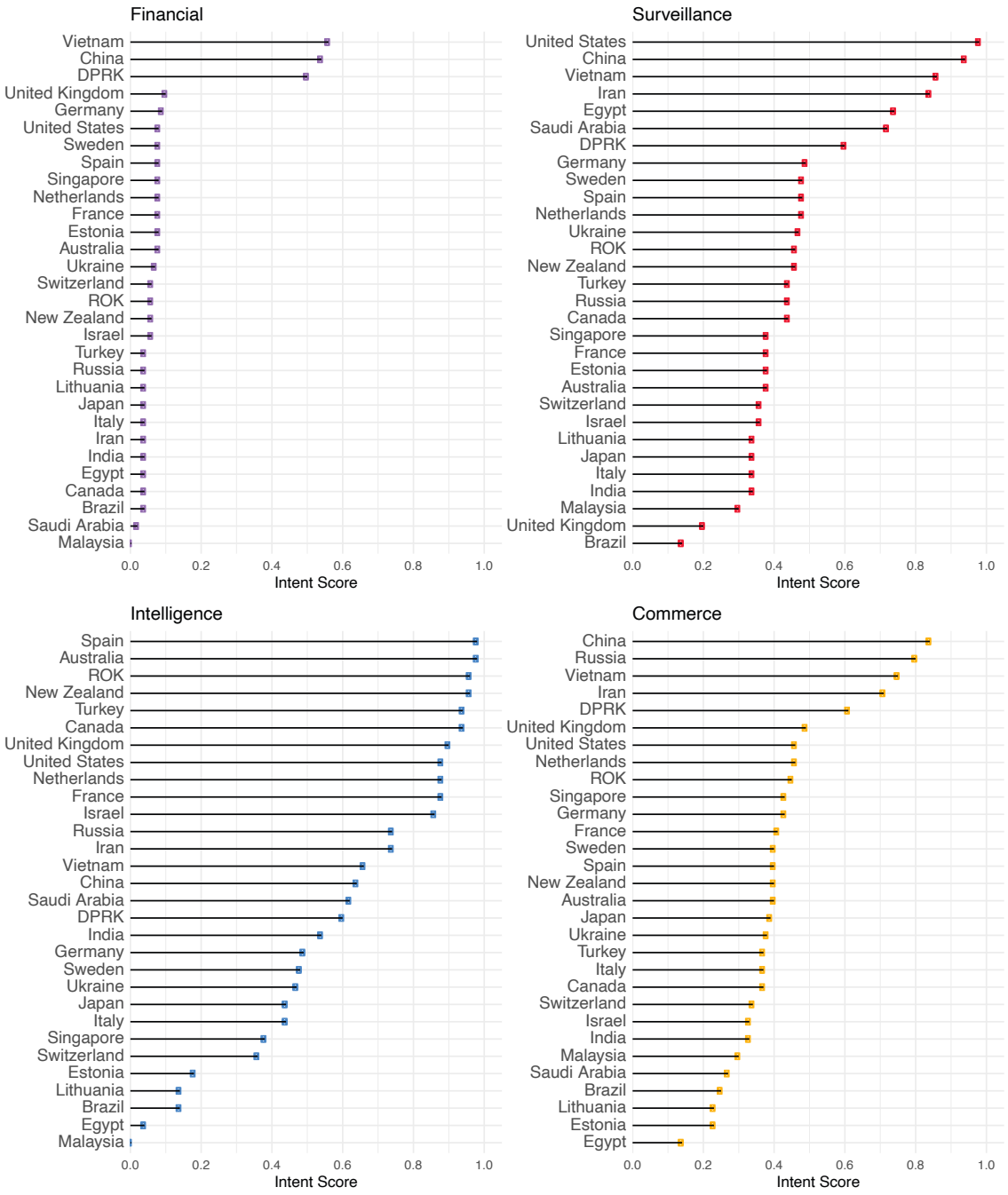

Figure 9.a. Results by Objective (Intent)

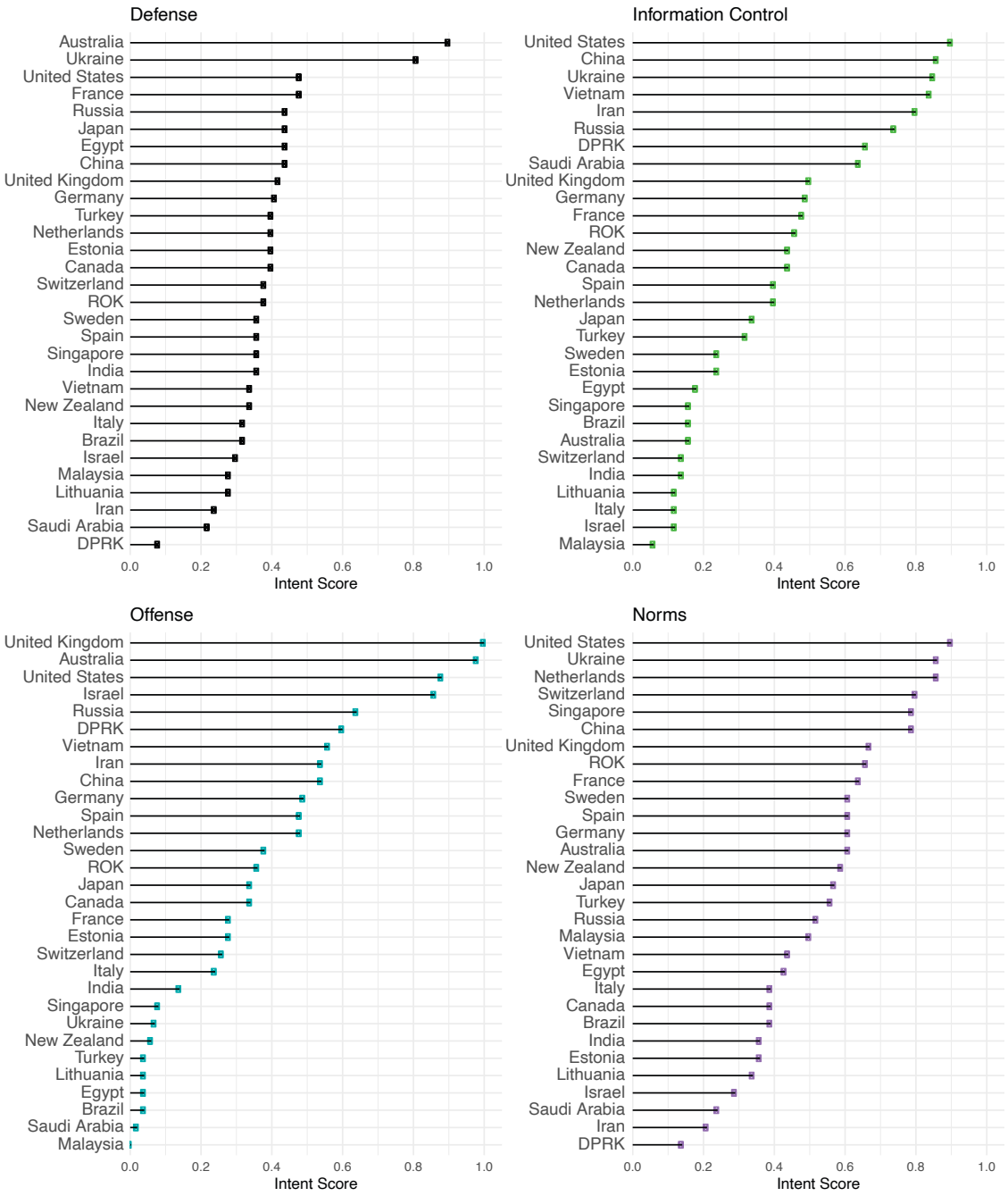

Figure 9.b. Results by Objective (Intent)

Annex C: Detailed Explanation of Intent Indicators

C.1 Intent Indicators by Objective

Amassing and Protecting Wealth

Table 5.

Indicator	Meaning	Source Description	Scoring Method
Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack	Observed in 1 or more attack: Yes/ No

Controlling And Manipulating The Information Environment

Table 6.

Indicator	Meaning	Source Description	Scoring Method
Data protection law strength	How well defined and articulated each state's data protection regime is	Using DLA Piper's Data Protection rating for each state: https://www.dlapiperdataprotection.com/	Heavy/ Robust/ Moderate/ Limited/ No information
Does the state's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the state has cyber capabilities to control and manipulate the information environment?	Like all large bureaucracies, militaries rely on clear hierarchies and effective plans. A military can only effectively employ cyber effects if commanders understand how and when they should be used, and how they complement conventional capabilities. In addition, all militaries face opportunity costs on the capabilities they choose to procure and they would be expected to justify in national defence planning documents the value that cyber effects bring.	Analysis of the online presence of each state's Ministry of Defence (MOD) and/or Armed Forces to find relevant documents. Relevant documents include: defence plans, defence strategies, military doctrine, defence white papers, defence cyber plans, defence cyber strategies, military cyber doctrine, defence cyber white papers, statements from senior military leaders, statements from MOD politicians on the state's cyber capabilities.	Yes/No
Does the state's military cyber unit or command acknowledge that the state has cyber capabilities to control and manipulate the information environment?	Having a dedicated military cyber unit or command shows that a state is seeking to enhance and grow its military cyber expertise and recruit to meet its need. Given the shortages of skilled cyber workers that all states face, cyber military units must compete to attract the very best. Military units will therefore seek to explain the role that they play and capabilities they offer.	Analysis of the online presence of each state's military cyber force to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber military leaders on the capabilities that specific military units possess.	Yes/No
Does the state's signals intelligence agency or foreign intelligence service acknowledge that the state has cyber capabilities to control and manipulate the information environment?	Acknowledgement that the state's intelligence agency has a cyber mission	Analysis of the online presence of each state's intelligence agency to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber intelligence agency leaders on the capabilities that the intelligence community possess.	Yes/No

Consistency of objective: is it pursued in >1 Strategy	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in >1 strategy: Yes/No
Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack	Observed in 1 or more attack: Yes/ No

Defining International Cyber Norms And Technical Standards

Table 7.

Indicator	Meaning	Source Description	Scoring Method
How many of the past five UN Cyber Government Group of Experts (GGE) consultations has the state participated in?	The UN General Assembly First Committee on Disarmament and International Security, which, through its successive Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security, has facilitated some of the first efforts to reach global consensus on the binding and non-binding norms that apply to the digital environment and the behaviour of States in their uses of ICT. A higher score in this indicator demonstrates that the state has been party to the UN GGE consultations.	Figures taken from: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf	1 = five times; 0.8 = 4 times; 0.6 = 3 times; 0.4 = 2 times; 0.2 = 1 time; 0 = none of these times

How many times has the state participated in the Internet Governance Forum (IGF) between 2015-2019?	The Internet Governance Forum (IGF) serves to bring people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors. At their annual meeting delegates discuss, exchange information and share good practices with each other. The IGF facilitates a common understanding of how to maximize Internet opportunities and address risks and challenges that arise.	Figures taken from: https://www.intgovforum.org/multilingual/content/mag-2020-members and https://www.intgovforum.org/multilingual/igf-2020-1st-mag-attendees	0.25 for government/ civil society/ technical community/ private sector
Has the state participated in Global Forum for Cyber Expertise capacity building activities?	The GFCE states that its mission is to strengthen 'international cooperation on cyber capacity building by connecting needs, resources and expertise and by making practical knowledge available to the global community.' States that participate demonstrate a willingness to help share cyber best practice and norms.	Figures taken from: https://thegfce.org/member-overview/	Yes/No
What is the rate of participation in ISO/ IEC Joint Technical Committees for ICT?	The International Organization for Standardization (ISO) and the International Electrotechnical Commission jointly deliver consensus-based, market relevant International Standards for information technologies. Shaping and adhering to ISO/IEC JTC demonstrate a commitment to improving these elements within their own state. The higher the score the more active said state is in international standards setting which is important for its domestic industry to be interoperable with international markets.	https://www.iso.org/technical-committees.html	# of ISO/IEC Joint Technical Committees X is a member of divided by 22 (total number of ISO/IEC JTC Committees. The score is a percentage of technical committees attended by said state.

What is the quality of participation across all 22 ISO/IEC Joint Technical Committees?	The International Organization for Standardization (ISO) and the International Electrotechnical Commission jointly deliver consensus-based, market relevant International Standards for information technologies. Shaping and adhering to ISO/IEC JTC demonstrate a commitment to improving these elements within their own state. The higher the score the more formal authority it has had on average in the technical committees and the more that state and its industry shapes the international standards agenda in ICT.	https://www.iso.org/technical-committees.html	Each state was given a score for each Technical Committee based on its role. The score was allocated as follows: 1 = Secretariat; 0.75 = Participant; 0.5 = Observer; 0.25 = ISO/IEC JTC Member; 0 = no affiliation. The average of its participation was then taken across all committees so the final score is between 0 and 1.
What is the quality of participation of the state across the International Telecommunication Union's Study Groups 13 (Future Networks), 17 (Security), and 20 (IoT and Smart Cities)?	Another international body which has national representation for setting technical standards for information technologies is at the International Telecommunications Union. We assume that the higher the score, the higher the quality of the participation the more influence the state has in setting international standards and norms in particular in ICT (as this is more government than industry driven).	https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx	Each state was given a score each its participation in each of the three study groups. The score was allocated as follows: 1 = Chairman; 0.75 = Vice Chairman; 0.5 = WP Chair; 0.25 = ITU Member State. The average of the state's participation across all three groups was taken, and the final range is between 0 and 1.
Has the state participated in bilateral or multilateral cyber defence exercises?	Demonstrates a willingness to share expertise and capacity building efforts with other states	Internet search of Government websites and reputable sources for references to participation in bi or multi-lat cyber defence exercises	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Observed in 1 or more attack: Yes/No

If Defining International Cyber Norms and Technical Standards activity is acknowledged in the state's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	See Strategy Score table
If Defining International Cyber Norms and Technical Standards activity is acknowledged in the state's national cyber strategy: include financial score	The state is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The state has announced increased cyber funding since the publication of the most recent strategy	Yes/No

Destroying or Disabling an Adversaries Infrastructure or Capabilities

Table 8.

Indicator	Meaning	Source Description	Scoring Method
Does the state's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the state has a destructive cyber capability?	Like all large bureaucracies, militaries rely on clear hierarchies and effective plans. A military can only effectively employ cyber effects if commanders understand how and when they should be used, and how they complement conventional capabilities. In addition, all militaries face opportunity costs on the capabilities they choose to procure and they would be expected to justify in national defence planning documents the value that cyber effects bring.	Analysis of the online presence of each state's Ministry of Defence (MOD) and/or Armed Forces to find relevant documents. Relevant documents include: defence plans, defence strategies, military doctrine, defence white papers, defence cyber plans, defence cyber strategies, military cyber doctrine, defence cyber white papers, statements from senior military leaders, statements from MOD politicians on the state's cyber capabilities.	Yes/No

Does the state's military cyber unit or command acknowledge that the state has a destructive cyber capability?	Having a dedicated military cyber unit or command shows that a state is seeking to enhance and grow its military cyber expertise and recruit to meet its need. Given the shortages of skilled cyber workers that all states face, cyber military units must compete to attract the very best. Military units will therefore seek to explain the role that they play and capabilities they offer.	Analysis of the online presence of each state's military cyber force to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber military leaders on the capabilities that specific military units possess.	Yes/No
Does the state's signals intelligence agency or foreign intelligence service acknowledge that the state has a destructive cyber capability?	Acknowledgement that the state's intelligence agency has a cyber mission.	Analysis of the online presence of each state's intelligence agency to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber intelligence agency leaders on the capabilities that the intelligence community possess.	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in >1 strategy: Yes/No
Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack.	Observed in 1 or more attack: Yes/No

Foreign Intelligence Collection For National Security

Table 9.

Indicator	Meaning	Source Description	Scoring Method
Does the state's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the state has cyber intelligence-gathering capability?	Like all large bureaucracies, militaries rely on clear hierarchies and effective plans. A military can only effectively employ cyber effects if commanders understand how and when they should be used, and how they complement conventional capabilities. In addition, all militaries face opportunity costs on the capabilities they choose to procure and they would be expected to justify in national defence planning documents the value that cyber effects bring.	Analysis of the online presence of each state's Ministry of Defence (MOD) and/or Armed Forces to find relevant documents. Relevant documents include: defence plans, defence strategies, military doctrine, defence white papers, defence cyber plans, defence cyber strategies, military cyber doctrine, defence cyber white papers, statements from senior military leaders, statements from MOD politicians on the state's cyber capabilities.	Yes/No
Does the state's military cyber unit or command acknowledge that the state has a cyber intelligence-gathering capability?	Having a dedicated military cyber unit or command shows that a state is seeking to enhance and grow its military cyber expertise and recruit to meet its need. Given the shortages of skilled cyber workers that all states face, cyber military units must compete to attract the very best. Military units will therefore seek to explain the role that they play and capabilities they offer.	Analysis of the online presence of each state's military cyber force to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber military leaders on the capabilities that specific military units possess.	Yes/No
Does the state's signals intelligence agency or foreign intelligence service acknowledge that the state has a cyber intelligence capability?	Acknowledgement that the state's intelligence agency has a cyber mission	Analysis of the online presence of each state's intelligence agency to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber intelligence agency leaders on the capabilities that the intelligence community possess.	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in >1 strategy: Yes/No

Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack	Observed in 1 or more attack: Yes/ No

Growing National Cyber and Commercial Technology Competence

Table 10.

Indicator	Meaning	Source Description	Scoring Method
What is the rate of participation in ISO/ IEC Joint Technical Committees for ICT?	The International Organization for Standardization (ISO) and the International Electrotechnical Commission jointly deliver consensus-based, market relevant International Standards for information technologies. Shaping and adhering to ISO/IEC JTC demonstrate a commitment to improving these elements within their own state. The higher the score the more active said state is in international standards setting which is important for its domestic industry to be interoperable with international markets.	https://www.iso.org/ technical-committees. html	# of ISO/IEC Joint Technical Committees X is a member of divided by 22 (total number of ISO/IEC JTC Committees. The score is a percentage of technical committees attended by said state.
What is the quality of participation across all 22 ISO/ IEC Joint Technical Committees?	The International Organization for Standardization (ISO) and the International Electrotechnical Commission jointly deliver consensus-based, market relevant International Standards for information technologies. Shaping and adhering to ISO/IEC JTC demonstrate a commitment to improving these elements within their own state. The higher the score the more formal authority it has had on average in the technical committees and the more that state and its industry shapes the international standards agenda in ICT.	https://www.iso.org/ technical-committees. html	Each state was given a score for each Technical Committee based on its role. The score was allocated as follows: 1 = Secretariat; 0.75 = Participant; 0.5 = Observer; 0.25 = ISO/IEC JTC Member; 0 = no affiliation. The average of its participation was then taken across all committees so the final score is between 0 and 100.

Does the state have a public-private partnership initiative to grow its domestic cyber industry, workforce, and raise awareness of cyber issues?	Private-sector organisations represent a source of capability to boost national expertise and an attack vector that adversaries can exploit. Therefore, it is important that states engage their private sectors and partner with them to tackle threats and meet national cyber objectives.	Analysis of the online presence of each state to find evidence of public-private partnerships that aim to increase the cybersecurity knowledge, skills, and focus of the state as a whole.	Yes/No
Is there evidence to show that the state has a cyber workforce strategy and/ or cyber supply chain management strategy	Building a domestic cyber workforce is critical for growing national cyber and technology competence. Therefore it is important that states develop strategies to build their cyber workforce and in lieu of that develop a cyber supply chain management strategy.	Analysis of the online presence of each state's intelligence agency to assess whether it acknowledges this objective.	Yes/No
Is the state a member of the Common Criteria Recognition Arrangement (CCRA)?	The Common Criteria is a standard that ensures that 'Information Technology (IT) products and protection profiles [and evaluations] are performed to high and consistent standards'. The CCRA offers mutual recognition of Common Criteria evaluation, allow states to export and import products and services to one another without re-evaluation.	Figures taken from: https://www.commoncriteriaportal.org/ccra/members/	Yes/No
Is the state a member of the IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)?	IECEE is a 'multilateral certification system based on IEC International Standards. Its Members use the principle of mutual recognition (reciprocal acceptance) of test results to obtain certification or approval at national levels around the world.' Joining this body removes certification barriers between states, allowing them to export and import cybersecurity and techology products	Figures taken from: https://www.iecee.org/dyn/www/f?p=106:40:0	Yes/No
Has the state published a plan or strategy on attracting inward investment towards cyber firms or growing its cyber exports?	The state is actively seeking to boost the cybersecurity industry's revenues	Internet search of Government websites to find evidence of specific advice or guidance to Cybersecurity exporters or seeking to attract foreign investors to invest in national cybersecurity products and firms	Yes/No

Is there evidence the state has invested in or funded cyber research?	Investment in R&D is an essential component of growing cybersecurity capability and capacity.	Analysis of the online presence of each state to find evidence of specific national funding of cybersecurity research, or if the state funds national universities and research establishments with cybersecurity outputs.	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in >1 strategy: Yes/No
Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack	Observed in 1 or more attack: Yes/No

Strengthening And Enhancing Cyber Defences

Table 11.

Indicator	Meaning	Source Description	Scoring Method
Has the state published a cybersecurity plan that defines how it will protect government systems and/or critical national infrastructure?	Even efforts to protect government IT systems require involvement and planning of private sector vendors. A plan or strategy will ensure a clear and consistent understanding of requirements and standards that must be met	Analysis of the online presence of each state for CNI protection plans or strategy, or plans to protect Government IT systems	Yes/No
Does the state undertake cyber awareness and cyber hygiene campaigns?	Is the state taking steps to protect its entire population and their private internet usage safe from cyber threats?	Internet search of national government websites for public outreach and advisory campaigns	Yes/No

Has the state stated it plans to undertake national active cyber defence-style effects?	Shift away from reactive national cyber defence to proactive defence [need to define this, but in essence China's great firewall, UK active cyber defence model, Russia's packet inspection, maybe Cybercom's forward defence]	Internet search of Government websites for references to national active cyber defence-type measures. Also looked for public comments by national politicians and intelligence agency/military leadership.	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in >1 strategy: Yes/No
Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack	Observed in 1 or more attack: Yes/No

Surveilling And Monitoring Domestic Groups

Table 12.

Indicator	Meaning	Source Description	Scoring Method
Does the state have at least one police or law enforcement agency with specialist cyber-crime expertise or that encourages citizens to report cyber-crime?	Shows that the state has given its law enforcement agencies the ability to prosecute cyber-crime and conduct cyber-based surveillance	Analysis of the online presence of each state for references to law enforcement expertise. Also looked for public comments by national politicians and senior police officers.	Yes/No
Does the state's domestic intelligence agency acknowledge surveillance cyber capabilities?	Acknowledgement that the state's intelligence agency has a cyber mission	Analysis of the online presence of each state's intelligence agency to assess whether it acknowledges this objective. Also looked for public comments by national politicians and senior cyber intelligence agency leaders on the capabilities that the intelligence community possess.	Yes/No

Is cyber crime, cyber terrorism, or domestic surveillance via cyber means referred to within the state's domestic counter-terrorism or homeland security strategy, plan, or law?	Shows the state is exploring cyber activity through the lens of CT and homeland security	Analysis of the online presence of each state's Minstry for the Interior or Homeland Security-focused department for national counter-terrorism or homeland security strategies, plans, and laws and whether it refers to cyber-based activities.	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	States that have pursued a particular objective over multiple strategies have demonstrated their commitment to achieve the objective. The maturity of understanding is likely to be higher.	Compare the objectives listed in the most recent strategy with those listed in the previous strategy (if one exists).	Objective present in >1 strategy: Yes/ No
Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent ('which requires preplanning and presdisposition'), it is also possible to infer general intent ('which is presumed from the act of commission (such as speeding)') from the actions of a state.	Use CFR Cyber Operations Tracker figures to assess whether a state has been attributed as conducting 1 or more attack	Observed in 1 or more attack: Yes/ No

C.2 **Intent Quality Of Strategy Assessment**

Table 13.

Score	Explainer
1	General Overview of Threats and Priorities
2	Detailed Analysis of Threats and Clearly Articulated Priorities
3	Division of Responsibilities between government departments
4	Detailed timeline OR success criteria
5	Detailed timeline AND success criteria
-1	Strategy not updated in past 5 years OR since expiration

Annex D: Capability Indicators

D.1 Detailed Explanation of Capability Indicators Mapping by Objective

Table 14.

#	Indicator	Amassing and Protecting Wealth	Information Control	International Cyber Norms	Disabling Adversary Infrastructure	Intelligence Collection	Growing National Cyber and Tech Competence	National Cyber Defense	Domestic Surveillance /Monitoring	Objective(s) Mapping Explanation
	Total	4	10	8	7	8	10	9	8	
1	Awareness of cybersecurity and risk literacy					✓	✓	✓		Measure the population's cybersecurity knowledge to defend against attacks and conduct safe cyber practices.
2	Bilateral Cyber Agreements			✓						International cyber norm-setting can be measured by how active a state has been in creating informal and formal statements of international collaboration.
3	Computer Infection Rates							✓		The more computers that can be affected by non-state-sponsored malware, the more vulnerable national cyber defense likely is.
4	Cyber Capacity building / foreign aid projects			✓						International cyber norm-setting can be measured by how active a state has been in promoting cyber-capacities in other states.
5	Cyber Military Staffing				✓	✓				It identifies the number of publicly acknowledged personnel assigned to military cyber roles.

6	Cyber Security Laws			✓				✓		Cybersecurity laws allow a state to better control the data of its own population, interact with other states, bolster defense, as well as set precedent for how they will interact with foreign partnerships.
7	Data Privacy Laws and Govern-ance								✓	Data privacy laws allow a state to better control the data of its own population, interact with other states, bolster defense, as well as set precedent for how they will interact with foreign partnerships.
8	Ecomm-erce economy						✓			More e-commerce sales allow more revenue into the state's private sector retailers, growing the domestic economy.
9	Existence of Cyber-security Incident Response Teams (CSIRTs)							✓		The existence of a CSIRT is an indicator that the state has provided resources to mitigating cyber vulnerabilities and related crises.
10	Freedom On The Net Score		✓						✓	The less freedom on the net there is within a state, the more likely it is that the government is effectively able to surveil and monitor its citizens, and the more likely it is that the state can effectively control information flow.
11	Global Soft Power		✓							The more soft power a state has, the more it can influence others in adopting or maintaining international norms.
12	Global Top 100 Technology Firms			✓			✓			A state's technology firms grow its domestic industry and influences the industries of states abroad, especially if the firm has a large number of foreign users.
13	Global Top 150 Cyber-security Firms				✓	✓	✓	✓		The greater number of cybersecurity ventures headquartered within a state, the greater the cybersecurity industry grows.

14	High Impact State-Sponsored Attacks	✓	✓		✓	✓	✓		✓	Sophisticated state-sponsored cyber attacks are defined as those with on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars. Similar to the general state-sponsored attacks indicator, this measures a state's initiative and sophisitication in achieving their objectives.
15	High-tech Exports			✓	✓	✓	✓			Exporting high-tech products to a foreign state can benefit a state's economy, and (depending on the state) may allow foreign intelligence access to the data the products collect on foreign citizens. This can result in foreign dependence on the high tech export, which could cause adversary capabilities to slow or halt if the exports stop.
16	ICT Imports						✓	✓		The more information and communication technology that is imported, the market need for domestic solutions may decrease, and the state may incur higher supply chain risk within its domestic cyber infrastructure.
17	Mobile infection \ Rates							✓		The more devices that can be affected by non-state-sponsored malware, the more vulnerable national cyber defense likely is.
18	Multilateral Cyber Agree-ments			✓						International cyber norm-setting can be measured by how active a state has been in creating informal and formal statements of international collaboration. Multilateral agreements demonstrate consensus building between multiple states

19	National Cyber Command				✓					Centralised Cyber Commands allow national governments to coordinate and harness multiple cyber capabilities to deploy military cyber means when needed.
20	Patent Applica-tions			✓			✓			The more patent applications exist within a state demonstrates innovation within the state's workforce, which may lead to commercial gain.
21	Population % on Social Media		✓						✓	The greater number of citizens using social media, the more likely their data will be on the internet, causing more individuals to be affected by domestic surveillance or data laws. However, more individuals on social media (in many cases) may result in a greater amount of the domestic populace vulnerable to foreign disinformation campaigns.
22	Population % on the internet		✓					✓	✓	The greater number of citizens using the internet, the more likely their data will be on the internet, causing more individuals to be affected by domestic surveillance or data laws. However, more individuals on the internet (in many cases) may result in a greater amount of the domestic populace vulnerable to foreign disinformation campaigns, cybercrime or cyber espionage attempts.

23	Private Sector Surveill-ance Companies		✓		✓	✓			✓	NEW State surveillance capabilities are increasingly purcahsed to improve interception and intrusion technologies from private firms for intelligence and surveillance purposes. The more of these surveillance technologies that are developed by private companies in a state, the more a state has access to these technologies.
24	Size of National Standards Bodies			✓						The size of the National Standards Bodies can indicate how much attention and effort is invested in setting cybernorms.
25	State-Sponsored Attacks	✓	✓		✓	✓	✓		✓	State-sponsored cyber attacks allow a state to collect foreign intelligence, conduct corporate espionage, surveil dissidents, spread disinformation, and disable adversary infrastructure.
26	Successful Google Content Removal Requests		✓							The more successful Google content removal requests demonstrate that a state has effectively taken down information on the internet, demonstrating an amount of control over the information space.
27	Top News Sites		✓							More internationally trafficked news sites headquartered within a state gives the state more power to push common narratives or ideals popular within a given state on the Internet.

28	Top Websites		✓			✓	✓			More internationally trafficked websites with corporations headquartered within a state gives the state more power to push common narratives or ideals popular within a given state on the Internet, and also allow the corporation that owns the website to generate more ad revenue or deliver more product to consumers.
29	Vulner-abilities in Domestic Machines							✓		The more vulnerable a state's computers are in general, the more susceptable to attack a state may be.

D.2 **Capability Indicators Scoring Explained**

Table 15.

#	Indicator	Meaning	Source	Year	Scoring Method
1	Awareness of Cybersecurity and Risk Literacy	State scores in the Global Cyber Risk Literacy	Oliver Wyman Forum	2021	The scores were calculated by Oliver Wyman Forum. These same scores were used for the Belfer Cyber Power Index.
2	Bilateral Cyber Agreements	Number and quality of bilteral formal and/ or informal agreements signed by the national government in cyberspace, scored by recency.	Harvard Belfer National Cyber Power Project	2022	For each of the agreements between states: 1 = meeting, remarks 2 = Joint Statement, cooperation, framework 3 =Agreement / MOU
3	Computer Infection Rates	Percentage of computers in state that are infected with malware	Comparitech	2021	Percentage of computers found to have a malware infection
4	Cyber Capacity building / foreign aid projects	An analysis of past and present international cyber capacity building projects	Harvard Belfer National Cyber Power Project	2022	The projects listed on the Cybil Portal were analysed by the Belfer National Cyber Power Index team. The more cyber capacity building projects, the higher the score for the state.
5	Cyber Military Staffing	Number of individuals in staff positions for military's cyber forces	Harvard Belfer National Cyber Power Project	2021	Number of individuals that are reported in open source that are working on cyber units of militaries.

6	Cybersecurity Laws	Measurement of how active a state has been in implementing content, privacy, and cybercrime laws	Harvard Belfer National Cyber Power Project	2021	0= no laws; 1= laws that cover one of the following: content, privacy, and crime 2= laws that cover two of the following: content, privacy, and crime 3= laws that cover content, privacy, and crime, outdated (< yr 2000) 4= laws that cover content, privacy and cybersecurity, recent update (>= yr 2000)
7	Data Privacy Laws and Governance	An analysis of data privacy laws in a state	DLA Piper	2021	The scores and analysis were undertaken by DLA Piper. The higher the score, the better legal provisions in place to protect personal data
8	E-Commerce Economy	National E-commerce sales as a percentage of GDP	Statista, UNCTAD and others	2021	Higher score indicates more e-commerce sales.
9	Existence of Cybersecurity Incident Response Teams (CSIRTs)	Existence of a Cybersecurity Incidence Response Team	Harvard Belfer National Cyber Power Project	2021	0 = no response team 1= plans to establish a CSIRT 2 = new national CSIRT team (less or equal 5 years) 3 = established national CSIRT team (more than 5 years) 4 = established national CSIRT team (more than 5 years) + member of the first response team
10	Freedom on the Net	Freedom House's score for how free citizens are online	Freedom House & Freedom of the World	2021	0-100: 3 separate scores aggregated together: a) obstacles to access b) limits on content c) violations of users' rights. For seven states we used freedom of the World rankings because Freedom House did not have the information.

11	Global Soft Power	State scores in the Global Soft Power Index	Brand Finance	2021	The scores calculated by Brand Finance's was part of their Soft Power index. These same scores were used for the Belfer National Cyber Power Index.
12	Global Top 100 Technology Firms	Number of Global Top 100 tech firms headquartered in state.	Thomson Reuters	2021	Count of top tech firms per state
13	Global Top 150 Cybersecurity Firms	Number of global top cybersecurity firms headquartered in state	Cybersecurity Ventures	2021	Number of Top 150 cybersecurity firms listed in the ranking.
14	High Impact State Sponsored Cyber Attacks	Number of publicly attributed cyber attacks	CSIS	2022	Count of cyberattacks attributed to state sponsored actors.
15	High Tech Exports	Percentage of high-tech exports as total of manufacturing exports	World Bank	2021	Higher values indicate more technology exports.
16	ICT Imports	ICT imports as a percentage of total imports	UNCTAD	2019	Higher number indicates higher dependence on imports, and puts a state's cyber defence at more risk of adversary intrusion
17	Mobile Infection Rates	Percentage of mobiles in state that are infected with malware	Comparitech	2021	Percentage of users' computers found to have a malware infection
18	Multilateral Cyber Agreements	Number and quality of multilateral formal and/ or informal agreements signed by the national government in cyberspace, scored by recency.	Harvard Belfer National Cyber Power Project	2021	For each of the agreements between states: 1 = informal/ conference / regional 2 = informal / conference / Global 3 = Formal Regional Agreement / Member of Regional Org 4 = Formal multilateral Agreement / Member of Global Org

19	National Cyber Command	The existence and age of a national cyber command.	Harvard Belfer National Cyber Power Project	2021	0 = no cyber command 1= plans to establish a cyber command 2 = new cyber command (less or equal 2 years) 3 = established cyber command (2-5 years) 4 = established cyber command (more than 5 years)
20	Patent Applications	Number of domestic patent filings by residents of that state	World Development Indicators	2019	Number of domestic patent filings (residents only). Per capita measure.
21	Population % on Social Media	Percentage of active social media accounts	Statista and others	2021	Share of internet users visiting social networking sites.
22	Population % on the Internet	Internet penetration rate within a state.	Statista and others	2021	Higher the more individuals use the internet
23	Private Sector Surveillance Companies	Number of private sector surveillance companies operating in state, presenting in international arms fairs	Atlantic Council	2021	Count of the number of surveillance companies that operate in a state that attended selected international arms fairs
24	Size of National Standards Bodies	Number of staff working in a state's national standards body	Harvard Belfer National Cyber Power Project	2021	Higher number indicates more people working in the state's national standards body
25	State Sponsored Cyber Attacks	Number of publicly attributed cyber attacks	CFR	2022	Count of cyberattacks attributed to state sponsored actors.
26	Successful Google Content Removal Requests	Number of takedown requests to Google from a government entity	Google	2020 -2021	Number of requests
27	Top News Sites	Number of news sites in the Similarweb Top 50 news sites listing that belong to organizations with their HQ in that state	Similarweb	2021	Number of sites in the Top 50
28	Top Websites	Number of websites in the Similarweb Top 50 websites listing that belong to organizations with their HQ in that state	Similarweb	2021	Number of sites in the Top 50
29	Vulnerabilities in Domestic Machines	Cumulative percentage of the vulnerabilities listed for a state's infrastructure in the Shodan database	Harvard Belfer National Cyber Power Project	2021	Cumulative percentage of the Shodan search results.

Cyber Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/project/cyber-project