CHINA CYBER POLICY INITIATIVE

National Cyber Power Index 2020

Methodology and Analytical Considerations

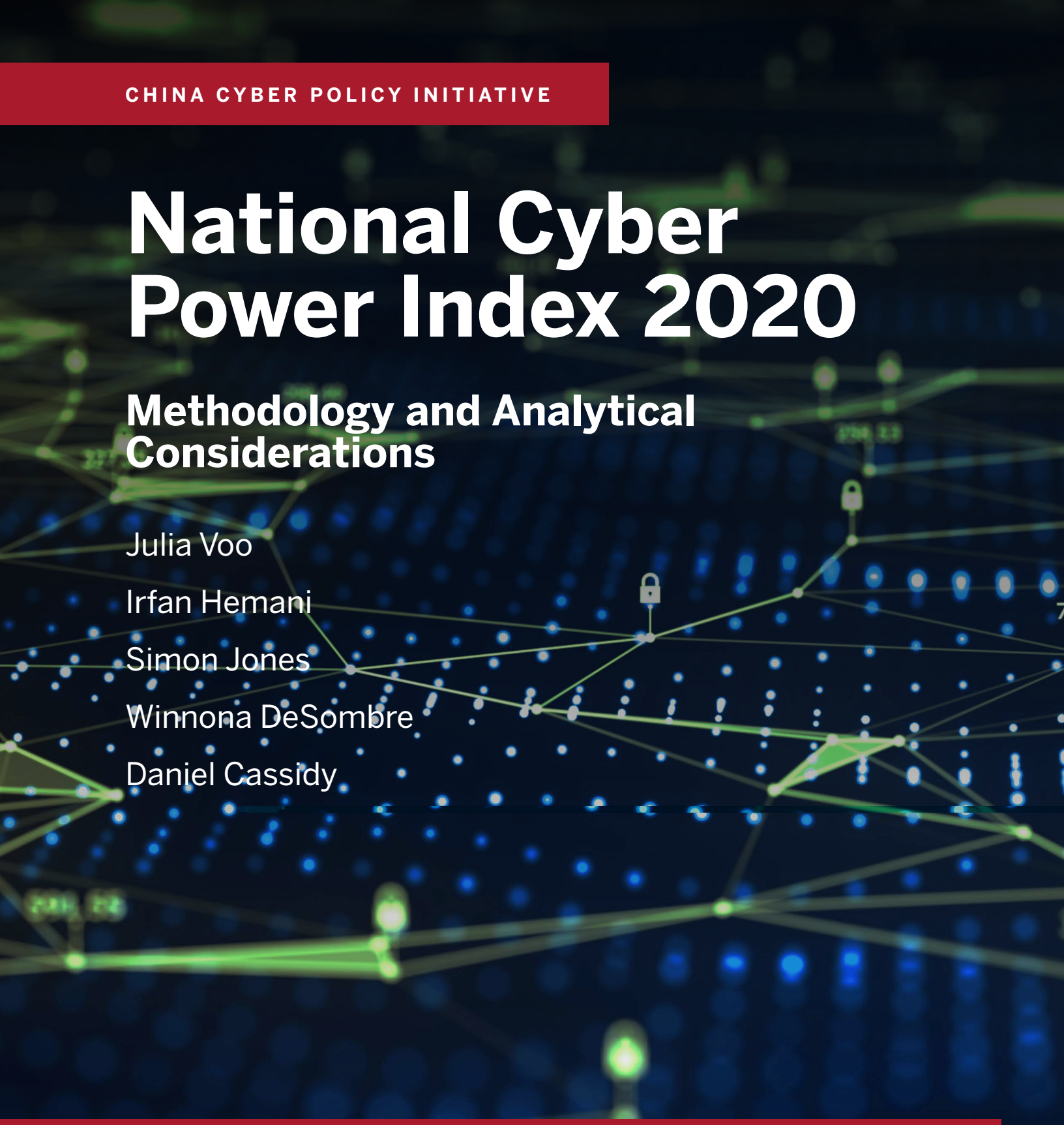
Julia Voo

Irfan Hemani

Simon Jones

Winnona DeSombre

Daniel Cassidy



HARVARD Kennedy School
CENTER
for Science and International Affairs

REPORT
SEPTEMBER 2020

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

www.belfercenter.org/CCPI

Design and layout by Andrew Facini

CHINA CYBER POLICY INITIATIVE

National Cyber Power Index 2020

Methodology and Analytical Considerations

Julia Voo

Irfan Hemani

Simon Jones

Winnona DeSombre

Daniel Cassidy

Anina Schwarzenbach

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
SEPTEMBER 2020

The Cyber Power Team

Julia Voo is the Belfer Center's Research Director for the China Cyber Policy Initiative

Irfan Hemani is the Head of the Security, Strategy and International in the UK Government's Cyber Security Policy Team and a non-resident Fellow

Simon Jones is the Director of Information for Massachusetts' Executive Office of Energy and Environment Affairs and a non-resident Fellow

Winnona DeSombre is a private sector threat intelligence researcher and a non-resident Fellow

Dan Cassidy is a strategy and crisis management expert in the UK Government and a non-resident Fellow

Anina Schwarzenbach is a Postdoctoral Fellow with the Belfer Center's International Security Program

Acknowledgements:

We would like to thank Eric Rosenbach for his mentorship, guidance, and support for the past year and more. Professor Jim Waldo for his all encouragement, humor, and challenge. James Shires, for his thoughts from day one (when it looked completely different) and for all his feedback since.

We are deeply appreciative for the methodological advice from Steve Worthington at Harvard's Institute for Quantitative Social Science.

Finally, much gratitude and affection for the advice and support from the larger Belfer Cyber Project family specifically Lauren Zabierek, Marcus Comiter, Utsav Sohoni, and Ariel Herbert Voss.

A Note to Readers

Which is the most powerful cyber nation in the world? That is the research question that a smart, creative, and hard-working team from the Belfer Center for Science and International Affairs at the Harvard Kennedy School seeks to answer with this innovative and intellectually illuminating study on cyber power. This is important work in both academia and the real world: the study threads the needle of providing robust academic insights in a policy-relevant model.

State-backed cyber actors are one of the greatest threats to national security. While leading the Department of Defense's efforts to counter cyber-attacks by Russia on our elections, North Korea's attacks on US critical infrastructure, and China's theft of America's intellectual property, I saw firsthand the range of objectives that states pursue through cyber means.

The canonical cyber-attacks of the past decade are one important source of data that illustrates the effort by states to extend their influence and power in the cyber domain. Through diplomatic efforts at the UN, however, some states increase their cyber power by hoping to proliferate their own authoritarian models of internet governance. In other fora, state representatives seek to shape the technical standards that govern the fabric of the internet to gain dominance in the geopolitics of technology and information.

Some of these actions are legitimate and constructive; others lie in a grey "space between" where international law and norms are still nascent. And a few are clearly malicious. But one thing is clear: these actions all contribute to a nation's overall ability to achieve national objectives, which is power in its most traditional form.

The underlying variables that contribute to cyber power are poorly understood. It is too easy to miss the full spectrum of intentions and capabilities that contribute to a state's cyber power. Understanding this spectrum is critical for improving a state's overall cyber strategy and policy.

As the Assistant Secretary of Defense in charge of cyber policy, I consistently sought and applied analytical methods to assess the various cyber threats to US national security. Quantitative models can sometimes lead to results that are not intuitive. For example, many would instinctively describe North Korea as presenting a high cyber threat to the US and would therefore determine it has high levels of overall cyber power. But closer inspection of the various facets of cyber power show the DPRK to be a weak actor in many key areas.

In this study, the Belfer Center team has produced the best model to-date for assessing cyber power. Their work is impressive: they developed and applied rigorous quantitative and qualitative models, reviewed over 1000 existing sources of data, compiled and developed 27 unique indicators to measure a states' cyber capabilities, and now host one of the best databases on cyber issues in the world.

The Belfer Center's mission is to provide leadership in advancing knowledge of critical policy-relevant knowledge of important international security issues. The National Cyber Power Index does just that. I urge policymakers around the world to use the NCPI to not only inform their cyber policy discussions but also as a template for improving their country's cyber posture going forwards.

I am proud of this team who questioned conventional wisdom and unpacked a complex policy problem with creativity and rigor. We should all be grateful for their contribution to better understanding the cyber domain.

—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

The Belfer National Cyber Power Index (NCPI) measures 30 countries' cyber capabilities in the context of seven national objectives, using 32 intent indicators and 27 capability indicators with evidence collected from publicly available data.

In contrast to existing cyber related indices, we believe there is no single measure of cyber power. Cyber Power is made up of multiple components and should be considered in the context of a country's national objectives. We take an all-of-country approach to measuring cyber power. By considering "all-of-country" we include all aspects under the control of a government where possible.[1] Within the NCPI we measure government strategies, capabilities for defense *and* offense, resource allocation, the private sector, workforce, and innovation. Our assessment is both a measurement of proven power and potential, where the final score assumes that the government of that country can wield these capabilities effectively.

The NCPI has identified seven national objectives that countries pursue using cyber means. The seven objectives are:

1. Surveilling and Monitoring Domestic Groups;
2. Strengthening and Enhancing National Cyber Defenses;
3. Controlling and Manipulating the Information Environment;
4. Foreign Intelligence Collection for National Security;
5. Commercial Gain or Enhancing Domestic Industry Growth;
6. Destroying or Disabling an Adversary's Infrastructure and Capabilities; and,
7. Defining International Cyber Norms and Technical Standards.

In contrast to the broadly held view that cyber power means destroying or disabling an adversary's infrastructure (commonly referred to as offensive cyber operations), offense is only one of these seven objectives countries pursue using cyber means.

1 We do not include non-state actors in our ranking.

The overall NCPI assessment measures the "comprehensiveness" of a country as a cyber actor. Comprehensiveness, in the context of NCPI, refers to a country's use of cyber to achieve multiple objectives as opposed to a few. The most comprehensive cyber power is the country that has (1) the intent to pursue multiple national objectives using cyber means and (2) the capabilities to achieves those objective(s).

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

The NCPI 2020's Most Comprehensive Cyber Powers across all seven objectives are, from 1st to 10th: US, China, UK, Russia, Netherlands, France, Germany, Canada, Japan, Australia.

We present three different indices. The NCPI, the Cyber Intent Index (CII), and the Cyber Capability Index (CCI). Both the CII and CCI are standalone measures. The NCPI is a combination of CII and CCI.

We recognize that national cyber objectives are not composed in isolation: cyber capabilities are just one of the suite of tools, i.e. alongside traditional military means, diplomacy, public policy, punitive measures, and trade policy, available for countries to employ to achieve their national objectives.

The NCPI builds on existing databases that measure specific elements of cyber power and collates this data with multiple indicators that were sourced in-house. Our data analyses followed a rigorous methodology and procedure, all of which are available upon request.

We verified our analysis of national cyber strategies using natural language processing. We have correlated the NCPI composite indicator with relevant measurable phenomena (similar composite indicators but also relevant quantities e.g. GDP/capita, International Telecommunications Union Cybersecurity Index etc.) to identify similarities or differences.

The Cyber Intent Index reflects the different prioritization that some countries place on developing specific objectives and are therefore more important to their conceptualization of cyber power than others.

For the DPRK we could not find reliable measurements for many of the capabilities listed in our index. We have therefore asked several experts to provide us with their assessments of the different capabilities as they relate to the DPRK to inform the NCPI. Researchers and practitioners should bear in mind that the DPRK is a special case when referencing its NCPI score in comparison to the other countries in this index.

We have used a Min-Max normalization technique to rescale the cyber capability indicators because it: (1) best reflects our conceptual framework; (2) is most appropriate for the data properties; and, (3) can be easily interpreted by users. The intent part of our formula can be considered as equivalent to a weight.

Researchers and practitioners should use the NCPI to gain a more comprehensive understanding of the components that comprise cyber power and how cyber means can be employed to achieve a range of objectives. Users who are interested in a specific national objective can analyze the NCPI by both intent and capabilities by objective to better understand their country of interest.

In this paper we contrast the NCPI with existing cyber-related indices, outline our conceptual framework, provide guidance on how to interpret our findings, share the methodology for scoring intent, capabilities and the composite indicator, list the sources we used, and provide an overview of the limitations of our approach.

The purpose of the NCPI is to broaden the discussion on cyber power to reflect that it can be applied to achieve more than destructive capabilities and that it is an important tool for governments to achieve multiple objectives. We believe that further transparency around national cyber objectives and capabilities is needed to make more relevant and effective policy and prevent dangerous escalation between countries. We hope that the NCPI helps move the discussion on cyber power and the utility of increased transparency around capabilities, forward.

1. Introduction

The public is informed of the cyber impacts of only a handful of countries: notably U.S., Israel, Iran, China, Russia and DPRK. Most news coverage reports on only the large-scale or dramatic offensive cyber-attacks. This is a misrepresentation of the full schope of the capabilities, objectives, and the range of actors in cyber space. Additionally, when reporting on these, there is no systematic measure or comparison of even this narrow range of cyber capability.

1.1 Objective of Belfer's NCPI 2020

The objective of the Belfer 2020 National Cyber Power Index (NCPI) is to provide a more complete measure of cyber power than existing indices.

We take an all-of-country approach to measuring cyber power. By considering "all-of-country" we include all aspects under the control of a government where possible. [2] Within the NCPI we measure government strategies, capabilities for defense *and* offense, resource allocation, the private sector, workforce, and innovation. Our assessment is both a measurement of proven power and potential, where the final score assumes that the government of that country can wield these capabilities effectively.

In contrast to existing cyber power indices, we dispute the notion that there is an absolute measure of cyber power and propose multiple components of cyber power. Furthermore, any measure of cyber power should be considered in relation to the national objectives of the country in question and their decision to use cyber means to achieve those objectives.

We have identified seven national objectives that countries pursue using cyber means. The NCPI considers cyber power within the context of these seven national objectives. No other ranking of cyber power does this.

2 We do not include non-state actors in our ranking.

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

We then measure a country's capability within each objective. The indicators we consider are in line with widely accepted definitions of cyber power within national security. For example, a cyber power has been described as "a country who is world class in safeguarding the cyber health of citizens, businesses and institutions; has the legal, ethical and regulatory regimes to foster public trust; and the ability to project cyber power to disrupt, deny or degrade adversaries".[3] However, we recognize that national objectives pursued using cyber means are not composed in isolation. Cyber capabilities are just one of a country's suite of tools, i.e. alongside traditional military means, diplomacy, sanctions, and tariffs, that are available for countries to deploy to achieve their national objectives.

Cyber power in the context of the NCPI is when a country effectively develops cyber capabilities to achieve its national objectives.[4] To differentiate between levels of intent and capability between countries across all objectives we assign the term "comprehensiveness" to describe a country's use of cyber to achieve multiple objectives as opposed to a few.

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

- Has the intent to pursue multiple national objectives using cyber means
- Has the essential 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 country is pursuing the least objectives using cyber means with the lowest level of intent and capability.

3 Jeremy Fleming, Director GCHQ, "Keynote Speech: The UK is a Global Cyber Power". *International Institute of Strategic Studies, Singapore*. Published February 25, 2019.

4 Voo, Julia., Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. "Reconceptualizing Cyber Power". *Belfer Policy Paper.* Published April 2020.

The NCPI scores 30 countries[5] against our unique framework. The selection of these countries grew out of the teams' original query of the often-cited five cyber superpowers,[6] countries with attributed APT groups,[7] and rumored rising cyber powers. Due to limited resources and access to open source data we were unable to include many more countries. The countries included in the NCPI have indicated, either overtly or covertly, their desire to be considered as a cyber power.

We opted for a transparent approach and provide a disaggregated measure that builds on both publicly available data and expert assessments. In this paper we contrast the NCPI with existing cyber power indices, outline our conceptual framework, provide guidance on how to interpret our findings, share the methodology for scoring intent, capabilities and the composite indicator, list the sources we used, and provide an overview of the limitations of our approach.

The NCPI provides a new conceptual framework and data to the discussion on cyber power. A better-informed understanding of which countries are and are not pursuing certain objectives and capabilities using cyber means will contribute to relevant, and more effective long-term strategies.

1.2 Contrasting the NCPI with Existing Cyber Indices

Over the past decade, several organizations have provided measures for an aspect of national cyber power. In this section, we provide a high-level conceptual comparison of the NCPI with three widely used frameworks for measuring cyber power. These three widely used frameworks are listed below:

5 The 30 countries are: Australia, Brazil, Canada, China, Democratic People's Republic of Korea (DPRK), Egypt, Estonia, France, Germany, India, Iran, Israel, Italy, Japan, Lithuania, Malaysia, Netherlands, New Zealand, South Korea, Russia, Saudi Arabia, Singapore, Spain, Sweden, Switzerland, Turkey, Ukraine, UK, USA, and Vietnam.

6 US, UK, Israel, China, and Russia. As highlighted in Voo, Julia., Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach. "Reconceptualizing Cyber Power". *Belfer Policy Paper.* Published April 2020.

7 The Five Eyes is an intelligence (signals, human, military) alliance between Australia, Canada, New Zealand, UK, and US

- The International Telecommunications Union (ITU)'s Global Cybersecurity Index[8] (GCI) has been released three times in the past decade. The ITU is a body of the United Nations and it is the oldest global international organization. The GCI is designed to encourage the development of international cyber resilience among ITU member states. It focuses on domestic cyber resilience and is based on members states' self-assessments.
- The Potomac Institute's Cyber Readiness Index 2.0 (CRI 2.0) [9] is designed to evaluate a country's maturity and commitment to securing its national cyber infrastructure and services. CRI 2.0 examines 125 countries (including: the top 75 countries from the ITU ICT Development Index and G20). Notably, the CRI 2.0 does not assign a score or a rank to the countries it analyses.
- The Economist Intelligence Unit & Booz Allen Hamilton (EIU & Booz) developed a "cyber power index" (CPI) in 2011[10] ranking 19 of the G20 countries.[11] In contrast to the other two indices that exclusively measure cyber security related capabilities, the CPI purports to provide a broader measure of cyber power. However, it is worth noting that the CPI, in contrast to Belfer's NCPI, does not measure offensive capabilities, and focuses largely on economic and resource indicators—which although are important to understanding the potential for developing cyber power does not provide the fullest picture of cyber capabilities.

Table 1 compares NCPI's ranking of the top ten cyber powers with the ranking provided by ITU (2018) and the Economist Intelligence Unit (2011). The Potomac Institute's ranking is not included because their index does not score or rank countries.

Table 2 compares the high-level concepts that comprise the NCPI with the three other indices.

8 International Telecommunicationdc Globcl Cyb(er)95 (6)9 (curitr)13 (y nude223(x.)]TJ /T1_2 1 Tf- 0.10 Tc 0.10 w [( )30 Ac)10 c

Table 1: Top-10 Comparison

#	Belfer Center: **National Cyber Power Index 2020**	International Telecommunications Union: **Global Cyber Security Index 2018**	Economist Intelligence Unit & Booz Allen Hamilton: **Cyber Power Index 2011**
1	United States	United Kingdom	United Kingdom
2	China	United States	United States
3	United Kingdom	France	Australia
4	Russia	Lithuania	Germany
5	Netherlands	Estonia	Canada
6	France	Singapore	France
7	Germany	Spain	South Korea
8	Canada	Malaysia	Japan
9	Japan	Canada	Italy
10	Australia	Norway	Brazil

Table 2: Concept Comparison

	Belfer Center: **National Cyber Power Index 2020**	International Telecommunications Union: **Global Cyber Security Index 2018**	Potomac Institute: **Cyber Readiness Index 2.0**	Economist Intelligence Unit & Booz Allen Hamilton: **Cyber Power Index 2011**
Year(s) Published	2020	2018	2015	2011
Iterations	1	3	2	1
Objective	To measure the cyber power of countries against their stated objectives	To measure the commitment of countries to increase their domestic security	To measure a country's commitment to securing its national cyber infrastructure and services	To measure cyber power by country
Countries Assessed	30	193 (2018)	125	19
Indicators	27 Capability; 32 Intent	25	7	39
Score	X	X		X
Ranking	X	X		X
Themes:				
National Objectives Drive Capability Development	X			
Evidence of Attacks	X			
National Online Content	X			
Domestic State Cyber Structures	X	X	X	X
Cyber Vulnerability Mitigation	X	X	X	X
Private Sector, Trade and Innovation	X	X	X	X
Connectivity	X	X	X	X
Workforce	X	X	X	X
Domestic and International Legal and Policy Frameworks	X	X	X	X

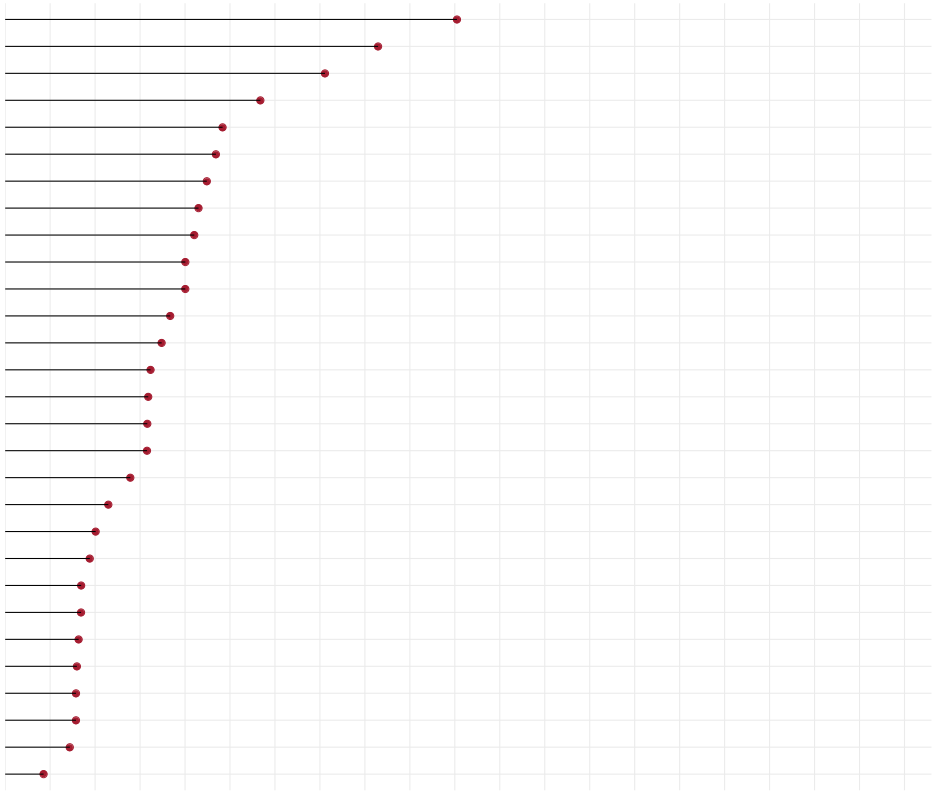
This comparison demonstrates that the NCPI uniquely provides a rigorous assessment of each country's national objectives that they seek to carry out with cyber means. Furthermore, that the NCPI considers both concepts that have been traditionally linked to assessments of cyber power and concepts that have so far been neglected by previous assessments.

2. National Cyber Power Index 2020

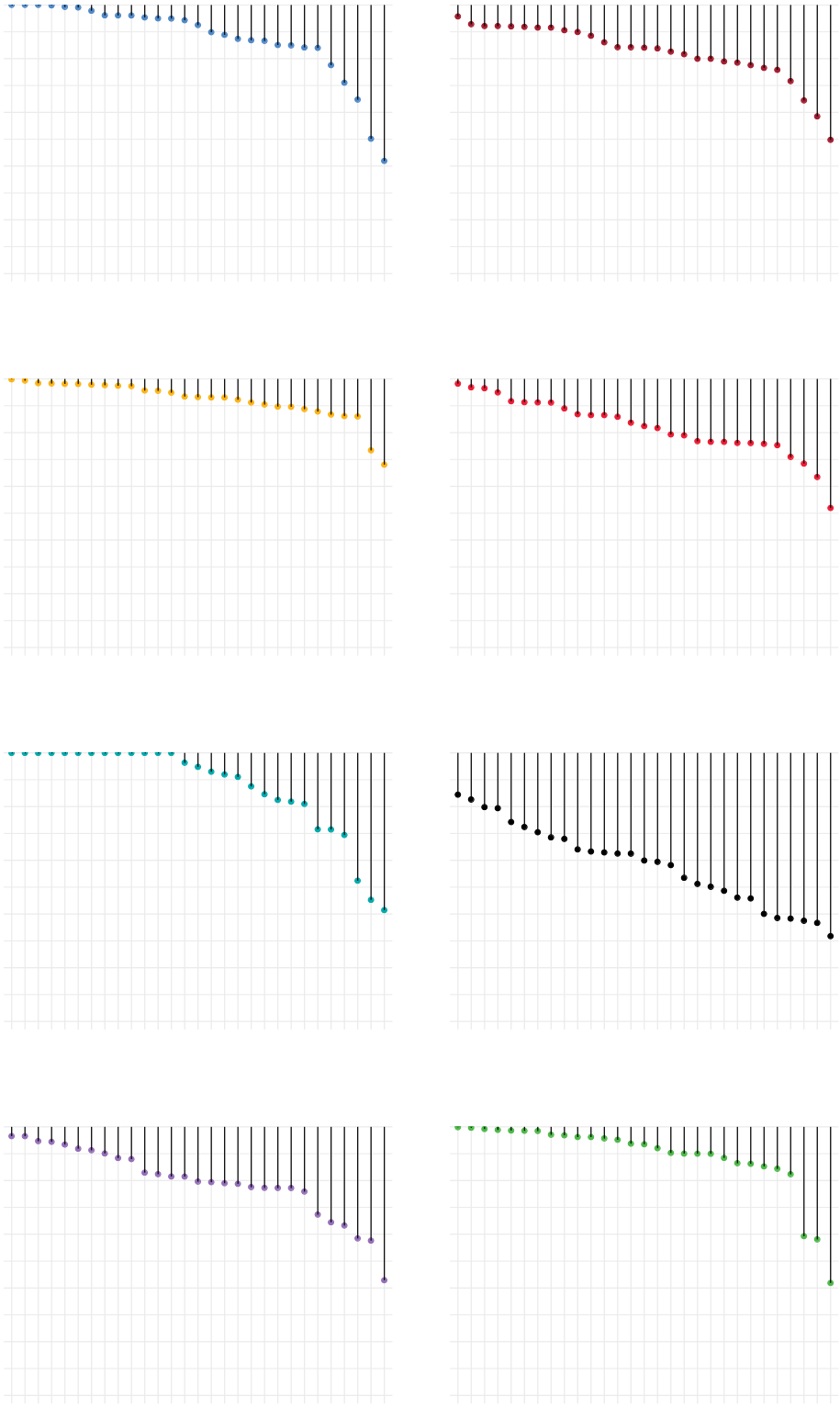
As seen in Graph 1, the top ten most comprehensive countries with the highest level of intent and capabilities across all seven objectives are as follows. Graph 2 shows a breakdown of the rankings by objective.

1. United States
2. China
3. United Kingdom
4. Russia
5. Netherlands
6. France
7. Germany
8. Canada
9. Japan
10. Australia

Graph 1: NCPI 2020: Most Comprehensive Cyber Powers



Graph 2: NCPI 2020 By National Objective

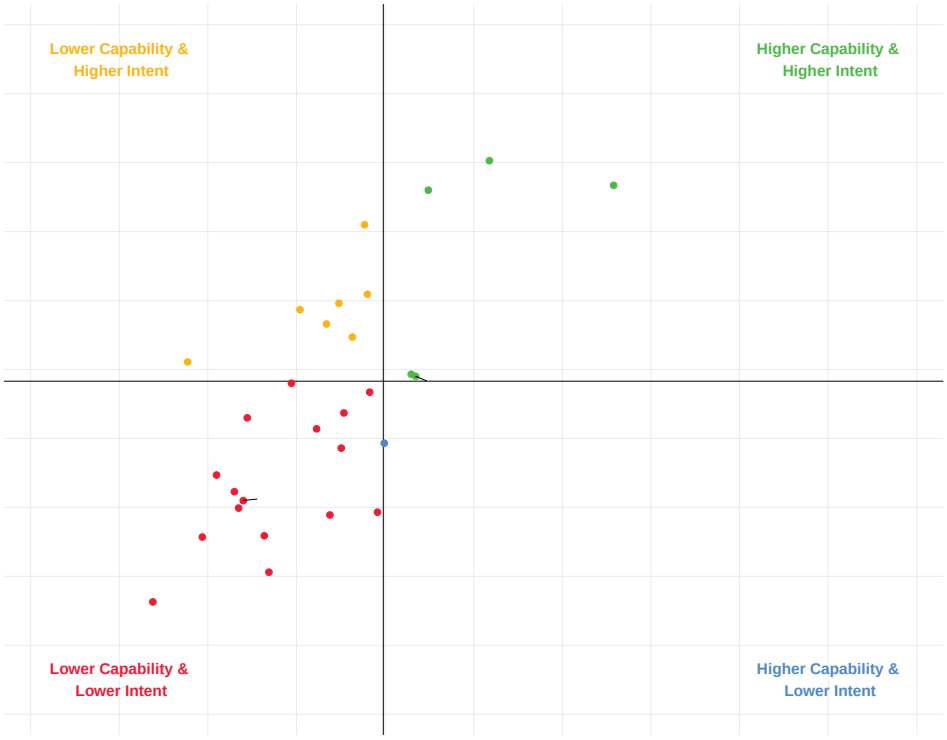


2.1 Interpreting the National Cyber Power Index 2020

Researchers and practitioners may use the NCPI in different ways. First, they might use the NCPI's aggregated measure of cyber power across all seven objectives to understand which country is the most comprehensive cyber power, as seen in Graph 1. Graph 1 favors countries that had high scores on both intent and capability for multiple cyber objectives, which leads us to assess that these countries are effectively using cyber means to achieve multiple policy goals. Each country has a different score based on each objective.

Because our analysis of cyber power is the product of intent and capability, we can plot countries within each objective into the following four quadrants seen in Graph 3. Note that we have drawn the quadrants on the mean values of intent and capability (the maximum value achieved by any country in the dataset was an intent score of 100 and a capability score of 80). Most of the countries cluster around the middle of the plot.

Graph 3: Plot of Cyber Power Rankings across Capability and Intent



Higher Capability, Higher Intent

E.g. US, UK, China, France, Germany

Countries with high levels of both intent and capability for a specific objective (or for multiple objectives as seen in Graph 1), are among the highest-ranking countries in the NCPI. These countries both signal in strategies and in previously attributed cyber-attacks that they intend to use cyber to achieve policy goals and have the capabilities to achieve them.

Higher Capability, Lower Intent

E.g. South Korea

Countries with high levels of capability, but low levels of intent for a specific objective or set objectives fall under two possibilities. The country in question may be trying to actively avoid a specific goal. For example, because the United States is home to multiple large-scale social media companies, passing legislation to better control online speech would be an effective way for the US to control online content for domestic audiences. However, because the United States strongly adheres to the right to freedom of speech enshrined in the First Amendment to its Constitution it likely has little intention to do so. The other possibility is that the country in question may be trying to use its cyber capabilities in secret, without openly stating that they intend to use cyber capabilities for specific goals.

Higher Intent, Lower Capability

E.g. Russia, Iran, Israel, Netherlands

These countries are actively signaling to other states that they intend to develop their cyber capabilities but have either a) not publicly disclosed their capabilities (through stated or demonstrated means), or b) do not currently have the capabilities at hand to achieve their cyber goals.

As for the latter, while they may be openly signaling future plans, these countries do not have the capability to become a comprehensive cyber power at present. For example, the Netherlands has stated their intent to "use... offensive capabilities and a broader response in the cyber domain",[12] especially against disruptive cyber actors, in their 2018 national cyber strategy.[13]

In addition, Iran has been credited for conducting multiple cyber-attacks which indicate that it has been aggressively pursuing some objectives through cyberspace. However, it was one of the lowest scoring nations with regards to its capabilities surrounding norms, cyber defenses, commercial gain, and information control beyond its borders, which are all weighted equally to offense in the NCPI.

Lower Intent, Lower Capability

E.g. Egypt, Lithuania

Countries that fall into this category either are not actively developing the capability and intent to project power in cyberspace, or have not published (or had published about them) a sufficient amount of information on their cyber strategy, cyber-attacks attributed to them, or capabilities used to measure cyber power in this study.

Country-specific analysis has been displayed through use of radar charts in the Annex. Individuals interested in a specific national objective within NCPI can view the data sources we have selected for capability or intent that contribute to the specific objectives in Chapters 3 and 4. In addition to viewing the overall comprehensiveness score we recommend that policy makers consider the capability and intent scores separately for any country of interest, as well as its overall score.

12 Netherlands National Cyber Security Strategy 2014, see https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1

13 The Netherlands proved their capabilities not just by having well-staffed cyber military units, but also by infiltrating Russian intelligence networks in 2015. These countries are likely currently projecting cyber power, achieving policy goals by using cyber capabilities, and actively signaling to other states that they intend to further develop their existing capabilities. See https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party.html

2.2 **Limitations**

The NCPI's objective-oriented analysis of national cyber power suffers from some limitations, which are mostly connected with the nature of the subject of "Cyber Power" itself. Here we will briefly address the most important limitations and challenges faced by the research team.

2.2.1 **Lack of Publicly Available Data on Cyber Capabilities**

There were instances where information was available for some, but not all countries. There were, understandably, difficulties in obtaining certain information that is often considered classified, such as the number of cyber military personnel or the number of people within intelligence services with a cyber remit. There were, however, other areas where less sensitive information was also unavailable, such as the number of skilled technology workers.

Similarly, countries may also deliberately shield their intent and capabilities from public knowledge for strategic reasons. We recognize that countries' deliberately choosing to be opaque will be vastly under-ranked in the index. We suspect that Israel falls into this category. This highlights the challenge of measuring cyber power, both to determine capabilities that would map to certain objectives, and to find measurements of these capabilities in open source. We also assert that, while a country may have intentions that are not published externally, both political will and harnessing of national resources are required for a country to pursue a particular objective, both of which can be signaled through publishing of national strategies and doctrines.

We also strongly believe that "Amassing Wealth or Extracting Cryptocurrency" is a top objective of some countries and that they employ cyber means to achieve it.[14] Unfortunately, we were not able to collect sufficient data for both intent and capability indicators that would allow us to measure each country against this objective. We consider this to be

14 "Amassing Wealth or Extracting Cryptocurrency" is when a country has conducted either illegal or legal wealth generation via cyber means. This includes the use of ransomware, attacking the digital infrastructure of banks and financial institutions, and blackmail based on information obtained via data breaches. Legal means include cryptocurrency generation and taxation.

an important objective that is pursued using cyber means and we hope to measure this objective in future iterations of NCPI when more data becomes available.

Other issues contributing to the relative lack of information on some countries as opposed to others is a combination of researchers and observers to date focusing on wealthier Western countries and as a result there is generally more publicly available English-language information. Our assessment of the national cyber strategies also relied on English translations when official English versions were not available. These translations may not be entirely accurate, where some words such as "informatization" are used in Russia and China and not in English-speaking countries. For this reason, Israel, DPRK, and Iran also likely appear lower on the NCPI than potentially expected.

2.2.2 **Lack of Data Surrounding Proxies in Cyberspace**

To ensure comparability of information across countries—both liberal democracies and not—we used proxy information on cyber operations, such as the existence of cyber military strategies and attribution of state-sponsored attacks.

The NCPI also includes by proxy the power held by some non-state actors such as technology companies. Where technology companies contribute to a country's economic strength and contribute to their innovation ecosystem, they have been included in the Digital Evolution index score. However, this does not consider the awesome power that some technology companies have independently of governments by virtue of their global reach, computing power and technological development. Google, Facebook, Baidu, or Huawei on their own may rank as highly as some of the countries at the top of our index. The countries that they reside in will reap benefits in terms of technical capability and access to information.

Another example would be one of the most prolific intelligence gathering tools that was developed in Israel will no doubt be of benefit to the Israeli government. The NCPI also does not include the power of mercenary

groups located within a country's national borders, affiliated with the government or not. Multiple devastating attacks that have originated in China, Russia, and other countries have been attributed to mercenary groups and other non-state actors.

2.2.3 **Simplifications**

Conventional military power, in comparison to cyber capabilities, has more tangible metrics such as the number of schools, soldiers, tanks, and nuclear arsenal a country has. It is more difficult to determine what constitutes a "cyber weapon".

We assume that the NCPI's indicators are an accurate reflection of the potential and real capability a country has to achieve those objectives. In the NCPI, each objective has between five to ten capability indicators. This simplification is required to be able to quantify and compare countries' capabilities against one another. However, we recognize that a) these indicators may not accurately and comprehensively measure the totality of a country's capability, and b) not all data available in the public domain are complete and accurate.

Where possible, we have used data that has been widely used by practitioners and academia often sourced from recognized institutions, such as the United Nations or World Bank, national governments, and other indices that have reliable methodologies for gathering data globally (such as the Freedom House Index[15]).

We have also included some innovative and less well-known data which help us to capture a broader range of cyber capabilities. For instance, to measure a country's strength to control the information environment we have included data on take down requests from Google and statistics from Amazon's Alexa Top 100 websites.[16]

15 See www.freedomhouse.org

16 Google operates a takedown request service where users can report content on a Google product that they believe violates the law or their rights. Google then reviews the product and considers blocking, limiting, or removing access to it. We accessed data on Government requests to remove content via Google's Transparency Report. See, https://transparencyreport.google.com/government-removals/overview?hl=en. See https://alexa.com for data gathered by Amazon on the top 100 websites visited by internet users using various browser extensions.

2.2.4 **Capturing the Duality of Cyber Capabilities**

A challenge of measuring cyber power is to account for its duality. Some capabilities add to cyber power in one national objective but are detrimental for another. For example, while a highly connected population can benefit a country's internet monitoring efforts, the potential impact of attacks becomes more likely and more severe. Therefore, we count the percentage of users connected to the internet within a country positively for internet monitoring and negatively for defense.

Moreover, within the open source data available, certain data can be both a measure of intent and capability. For example, each operation within the Council on Foreign Relations' Cyber Operations Tracker represents both a measure of intent and capability. By having an attributed state-sponsored operation, a state has revealed its intention to achieve an objective in cyberspace, as well as its capability to do so. For example, when the compromise of Sony Pictures Entertainment was attributed to DPRK, the international community was able to determine that DPRK had both the intent and capability to control the information environment, by hindering viewership of the film.

Another example is national cyber legislation. National cyber legislation reveals both the extent of a country's intention to control cyber activities, as well as the capabilities or funding that a government is allocating to do so. To deconflict these two examples, we have created different measurements from the same datasets. For the Cyber Operations Tracker, if a state has conducted at least one operation that achieves a particular objective, we have measured that as an intent indicator.[17] We have then measured the number of attributed operations achieving that objective as a measure of capability. For cyber legislation, we measure intent by analyzing specific laws and strategies, and to measure capability we consider the number of different types of cyber legislation and the timeliness of their updates.

17 A limitation of our research is that we cannot account for non-attributed cyber operations that have occurred.

3. Conceptual Framework

Countries use cyber capabilities to achieve their wider policy goals. In this section, we highlight the national objectives countries have historically pursued using cyber means. We then explain how a country's intent to pursue those objectives, and the capabilities required to achieve those objectives, create our formula for cyber power.

3.1 National Objectives

While it seems accurate to assume that the most technically capable or best equipped country is the most powerful, we argue that cyber power is made of different components. We pursue a holistic approach and consider all components to assess the overall cyber power. Cyber power should be measured in relation to each country's national objectives.

The most comprehensive cyber power is the country that most ably uses cyber means to achieve the most objectives. We recognize that countries have non-cyber means to achieve the same objective(s) and a country may elect to do that instead. However, within the NCPI we do not consider these other tools at a country's disposal. For example, a country that seeks to use surveillance to monitor domestic groups may use cyber means to complement the traditional tools it has available, such as gathering human intelligence and conducting physical surveillance. The focus of our research is on how a country develops and uses its cyber capability to meet national objectives.

To understand how capable a country is, we started by identifying the range of national objectives that countries may try to achieve via cyber means. International relations theory forms the basis of our understanding of how countries theorize national objectives. The Council on Foreign Relations' Cyber Operations database[18] of publicly attributed

18 Most of the objectives were identified through analyzing the Council on Foreign Relation's "Cyber Operations Tracker". See, https://www.cfr.org/interactive/cyber-operations. We also mapped each cyber-attack within the database (as of December 2019) to the objectives below, to use real historical cyber-attacks as a measure of cyber power capability.

state-sponsored incidents provided us with an insight of how some countries have deployed their cyber capabilities. Based on this research, we identified seven cyber objectives that countries have broadly pursued between 2005-2019 that we have explained in Table 3.

Table 3: Definitions of National Objectives[19]

Cyber Power Objectives

Common objectives states will attempt to acheive through cyberspace, as determined by the Belfer Center Cyber Power Team.

1	**Surveilling and Monitoring Domestic Groups**	A country 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.
2	**Strengthening and Enhancing National Cyber Defenses**	A country has prioritized enhancement of the defense of government and national assets and systems, and improved national cyber hygiene and resilience. This includes active defence of government assets, promoting cybersecurity and cyber hygiene to key industries and the general population, and raising national awareness of cyber threats.
3	**Controlling and Manipulating the Information Environment**	Reflecting the duality of information controls, a country has prioritized using electronic means to control information and change narratives at home and abroad, AND/OR attempted to protect the internet privacy and free speech of its citizens. 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.
4	**Intelligence Gathering and Collection in other Countries for National Security**	A country 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 countries seek to improve their situational awareness and understanding of a foreign country. 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, such as Members of Parliament.
5	**Growing National Cyber and Technology Competence**	A country 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 by conducting industrial espionage against foreign companies and countries to facilitate technology transfer. Legal means include investment in cybersecurity research and development and prioritizing cybersecurity workforce development.
6	**Destroying or Disabling an Adversary's Infrastructure and Capabilities**	A country 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 cyber attacks on critical infrastructure, and DDOS attacks on government communications networks. It also includes cyber attacks to demonstrate intent and capability to deter an adversary from acting.
7	**Defining International Cyber Norms and Technical Standards**	A country 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 cyber crime and share technical expertise and capabilities.

19 Table created by authors.

An Eighth Objective: Amassing Wealth and Extracting Cryptocurrency

The 2020 NCPI assesses countries against seven objectives, however there is one objective clearly missing. The missing objective, "Amassing Wealth and Extracting Cryptocurrency", is defined as follows:

> A country has conducted either illegal or legal wealth generation via cyber means. Illegal and legal wealth generation via cyber means. This could include the use of ransomware, attacking the cyber infrastructure of banks and financial institutions, and blackmail based on information obtained via hacks and data breaches. It could also include legal means, such as incentivizing and encouraging domestic actors to develop exportable cybersecurity products, and the development of cryptocurrencies.

We attempted to collect our own data to demonstrate "Amassing Wealth and Extracting Cryptocurrency" through exploring the availability of data on Bitcoin cash withdrawals, mining statistics, and successful scams attributed to criminal actors within a specific country. We recognize that much of this activity is not state-sponsored behavior.[20]

Unfortunately, for this years' index we were unable to find the above data, nor were we able to find measurements of capabilities that could serve as proxies for the capabilities we wanted to measure. As a result, we excluded this objective from this years' study because the data that was available would overly skew the results. We hope that relevant data to measure capability around "Amassing Wealth and Extracting Cryptocurrency becomes available in coming years so that we can include it in future iterations of the NCPI.

20 See https://qz.com/1194051/a-new-world-bank-project-shows-that-wealth-not-gdp-is-the-best-gauge-of-a-countrys-progress/

What Objective(s) are Countries' Prioritizing, and Can They Be Achieved?

To measure a country's cyber power, we must answer the following questions:

1. Which objective(s) does a country intend to pursue in cyberspace?
2. What capabilities does a country have that could achieve those objective(s)?

The first question is a measure of intent, while the second is a measure of capability. Both terms are used in the classic definition of national power and the discussion of adversarial threats.[21]

Intent is a measurement of the quality and quantity of *government planning initiatives (*i.e. national cyber security strategies, crisis plans, and other related government planning documents). It is a subjective assessment of the government's "observed behavior" on cyber relevant issues.[22]

Capabilities are measurements of the quality and quantity of *country output* related to one or more cyber objectives (i.e. number of patents filed per year, number of global top security firms, number of skilled workers).

The distinction between intent and capability is important for two reasons:

1. A government may have the capabilities to achieve an objective using cyber means but not have the intent to do so.
2. A government may wish to pursue an objective through cyber means but lacks the required capability or resources to actually do so.

21 See https://www.heritage.org/military-strength/introduction and https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

22 https://www.mitre.org/sites/default/files/pdf/10_2914.pdf

National Cyber Power Index Formula

For our NCPI Formula we draw on intelligence and national power literature. [23] There, intent and capability parameters are multiplied against each other to obtain threat and power estimates.[24]

There is a dynamic relationship between capability and intent. If capability is taken as the base line ability to exercise cyber power, then a country's intent is its vector, i.e. it establishes both the magnitude and direction of travel of its cyber power. A strong intent magnifies the effect of cyber capability, whereas lower intent score would hinder an otherwise strong capability.

We score each country based on their intent to pursue each of the seven objectives and capability to achieve said objective. We compute the NCPI intent scores by multiplying—for each national objective—a country's capabilities with its intent. The NCPI intent score reflects the different prioritization that some countries place on leveraging specific cyber capabilities, and therefore can be considered as a weight. This assumes that a country can only fully deploy its cyber capabilities in a domain, such as national surveillance, if it shows a 100 percent intent to do so.

Therefore, in the NCPI, a country scores highly in an objective only if it has both strong intent and the necessary capabilities to achieve the objective, as capabilities or intent alone are not sufficient. In formula form, national cyber power of a country is the product of capability and intent:

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

where $\boldsymbol{x}$ represents one of the seven objectives:

23 Singer, J. D. (1958). Threat-perception and the armament-tension dilemma. *Journal of Conflict Resolution*, *2*(1), 90-105.

24 Cline, R. S. (1993). *The power of nations in the 1990s: a strategic assessment*. University Press of America.

1. Surveilling and Monitoring Domestic Groups
2. Strengthening and Enhancing National Cyber Defenses
3. Controlling and Manipulating the Information Environment
4. Intelligence Gathering and Collection in other Countries for National Security Objectives
5. Growing National Cyber and Technology Competence
6. Destroying or Disabling an Adversary's Infrastructure and Capabilities
7. Defining International Cyber Norms and Technical Standards

4. Methodology and Discussion

4.1 Scoring Intent and Sources

To identify which objective(s) each country is pursuing we created a set of unique 32 intent indicators, alongside additional assessments captured as 'intent factors', and attributed attack data, that together formulate an intent score. Half of the intent score was formulated using indicators derived from each country's public cyber-related documents, public announcements and national cyber strategies, including evidence of funding. Given the importance that we placed on demonstrated intent, the other 50% of the intent score was allocated to evidence of attributed attacks.

From this evidence of attributed attacks, together with the other indicators that demonstrate preplanning and predisposition, it is possible to infer an overall general intent; that "which is presumed from the act of commission" from the actions of a country.[25] Therefore, the intentions of a country can also be inferred from the cyber-attacks and activities it conducts.

We include demonstrated intent because a country may not publicly state their intention to achieve a specific objective for strategic reasons. However, there may be evidence that said country has pursued these objectives through attributed cyber operations. For example, the Chinese government has denied its use of cyber espionage to steal US intellectual property for multiple years, describing the accusations as "slanderous".[26] However, analysis conducted by multiple private sector organizations have attributed cyber operations targeting US organizations back to Chinese state-actors.[27]

We examined the entries in CFR's Cyber Operations Tracker between 2015 to December 2019 to determine where a country has had a cyber operation attributed to it that helped the country achieve one of the seven objectives. If a country had one or more cyber operations attributed to it, we would give the country full marks on demonstrated intent for that objective. Due

25 Riverside City Sheriff's Department (1975). *Element of Intent in Criminal Law.* Mount San Jacinto College.

26 Philip Wen. (2018) "China Denies Slanderous Economic Espionage Charges from US allies". Reuters.

27 Many of these attacks are captured in the Council on Foreign Relations' Cyber Operations Tracker

to the covert nature of cyber operations, we assume that if a country had one attributed cyber operation, the country likely had conducted other cyber operations that achieved similar goals and would likely continue to pursue these methods.

As for stated intent, we conducted a two-pronged approach: an assessment of a country's stated intent by objective in the public domain, as well as an in-depth analysis of overall intent.

A number of international institutions, including the UN and EU recommend that countries produce a national cyber strategy, with ITU noting that "By developing and implementing a National Cybersecurity Strategy, a nation can improve the security of its digital infrastructure and ultimately contribute to its broader socio-economic aspirations. National leaders need to be strategic about the opportunities offered and the risks posed to their countries by the digital environment; they also need to establish a clear vision of the digital future they wish to create."[28] On this basis, we looked at several factors relating to each country's cyber strategy, including:

1. How comprehensive is the country's cyber strategy—does it include specific actions, owners, and objectives?
2. How long has the country had a cyber strategy for?
3. How regularly has the country updated its cyber strategy?
4. How recently has the country updated its strategy?
5. Has the country announced increased cyber funding since it last published its strategy?

We conducted textual analysis of each country's cyber strategy, as well as other similar documents, to determine what objectives were laid out in each document. To verify the findings, we applied natural language processing (NLP) to pull out the top words and trigrams (sets of three consecutive words) within each strategy. If a word or trigram referring to an objective was surfaced using NLP and not surfaced through the manual

28 International Telecommunications Union. (2018). "Guide to Developing a National Cybersecurity Strategy—Strategic Engagement in Cybersecurity"

scan, we double checked our assessment. For example, the words "norms, international, Interpol" would likely refer to international norms, while the trigram "actively, punish, adversary" would likely refer to the destruction of adversary infrastructure. Countries without a publicly available strategy, such as Iran, were assessed using expert analysis and third-party documents to identify and score their intent to achieve objectives.

A country that has a long-standing, publicly available cyber strategy, which is publicly funded, would have a more-established governance framework facilitating delivery of the strategy[29]. A long standing publicly available cyber strategy increased the score a country achieved for its intent. Given the dynamic nature of cyberspace and the rapidly changing threats and opportunities, a country that did not regularly review its strategy is less likely to be a leader in cyber thinking.

A study of iterations of national cyber strategies demonstrated how the application of cyber means has evolved over time. Looking at whether a cyber operation that achieved one of the seven objectives had been attributed to the country's government proved a country's resolve to achieve the objective through cyber means. Countries that have consistently pursued cyber objectives for a longer period received a higher score.

We extensively researched each country's websites, online publications, and comments made by senior government figures to the media. With the exception of the DPRK, we only assessed attributed or official government resources. We did not use third-party sources, or leaked or hacked information, as we wanted to establish the specific message each country was communicating on its objectives and intentions. Finally, we analyzed membership of and participation in international institutions and organizations.

Table 4 shows how these strategy-based indicator scores fit into the overall intent score. Table 5 shows the full set of questions that the indicators and intent factors sought to address. The scoring method of these intent indicators is displayed by objective in Annex C.

29 We recognize that some anomalies are able to execute government policy and be effective without a public strategy and dedicated resource.

Table 4: Key for Scoring Intent Factors in Cyber Strategies

Indicator	Scoring Method	
The total period over which the country has had a Cyber Strategy	Number of years from first strategy to 2020	
Frequency of Strategies	Period from first to last strategy divided by the total number of strategies published	
Years since strategy last updated	Number of years from last strategy to 2020	
Strategy review score	Score based on how many of the following elements the strategy contains:	
	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 critera
	5	Detailed timeline AND success critera

Table 5: Questions asked in Overall Intent Scoring (by Objective)

#	Surveillance	Defense	Control	Intelligence	Financial	Commercial	Offense	Norms
1	Does the country have at least one policy or law enforcement agency with specialist cyber-crime expertise or that encourages citizens to report cyber-crime?	Has the country published a cyber security plan that defines how it will protect government systems and/or critical national infrastructure?	Data law protection strength	Does the country's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the country has cyber intelligence-gathering capability?	Is the country a member of the Common Criteria Recognition Arrangement (CCRA)?	What is the quality of participation across all 22 ISO/IEC Joint Technical Committees?	Does the country's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the country has a destructive cyber capability?	How many of the past five UN Cyber Government Group of Experts (GGE) consultations has the country participated in?
2	Does the country's domestic intelligence agency acknowledge surveillance cyber capabilities?	Does the country undertake cyber awareness and cyber hygiene campaigns?	Does the country's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the country has cyber capabilities to control and manipulate the information environment ?	Does the country's military cyber unit or command acknowledge that the country has a cyber intelligence gathering capability?	Is the country a member of the IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)?	Does the country have a public-private partnership initiative to grow its domestic cyber industry, workforce, and raise awareness of cyber issues?	Does the country's military cyber unit or command acknowledge that the country has a destructive cyber capability?	How many times has the country sponsored UN GGE related resolutions between 2012-2016? Out of a total of five.
3	Is cyber crime, cyber terrorism, or domestic surveillance via cyber means referred to within the country's domestic counter-terrorism or homeland security strategy, plan, or law?	Has the country stated it plans to undertake national active cyber defense-style effects?	Does the country's military cyber unit or command acknowledge that the country has cyber capabilities to control and manipulate the information environment?	Does the country's signals intelligence agency or foreign intelligence service acknowledge that the country has a cyber intelligence gathering capability?	Has the country published a plan or strategy to attract investment towards cyber firms or growing its cyber exports?	Is there evidence the country has invested in or funded cyber research?	Does the country's signals intelligence agency or foreign intelligence service acknowledge that the country has a destructive cyber capability?	How many times has the country participated in the Internet Governance Forum (IGF) between 2015-2019?
4	Consistency of objective: is it pursued in >1 strategy?	Consistency of objective: is it pursued in >1 strategy?	Does the country's signals intelligence agency or foreign intelligence service acknowledge that the country has cyber capabilities to control and manipulate the information environment?	Consistency of objective: is it pursued in >1 strategy?	Consistency of objective: is it pursued in >1 strategy?	Consistency of objective: is it pursued in >1 strategy?	Consistency of objective: is it pursued in >1 strategy?	Has the country participated in the Global Forum for Cyber Expertise capacity building activities?
5	If surveillance activity is acknowledged in the country's national cyber strategy: include strategy score	If strengthening and enhancing national cyber defenses activity is acknowledged in the country's national cyber strategy: include strategy score.	Consistency of objective: is it pursued in >1 strategy?	If intelligence activity is acknowledged in the country's national cyber strategy: include strategy score	If amassing wealth and/or extracting cryptocurrency activity is acknowledged in the country's national cyber strategy: include strategy score	If growing national cyber and technology competence activity is acknowledged in the country's national cyber strategy: include strategy score	If destructive activity is acknowledged in the country's national cyber strategy: include strategy score	What is the quality of participation across all 22 ISO/IEC Joint Technical Committees?
6	If surveillance activity is acknowledged in the country's national cyber strategy: include financial score	If strengthening and enhancing national cyber defenses activity is acknowledged in the country's national cyber strategy: include financial score	If controlling and manipulating the information environment activity is acknowledged in the country's national cyber strategy: include strategy score	If intelligence activity is acknowledged in the country's national cyber strategy: include financial score	If amassing wealth and/or extracting cryptocurrency activity is acknowledged in the country's national cyber strategy: include financial score	If growing national cyber and technology competence activity is acknowledged in the country's national cyber strategy: include financial score	If destructive activity is acknowledged in the country's national cyber strategy: include financial score	What is the quality of participation across the International Telecommunication Union's Standardization Study Groups 13 (Future Networks), 17 (Security), and 20 (IoT and Smart Cities)?
7	Has the country been attributed to a cyber attack that assists this objective? (50% of the score)		If controlling and manipulating the information environment activity is acknowledged in the country's national cyber strategy: include financial score	Has the country been attributed to a cyber attack that assists this objective? (50% of the score)	Has the country been attributed to a cyber attack that assists this objective? (50% of the score)	Has the country been attributed to a cyber attack that assists this objective? (50% of the score)	Has the country been attributed to a cyber attack that assists this objective? (50% of the score)	Has the country participated in bilateral or multilateral cyber defense exercises?
8			Has the country been attributed to a cyber attack that assists this objective? (50% of the score)					Consistency of objective: is it pursued in >1 strategy?
9								If defining international cyber norms and technical standards activity is acknowledged in the country's national cyber strategy: include strategy score.
10								If defining international cyber norms and technical standards activity is acknowledged in the country's national cyber strategy: include financial score.

Cyber Intent Index (CII)

The Cyber Intent Index is based on the ratings of 32 indicators which are grouped under the seven national objectives: (1) surveillance, (2) defense, (3) control, (4) intelligence, (5) commerce, (6) offence, and (7) norms. These, combined with the score for intent factors within Cyber Strategies, plus the score for attributed attacks make up the overall intent score.

A country's overall rating is the average of the seven national objectives. We used a combination of dichotomous (1 for a yes and 0 for a no answer); three-point scoring system (the possibility of a 0.5 score is introduced, to capture "grey areas"); and a percentage (shown in decimal form, between 0.00 and 1.00).[30]

A country's overall rating is the average of the seven national objectives converted to a scale of 0 to 100 percent.

Results

After scoring the 30 countries across the 7 objectives, the top ten highest scoring countries for intent were:

1. China
2. United States
3. United Kingdom
4. Russia
5. Netherlands
6. Israel
7. Spain
8. Australia
9. Canada
10. Iran

30 A similar approach was taken by the Economist Intelligence Unit Democracy Index and by Freedom House's Freedom in the World Index.

Table 6 shows the top ten ranking for intent by each objective.

Table 6: Top 10 Intent Ranking by Objective

#	Surveillance	Defense	Control	Intelligence	Commercial	Offense	Norms
1	Russia	UK	US	UK	China	UK	UK
2	China	Netherlands	China	US	Iran	US	Germany
3	Vietnam	France	Russia	Spain	UK	Israel	US
4	Saudi Arabia	US	Vietnam	Netherlands	Japan	Spain	Japan
5	UK	China	Israel	Israel	Switzerland	Russia	France
6	Estonia	Japan	Iran	Russia	Netherlands	Iran	Switzerland
7	Netherlands	Canada	UK	New Zealand	Sweden	China	Netherlands
8	Australia	Sweden	Germany	Canada	Australia	Netherlands	China
9	US	Estonia	New Zealand	Australia	US	Estonia	Canada
10	Switzerland	Australia	France	China	Russia	Australia	Australia

Analysis

Each of the countries in the CII top 10 have a comprehensive range of evidence across all objectives. Unsurprisingly, these countries scored highly in "strengthening and enhancing national cyber defenses". Given the long-term focus of these countries in securing themselves against cyber-attacks, most of these countries have not only tried to increase the resilience of their domestic populations, but also pursued active cyber defense measures, such as US CYBERCOM's persistent engagement strategy.

The weighting given to demonstrated intent within the score using attributed attack data propelled several countries' up the rankings. This in part explains why China achieved the highest score for intent, scoring above other countries who were more explicit in strategic documentation as to their intent, or were equally active in international fora.

The scores for destructive cyber intent were the most polarizing. Just under half the countries in our index are either not actively pursuing this objective, have not publicly confirmed they are pursuing it, or have not been observed pursuing it. We assess that this is for two main reasons: firstly, the high level of technical competence needed to achieve these objectives, and secondly, the international debate around how destructive cyber capabilities comply with international law on armed conflict. The nations that scored the highest in the destructive category were the UK and the US, followed by Russia with the score gained by other nations quickly tapering off. Few nations have been observed conducting a destructive act using cyber capability. China, DPRK, the Netherlands, Iran, Israel, Russia, Spain, UK, and the US were the only nations which received a score under this objective. Many nations did not score highly or at all in this category mainly because they are officially silent on whether they might undertake destructive cyber operations. On this point, China's intent score for offense is particularly interesting as their official position is that they are against all forms of cyber-attacks and advocate for the peaceful use of cyberspace.

15 countries demonstrated their intelligence intent by conducting cyber-attacks that focused on the collection of information to improve their situational awareness and understanding of a foreign country. Interestingly, 21 countries acknowledged that they conduct intelligence activities using cyber means, either through their military or through their signals or foreign intelligence agency. Conversely, only three countries have been observed conducting cyber-attacks for the purposes of industry espionage, but 29 of the countries have also sought to grow their domestic cyber and tech competence via legal means.

While 29 countries were observed pursuing legal wealth generation via cyber means, only one country was observed pursuing it via illegal means—DPRK. Only one country was assessed to have not demonstrated its wealth generation intent at all—Egypt.

There are several limitations of this analysis that it is important to note. Firstly, this project conducted searches in both English and the native language of each country, using commercially available language translation software, and, where provided, English translations of non-English

documents. While our approach endeavored to be exhaustive, it is possible that documents were missed, or the sentiment expressed was lost in translation. However, we also approached this analysis from the perspective that; for a country to demonstrate specific intent it should be positively and actively communicating its intentions to its domestic population and foreign observers. Therefore, documents that were difficult to locate on obscure websites or behind firewalls do not communicate intent and we feel that the language limitations did not fundamentally undermine our search process.

Secondly, some countries are clearly less willing to be transparent and publicly share information, particularly around military and intelligence matters. DPRK was the most secretive, For DPRK, we relied on credible, non-state issued sources to allow us to offer scores for it across all objectives. The only official DPRK sources we used were from its universities. It was also very difficult to find information on the role and priorities of the Egyptian military and intelligence community, as well as their counterparts in a range of other countries.

Unsurprisingly, countries that had declared AND demonstrated their intent scored highest in each objective. Largely due to its transparency on cyber matters, as well as having conducted cyber intelligence and offensive operations, the UK takes the top spot in four categories for intent.

Surveillance: Russia, China, Vietnam, and Saudi Arabia occupied the top spots for the domestic surveillance objective. In addition to all four countries having been observed shutting down "illegal content"[31] within their domestic populace, all had law enforcement bodies and domestic intelligence agencies with specific cyber capabilities, and all bar Saudi Arabia referenced cyber threats within their homeland security or domestic terrorism strategies or plans.

Control: This objective reflects the duality of cyber means. To score highly in this objective a state has demonstrated control through either removing extremist material and refuting foreign propaganda or through domestic propaganda and creating and amplifying disinformation overseas. The

31 Russell, Jon. "Vietnam Threatens to Penalize Facebook for Breaking Its Draconian Cybersecurity Law." *TechCrunch*, TechCrunch, 9 Jan. 2019, techcrunch.com/2019/01/09/vietnam-threatens-to-penalize-facebook/.

United States topped this objective because of the former. The US scores highly because of US military and intelligence agencies' role in disrupting the Islamic State's ability to recruit and communicate with its fighters and efforts to limit Tehran's ability to spread propaganda post-9/11. In contrast, China and Russia's high rank is due in large part to the disinformation campaigns that have been attributed to both countries since 2016.

Destructive: The cyber and military strategies of the UK, Israel, and the US acknowledge that these countries have developed destructive cyber capabilities. In addition, all three countries have demonstrated these capabilities in offensive operations.

Intelligence: Given the information revealed in the Snowden leaks, it is unsurprising that the UK and US top the intelligence objective. Spain taking third place is possibly more interesting. Like the UK and the US, Spain's military and intelligence agencies have declared and demonstrated their intent to use cyber means to gather intelligence.

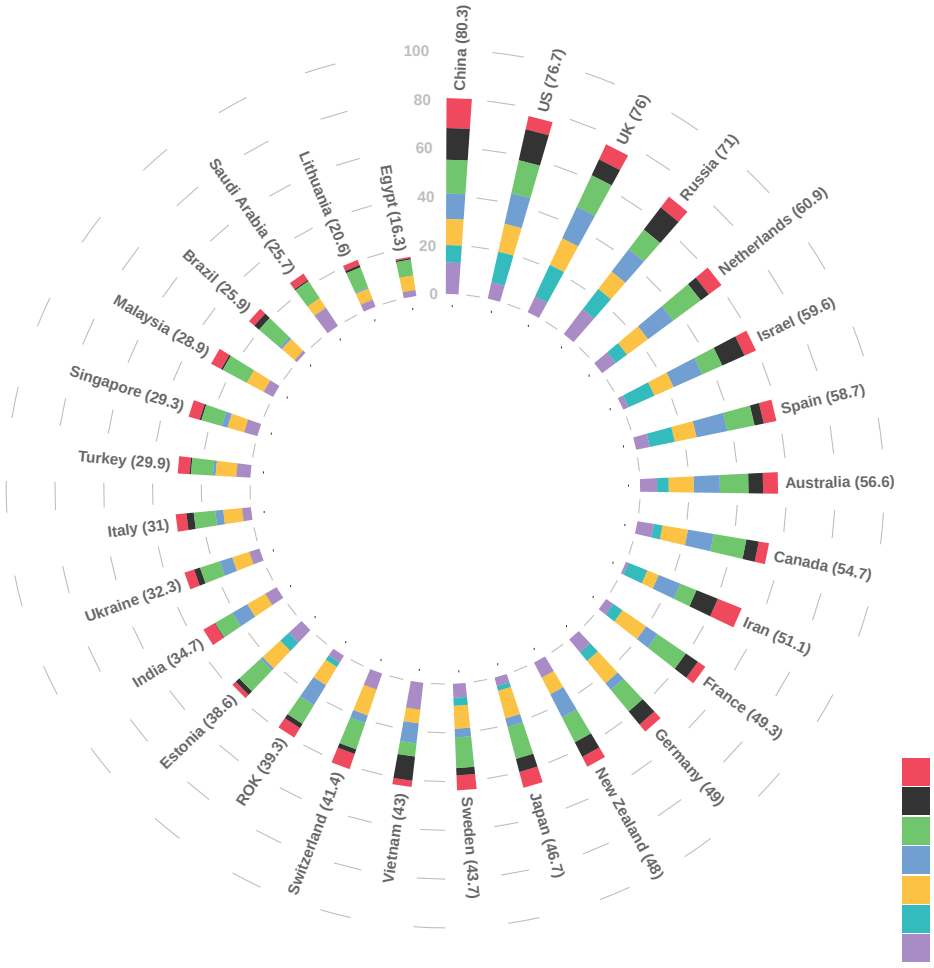
Commercial: In-line with recent headlines in Western countries, China tops the Growing National Cyber and Technology Competence objective. Along with DPRK and Iran, China is one of only three countries assessed to be pursuing this objective through both legal and illegal means. It has been both observed conducting industrial espionage and sought to incentivize and grow its domestic cyber expertise through research and development, and public-private partnerships.

Norms: Of the 29 countries we found cyber strategies for, 27 of the countries noted their pursuit of Defining International Cyber Norms and Technical Standards in their strategy. Only Egypt and India did not. Germany came second in this indicator, which is consistent with Germany's wider support for international institutions and international capacity building initiatives.

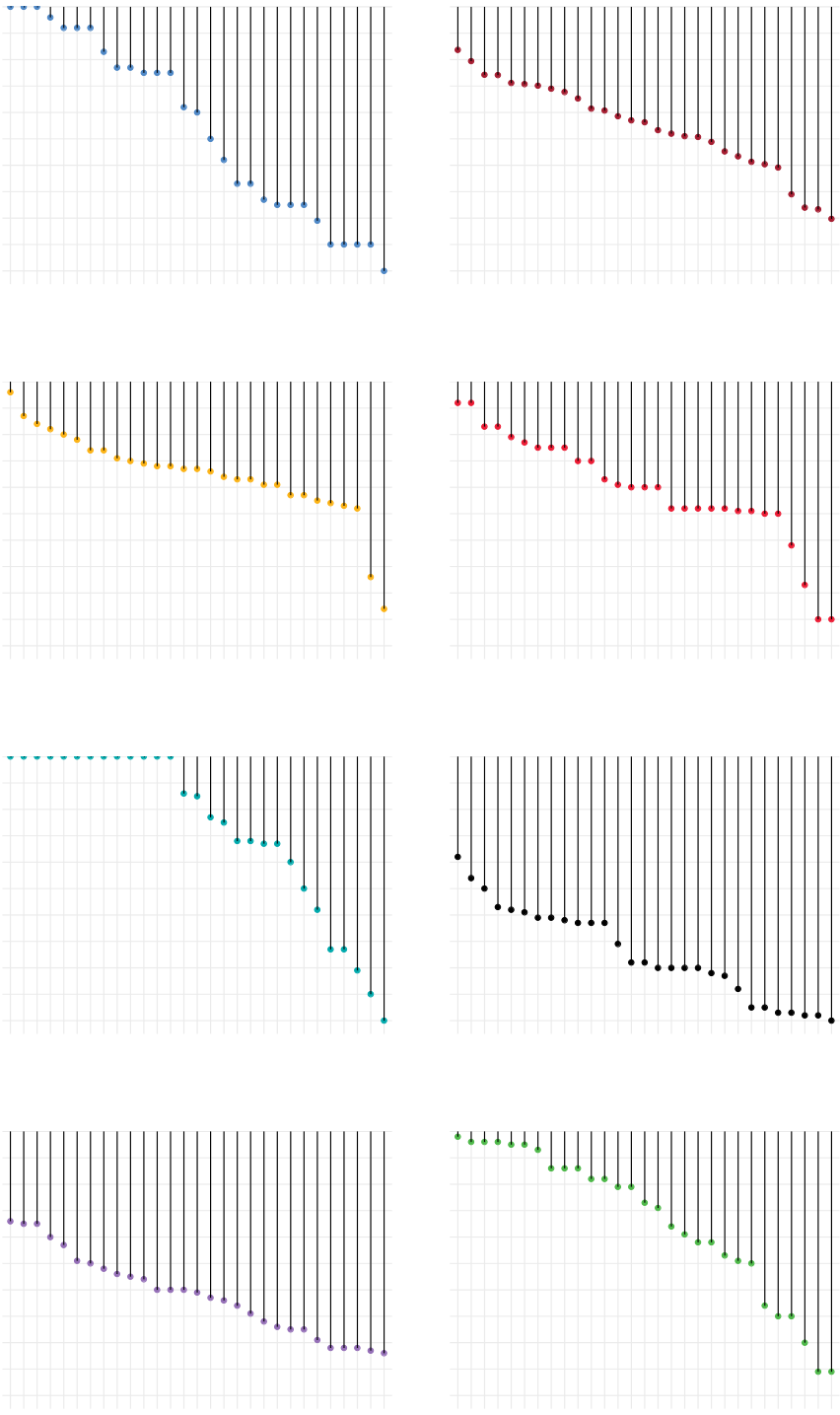
Defense: All the top five countries for the cyber defense objective have pursued both increased cyber resilience and active cyber defense measures.

Graph 4 displays CII by Country across all seven objectives. Graph 5 displays the CII broken down by objectives.

Graph 4: CII 2020 by Country



Graph 5: CII 2020 by Objective and Country



4.2 **Scoring Capabilities and Sources**

To become a cyber power, a country requires capabilities to achieve their intended objectives. Cyber capabilities relate to the creation, control and communication of electronic and computer-based information infrastructure, networks, software, and human skills.[32] Therefore, countries invest in a wide range of resources including areas such as military cyber capabilities, cyber defense, and surveillance, but also in human capacity, institutional strengthening, and domestic policy. In addition, being able to influence the global context of cyberspace, be that through technical standards, international norms, or exports, allows countries to cultivate an environment in which they can protect their interests and exercise their power to extend their zones of influence. Thus, countries will attempt to control cyberspace not just within their own borders, but internationally as well. We have considered all the above elements when assessing countries' cyber capabilities by objective.

The complex source of cyber power is reflected in our mapping of each national objective to indicators that reflect a country's capability to achieve said objective. Many indicators contribute to more than one objective and as a result some indicators have counted in multiple objectives to reflect that overlap. Table 7 explains the mapping of indicators to national objectives and a high-level overview of our approach to scoring. Annex B provides a more in-depth description surrounding each capability indicator's scoring.

The 27 capability indicators included in the NCPI reflect a more comprehensive list of capabilities than what was previously available moving us toward a more realistic and comparable understanding of cyber power at the national level. The data collected on capabilities can be categorized into eight themes: Evidence of Attacks; National Online Content; Domestic State Cyber structures; Cyber Vulnerability Mitigation; Private Sector, Trade, and Innovation; Connectivity; Workforce; and Legal and Policy Frameworks.[33]

32 Daniel T. Kuehl. 2009. 'From Cyberspace to Cyberpower: Defining the Problem', In Franklin Kramer, Stuart Starr and Larry K. Wentz (eds.) *Cyberpower and National Security*. Washington DC: National Defense University Press. p24

33 These themes are purely for conceptual ease and do not affect our NCPI calculations.

Table 7: Capability Indicators Mapped to Objectives

Cyber Military Doctrine

Cyber Capability Index (CCI)

The CCI is on a scale from 0 to 100 percent of the capabilities measured, and it is based on the ratings of 27 indicators which are grouped by the seven national objectives.

The CCI can be broken down by objective and that score is based on the average value of the normalized indicators that inform said objective. The overall rating of the CCI is the average across all 7 objectives.

Before aggregating the indicators, we rescaled them using the Min-Max normalization technique, which rescales data on different intervals based on minimum and maximum values. Some of our indicators do not follow a Gaussian distribution, which prevents us from using other normalization techniques (such as the z-standardization). The min-max technique is widely applied for constructing composite indicators.[34] It has the advantage of setting the boundaries of all indicators between an identical range (a min of 0 and a max of 1). For every capability indicator, the minimum value gets transformed into a 0, the maximum value gets transformed into a 1, and every other value gets transformed into a decimal between 0 and 1.

One disadvantage is that the technique is based on the extreme values of a distribution which strongly influence the final output. We have performed a series of sensitivity checks using other normalization techniques to test for a potential bias resulting from extreme values (see Section 4's subsection on sensitivity analysis).

Results

The top ten countries per objective are listed in Table 8 below. Capabilities by country and more specific rankings can be found in the Annex.

34 Patro, S., and Kishore Kumar Sahu. "Normalization: A preprocessing stage." *arXiv preprint arXiv:1503.06462* (2015).

Table 8: CCI 2020 by Objective

#	Surveillance	Defense	Information Control	Intelligence	Commercial	Offense	Norms
1	US	China	US	US	US	Russia	US
2	UK	Singapore	Russia	UK	South Korea	US	France
3	France	Canada	China	China	China	China	Japan
4	China	France	South Korea	Germany	Japan	Germany	China
5	Japan	Switzerland	Sweden	Singapore	UK	UK	Germany
6	Sweden	Netherlands	Singapore	Israel	Singapore	France	Singapore
7	Canada	US	UK	France	Netherlands	Netherlands	UK
8	Germany	Japan	New Zealand	Malaysia	Germany	Spain	Malaysia
9	New Zealand	Germany	Saudi Arabia	Estonia	France	Estonia	South Korea
10	Israel	Sweden	Canada	Netherlands	Switzerland	Canada	India

Analysis

The US scores highest on five out of seven objectives. Russia, which ranks tenth overall in the CCI, tops the list for the offense[35] objective. China leads the ranking on cyber defense capabilities, Within its portfolio of cyber capabilities, national cyber defense is the objective the US' scored the lowest where it ranked 7th out of 30 countries.

China is in the top 5 for every single objective. In recent years, China has invested heavily in research and development of technologies that allow the country to achieve multiple objectives in cyberspace. These results reflect China's increasingly dominant position in cyberspace but also highlight the significant gap in capability between China and the US in most areas.[36]

The UK scores particularly high in two domains and comes third in the overall ranking: intelligence and surveillance (in both cases the country is

35 Offense is short form for the destruction and disablement of adversary infrastructure objective.

36 Inkster, N., 2018. *China's Cyber Power*. Routledge.
Cheung, T.M., 2018. The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, *3*(3), pp.306-326.

topped only by the US). This is of no surprise: the country has traditionally held strong positions in both the foreign intelligence collection for national security purposes and the surveillance and monitoring of domestic groups.[37] It has also devoted a substantial amount of public money to strengthen its capabilities to achieve several of the assessed objectives.

Norms capabilities relied on a mix of international treaties and standards bodies, as well as the norms defined by the technology a country exports. Because of that, Japan and the US find themselves near the top of the list.

Russia is positioned at the forefront of the offense objective. The country has an established cyber command and detailed cyber military doctrine, as well as making headlines in this space over several years.[38] Most notably, the country has carried out a large amount of disruptive cyber-attacks over the past years.[39] This is a clear demonstration of its capability to destroy and disrupt adversary infrastructure.

Singapore has focused heavily on national defense.[40] The country has not taken any (known) disruptive actions in cyberspace, focusing its resources on strengthening and enhancing its defense capabilities instead. Next to Singapore, China, Canada, France, and Switzerland are all invested toward promoting an environment that serves the same goal.

One area where the ranking is at odds with conventional thought is around Israel. Israel is often put at the top of pseudo-rankings by commentators, particularly highlighting its capabilities around offensive cyber and intelligence gathering. We agree that this is an anomaly in this ranking, and this could be down to several factors. Importantly, this index uses only open source data. Much of Israel's cyber program is coordinated and directed covertly, and not in the public or business sectors. Secondly, this section

37 Kris, D.S., 2015. Trends and predictions in foreign intelligence surveillance: The FAA and beyond. *J. Nat'l Sec. L. & Poly*, *8*, p.377.
Leigh, I., 2010. Intelligence and the Law in the United Kingdom. In *The Oxford Handbook of National Security Intelligence*.

38 Giles, K., 2012, June. Russia's public stance on cyberspace issues. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (pp. 1-13). IEEE.

39 Attacks are included in CFR's Cyber Operations Tracker.

40 Ventre, D. ed., 2013. *Cyber Conflict: competing national perspectives*. John Wiley & Sons.
Ad'ha Aljunied, S.M., 2019. The securitization of cyberspace governance in Singapore. *Asian Security*, pp.1-20.

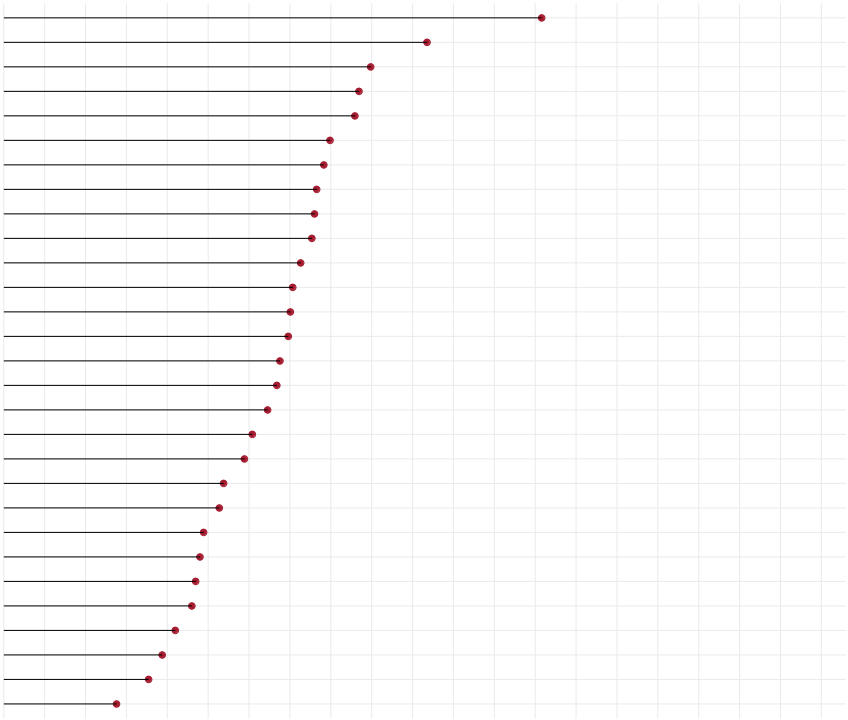
of the NCPI measures capability. When looking at intent, Israel scored highly for those two objectives. However, it does not necessarily have the cyber-military industrial capacity, the economic power, or other key measures that have been considered to measure capability here.

The index also highlights several countries not normally associated with being cyber powers, as having strong capabilities in certain areas. Malaysia is in the top 10 four times for information control, intelligence, commercial gain and norms and laws. Sweden is in the top 10 for three objectives: surveillance, cyber defense, and information control. Switzerland made the top 10 for cyber defense and commercial gain.

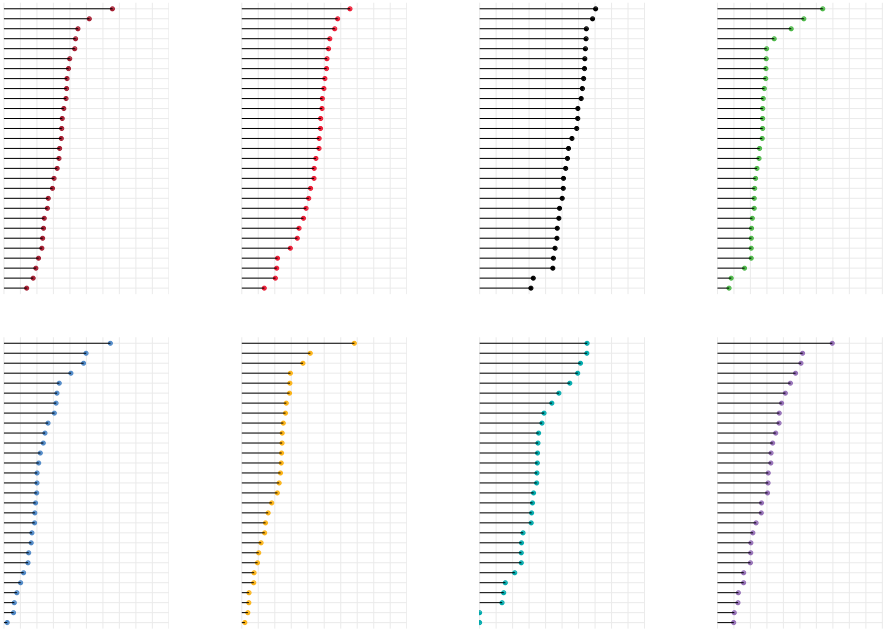
Estonia, often heralded as a beacon of cyber and digital capability, made the top 10 for only two objectives: intelligence and offense. Whilst this is impressive for a country of under 1.5 million, it is perhaps not as impressive as the team were expecting.

Germany, a country not often talked about when discussing cyber capability, was ranked in the top 5 for intelligence, offense, and norms, being able to draw on its strong industrial base and its well-organized military and civilian capabilities.

Graph 6: CCI 2020 Across All Objectives



Graph 7: CCI by Individual Objective



4.3 Construction of the Aggregated NCPI

Missing Data and Normalization of Indicators

Although we have carefully selected the indicators that inform our NCPI we were not able to find data for all 30 countries included and each of our indicators. All indicators included in the NCPI index reflect the availability of data for at least 21 (70%) of the 30 countries and where we had reasonable proxies for the missing data points. Indicators that did not meet this threshold were not included. We sourced multiple indicators in house and followed a rigorous coding scheme and procedure, all of which are available upon request.

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

- Computer Infection rate—estimated values for Israel and New Zealand
- Mobile Infection rate—estimated values for Israel and New Zealand
- Patent Applications—estimated values for Lithuania
- Information and Communication Imports—estimated values for Egypt, Saudi Arabia, Singapore, Switzerland, and Vietnam
- E-commerce—estimated values for Israel
- Freedom on the Net—estimated values for DPRK, Israel, Lithuania, Netherlands, New Zealand, Spain, Sweden, and Switzerland

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 get 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. Surveillance technology, for instance, maps to both the national objective of domestic surveillance and the national objective of intelligence gathering and is therefore counted twice in the NCPI. This 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 CCI and NCPI for a country that scores highly on that capability indicator.

We compute the NCPI intent scores by multiplying—for each objective—a country's capabilities with its intent to achieve said objective. For each country, through the intent measure we are effectively putting a weight on its capabilities. The intent part of our NCPI Index can be considered as equivalent to a weight. The NCPI intent score reflects the different prioritization that some countries place on leveraging specific cyber capabilities. This assumes that a country can only fully deploy its cyber capabilities in a domain, such as national surveillance, if it shows a 100 percent intent to do so. In all other cases we adjusted the value of the individual capability indicators according to the strategic importance each country attributes to them.

Sensitivity Analysis

We have performed sensitivity analyses on the index to test the impact of our analytical framework. Most importantly, we have computed our NCPI weighing each capability equally. This alternative framework does not affect our ranking in a substantial manner.

The capability indicators have been measured on different scales. We have standardized each indicator to bring variables with different response scales to a comparable metric. We have opted for a procedure known as Min-Max normalization which is widely used across disciplines to transform raw data. This normalization technique, comes, however, with some limitations. Among others, extreme values influence the final score. Other techniques, such as the z-standardization, are more robust vis-a-vis outliers and better suited to reflect the variation in the measures.[41] Some of our measures are not normally distributed, limiting our choice to the Min-Max normalization. We have, however, performed some quality checks with the other measures that follow a normal distribution. Among others, we have computed the capability index using z-standardization and compared the results with our method of choice.

We have correlated both the composite indicator and its dimensions with other existing measures. For instance, we have correlated the composite indicator with relevant measurable phenomena (similar composite indicators but also relevant quantities e.g. GDP, GDP per capita, etc.) to identify similarities or differences.

As expected, the NCPI is positively related to both the ITU Cyber Index, shown in Graph 8, and the GDP per capita, shown in Graph 9. This correlation indicates that the higher the cyber resilience of a country and the more wealth a country has the greater its national cyber power.

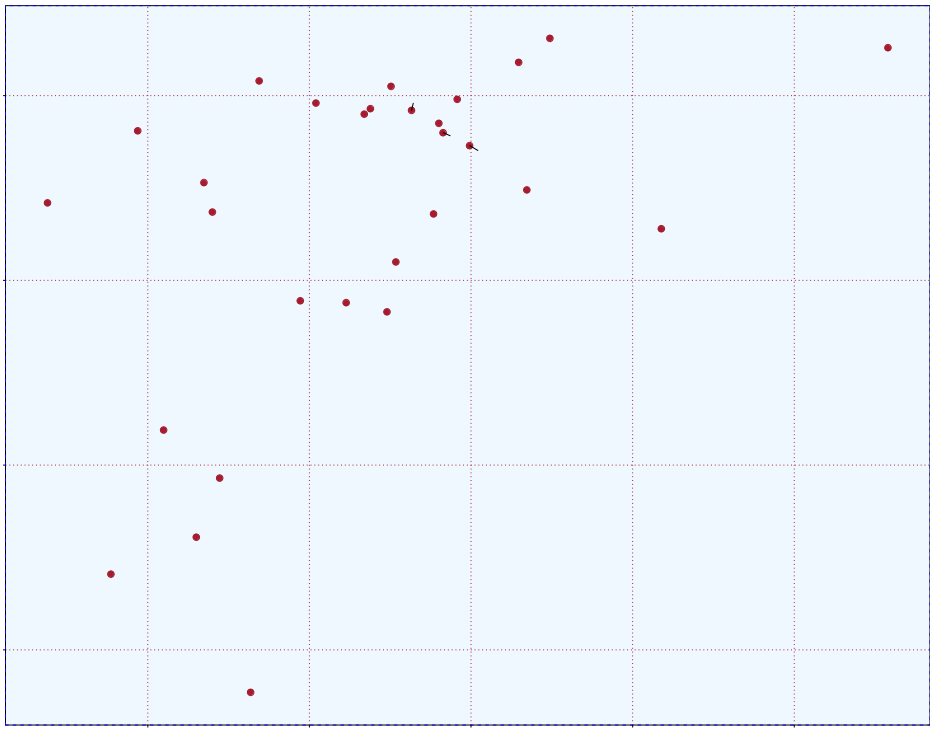
As Graph 8 shows, there are also important differences. For example, when comparing the NCPI with the ITU Global Cyber index we find that Egypt,

41 Carrino, L. (2017). The role of normalization in building composite indicators. rationale and consequences of different strategies applied to social inclusion. In *Complexity in Society: From Indicators Construction to their Synthesis* (pp. 251-289). Springer, Cham.

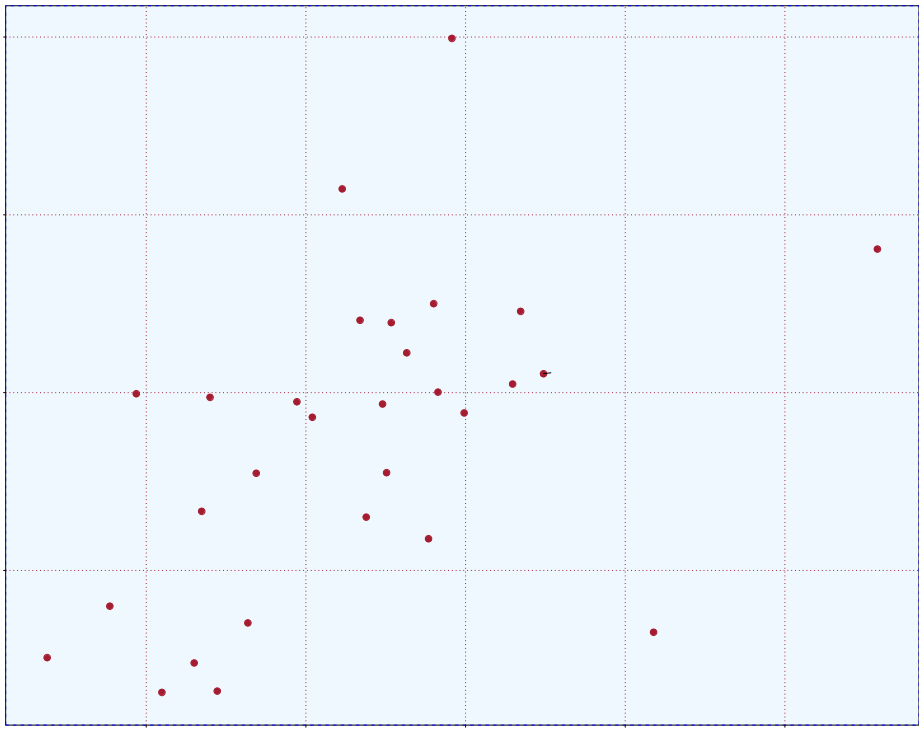
Lithuania, Turkey, and Saudi Arabia score relatively high on the ITU but low on the NCPI.

The results from the correlation between the NCPI and the GDP per capita suggest a linear relationship between the two measures: higher GDP per capita equates higher national cyber power. There are, however, important outliers, where China is a notable example. Although the GDP per capita is low in China, its NCPI ranking is particularly high.

Graph 8: Correlation Between Belfer NCPI and ITU Global Cyber Index



Graph 9: Correlation Between Belfer NCPI and GDP per Capita



5. Conclusion

Belfer's National Cyber Power Index is a new approach to conceptualizing and measuring cyber power at the country level. We provide a multidimensional and disaggregated measure of national cyber power that reflects the complexity of the concept. The measure distinguishes between seven main objectives of cyber power: (1) Surveilling and Monitoring Domestic Groups; (2) Strengthening and Enhancing National Cyber Defenses; (3) Controlling and Manipulating the Information Environment; (4) Intelligence Gathering and Collection in other Countries for National Security Objectives; (5) Growing National Cyber and Technology Competence; (6) Destroying or Disabling an Adversary's Infrastructure and Capabilities; and, (7) Defining International Cyber Norms and Technical Standards.

Cyber capabilities are multi-use; every measure of cyber power can at once empower and expose it to vulnerabilities.

Researchers and practitioners may use the NCPI in different ways. First, they might use the NCPI's aggregated measure of cyber power across all seven objectives to understand which country is the most comprehensive cyber power. Second, our NCPI framework can help a broader audience better understand how each objective contributes to cyber power, and how countries with varying levels of intent and capability may interact in cyberspace. Third, users who are interested in a specific national objective or component of our NCPI can view our analysis by: one of the seven national objectives to identify the most capable countries in the area; by intent; or capability.

We have created the NCPI with the aim of providing a measure to help policy practitioners and academics move the cyber policy conversation forward. Based on the current state of the field, there is still room to develop a more precise and nuanced framework for understanding cyber power but our framework and the data we have collected can still move the cyber policy conversation beyond its current focus on offensive cyber. Finally, we hope that this study encourages more transparency around cyber capabilities and intent which is a critical component for preventing dangerous escalation and conflict between countries.

Bibliography

Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat, espionage, sabotage, and revenge*. Retrieved from https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

Barker, T. (2017, May 26). Germany Strengthens its Cyber Defense. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/germany/2017-05-26/germany-strengthens-its-cyber-defense%0D

Bellingcat. (2018, October 4). 305 car registrations may point to massive GRU security breach. *Bellingcat*. Retrieved from https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/

Breene, K. (2016) "Who are the cyberwar superpowers?" *World Economic Forum*. Date accessed, 30 January 2020. https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Connell, M. (2014). *Deterring Iran's Use of Offensive Cyber*. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a617308.pdf

Council on Foreign Relations (2019), 'Cyber Operations Tracker'. Accessed December 2019. https://www.cfr.org/interactive/cyber-operations.

Curley, M. G. (2018). The Provision of Cyber Manpower. *MCU Journal*, *9*(1), 191–217.

Curtis E Lemay Center for Doctrine Development and Education. (2016). "An Effects-Based Approach to Planning," *Air University Alabama.* Last modified, 4 November 2016. Date accessed, 30 January 2020. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D19-OPS-Effects-Based-Plan.pdf

Denning, D. (2017, December 12). Iran's cyber warfare program is now a major. *Newsweek*. Retrieved from https://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427

DOD. (2016, October 24). All Cyber Mission Force Teams Achieve Initial Operating Capability. *Www.Defence.Com*. Retrieved from https://www.defense.gov/Newsroom/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/

DOJ. (2018). *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps*. Retrieved from https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

Economist Intelligence Unit (2006) Democracy Index. Accessed June 30, 2020. https://www.economist.com/media/pdf/DEMOCRACY_INDEX_2007_v3.pdf

Economist Intelligence Unit & Booz Allen Hamilton (2011) ""Cyber Power Index: Findings and Methodology 2011", Date accessed, 30 January 2020. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

Freedom House. (2020) Freedom in the World Methodology. Accessed June 30, 2020. (https://freedomhouse.org/reports/freedom-world/freedom-world-research-methodology).

Gao. (2019). Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations, (August). Retrieved from https://www.gao.gov/assets/710/700940.pdf

GlobalStats (2020). "Search Engine Market Share Worldwide—May 2019-2020". *Statcounter.* Accessed June 20th, 2020. https://gs.statcounter.com/search-engine-market-share

Hathaway, M., Demchak, C., Kerben, J., Mcardle, J., & Spidalieri, F. (2016). *Germany Cyber Readiness at a Glance*. Retrieved from www.potomacinstitute.org

International Telecommunications Union. (2018). "Global Cybersecurity Index 2018," Published 2019. Date accessed, 30 January 2020.

Jiji. (2018, December 1). Japan working on ability to counter cyberattacks. *Japan Times*.

Joshi, S. (2013, June 19). An IT superpower, India has just 556 cyber security experts. *The Hindu*. Retrieved from https://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece

Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*. Washington, D.C.: National Defense University Press

Langner, R. (2016) "Cyber Power—An Emerging Factor in National and International Security". *Center for International Relations and Sustainable Development*. Autumn, Issue No.8. Accessed on June 7, 2020.

Laudrain, A. (2019, February 26). France's new offensive cyber doctrine. *Lawfare*. Retrieved from https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

Lewis, J. A. (2019). *Iran and Cyber Power*. Retrieved from https://www.csis.org/analysis/iran-and-cyber-power

Mandiant. (2013). *Apt1: Exposing One of China's Cyber Espionage Units*. https://doi.org/10.1007/3-540-30683-8_102

McGhee, A. (2017, June 30). Cyber Warfare unit set to be launched by Australian Defence Forces. *ABC News*. Retrieved from https://www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230

Mueller, R. S. (2019). *Report by Special Counsel Robert S. Mueller on the Investigation into Russian Interference in the 2016 Presidential Election. Volume I.*

OECD (2008). 'Handbook on Constructing Composite Indicators: Methodology and User Guide". *Organisation for Economic Co-operation and Development*. Date accessed September 4th 2020. Available here: www.oecd.org/publishing/corrigenda

Oliphant, R. (2017, May 6). Who are Russia's Cyber-warriors and what should the west do about them? *Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2016/12/16/russias-cyber-warriors-should-west-do/

Oliphant, R. (2018, October 4). What is Unit 26165, Russia's elite military hacking center? *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2018/10/04/unit26165-russias-elite-military-hacking-centre/

Tkacheva, O., Schwartz, L., Libicki, M., Taylor, J., Martini, J. and Baxter, C., (2013) "Internet Freedom and Political Space". *RAND Corporation*. Santa Monica, CA: RAND Corporation Accessed on June 7, 2020. https://www.rand.org/pubs/research_reports/RR295.html. Also available in print form.

The Associated Press. (2015, January 6). South Korea: North Korea has 6,00-member cyber army. Retrieved from https://phys.org/news/2015-01-south-korea-north-member-cyber.html

U.S. Department of Commerce & U.S. Department of Homeland Security, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future," *National Institute of Standards and Technology: Computer Security Resource Center.* Published 10 May 2018. Accessed 30 January 2020. https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/supporting-growth-and-sustainment-of-the-cybersecurity-workforce/final

Vavra, S. (2017). axios.com. Retrieved from https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html

Vidoli, Francesco, and Elisa Fusco (2019). *Compind: Composite Indicators Functions*. Date accessed September 4th 2020. Available here: https://CRAN.R-project.org/package=Compind

Voo, Julia., Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach (2020). "Reconceptualizing Cyber Power". *Belfer Policy Paper.*

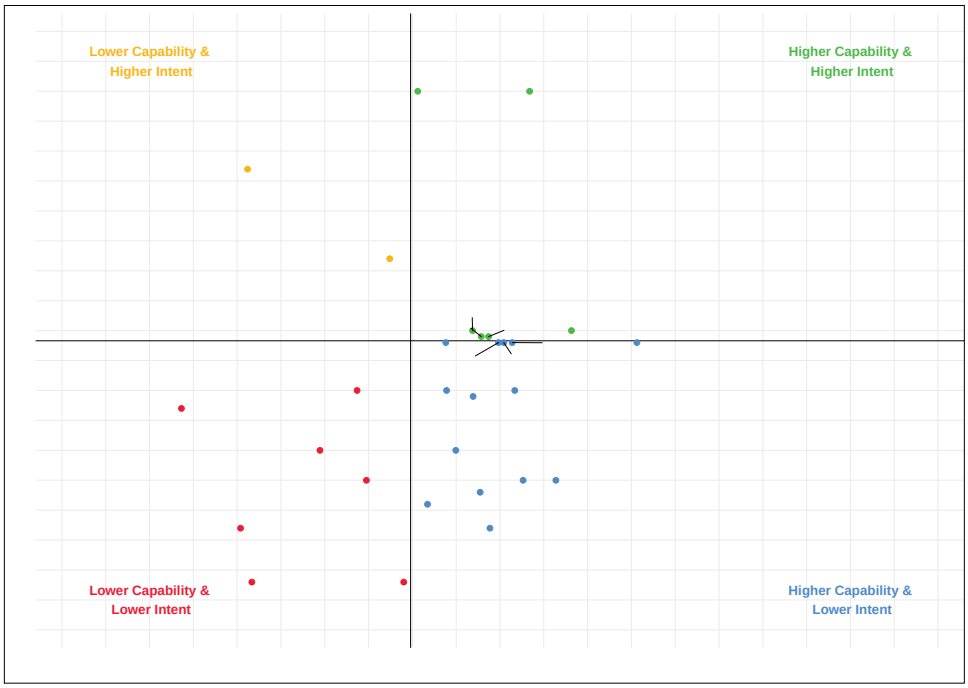
Wen, Philip. (2018) "China Denies 'Slanderous' Economic Espionage Charges from US allies". *Reuters*. Published December 18, 2018. Accessed June 30, 2020. https://www.reuters.com/article/us-china-cyber-usa-ministry/china-denies-slanderous-economic-espionage-charges-from-u-s-allies-idUSKCN1OK03Y

White House. (2018). "National Cyber Strategy of the United States of America Cyber Strategy". Published September 2018. Accessed 30 January 2020. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Zaaiman, J., & Louise, L. (2015). *Proceedings of the 10th International Conference on Cyber Warfare and Security ICCWS-2015*. Reading: Academic Conferences and Publishing International Limited. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=piikBwAAQBAJ&oi=fnd&pg=PA20&dq=compare+Military+Cyber+power+manpower&ots=EXxOscvBdz&sig=BYSy1JGfaj76m1TKHb8UD8W8wqY#v=onepage&q=compare Military Cyber power manpower&f=false

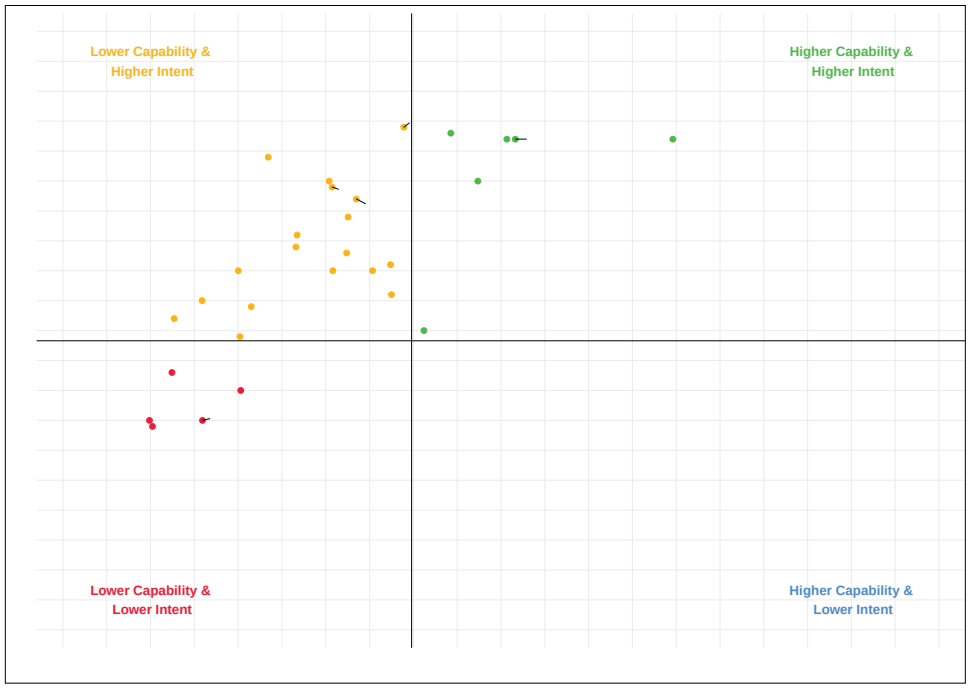
Annex A. **NCPI Plot Charts by Objective**

Surveillance

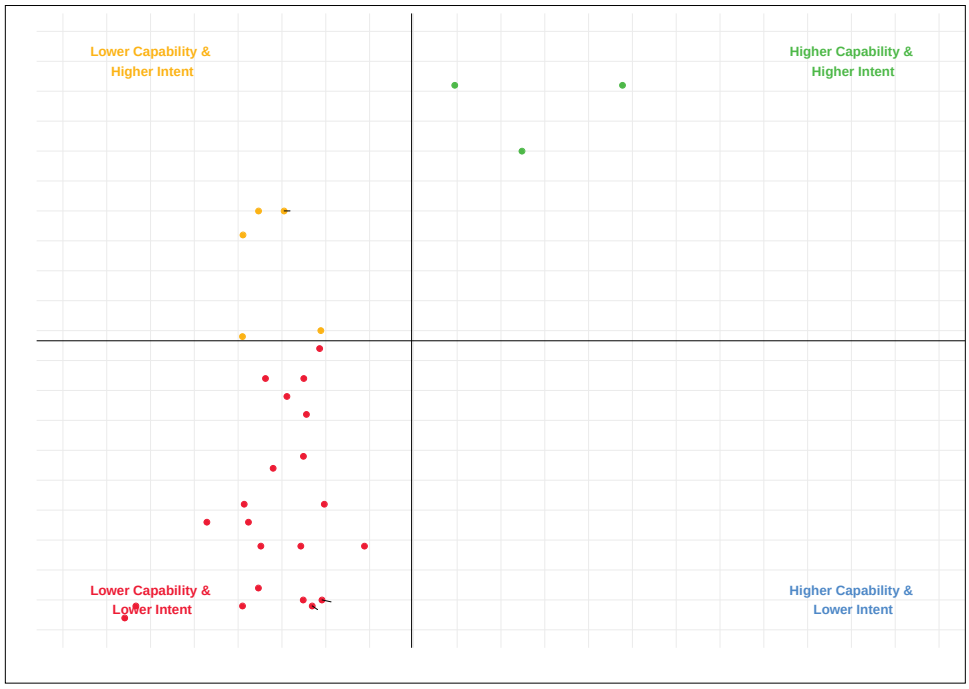


Defense

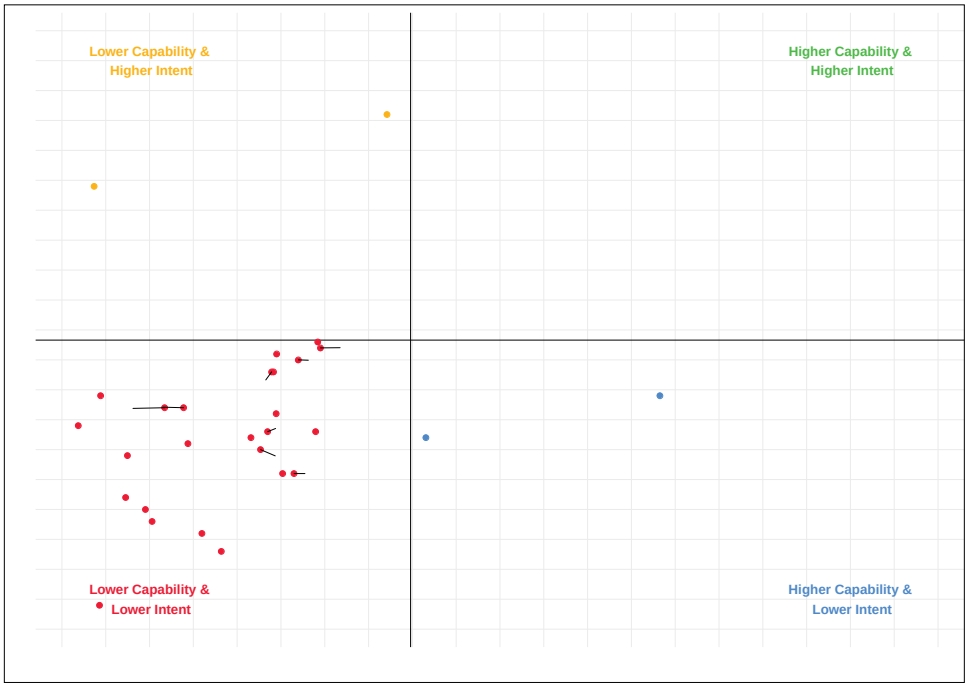
Norms



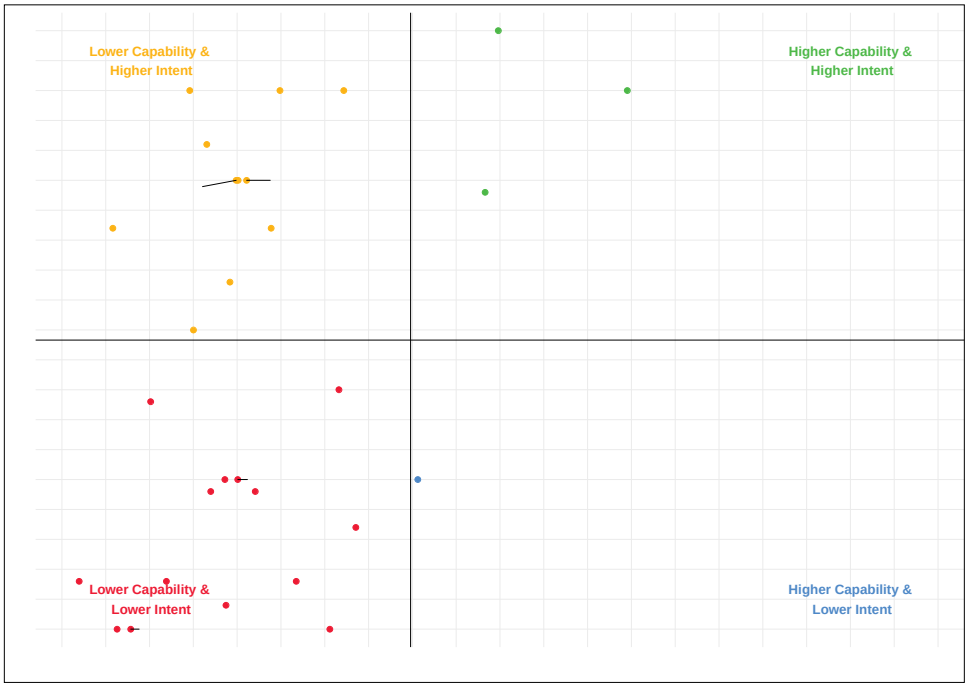
Information Control



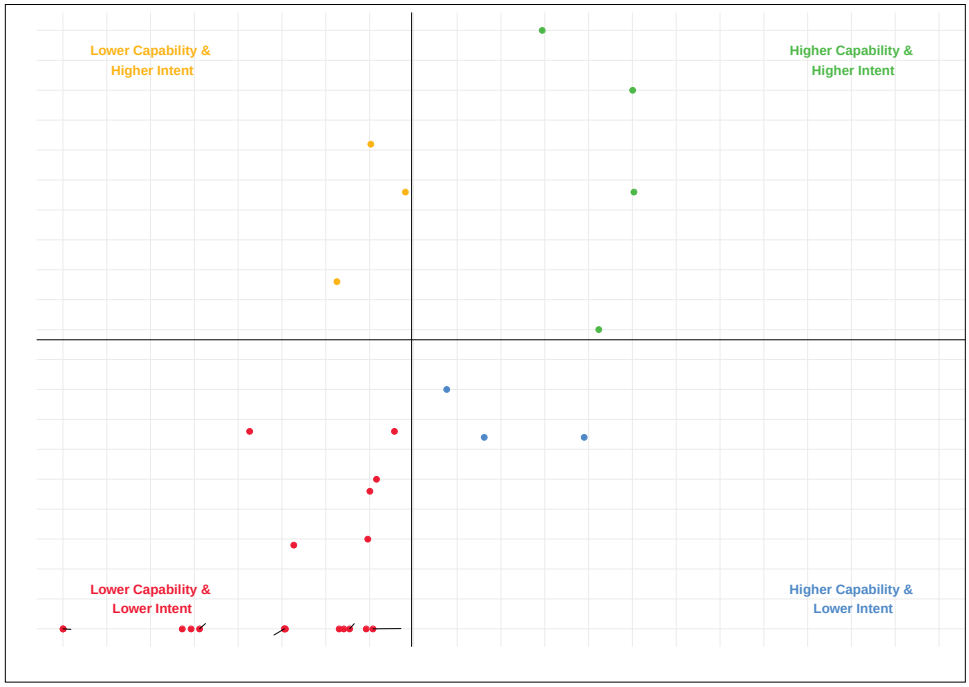
Commerce



Intelligence



Offense


Lower Capability &
Higher Intent
Higher Capability &
Higher Intent
Lower Capability &
Lower Intent
Higher Capability &
Lower Intent

Annex B. **Detailed Explanation of Intent Indicators by Objective**

Surveillance

Indicator	Meaning	Source Description	Year	Scoring Method
Does the country's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the country 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 country'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 country's cyber capabilities.	2020	Yes/No
Does the country's military cyber unit or command acknowledge that the country has a destructive cyber capability?	Having a dedicated military cyber unit or command shows that a country 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 countries 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 country'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.	2020	Yes/No
Does the country's signals intelligence agency or foreign intelligence service acknowledge that the country has a destructive cyber capability?	Acknowledgement that the country's intelligence agency has a cyber mission	Analysis of the online presence of each country'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.	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	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 country.	Use CFR Cyber Operations Tracker figures to assess whether a country has been attributed as conducting 1 or more attack	2020	Observed in 1 or more attack: Yes/No
If destructive activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If destructive activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No

Defense

Indicator	Meaning	Source Description	Year	Scoring Method
Has the country published a cyber security 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 country for CNI protection plans or strategy, or plans to protect Government IT systems	2020	Yes/No
Does the country undertake cyber awareness and cyber hygiene campaigns?	Is the country 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	2020	Yes/No
Has the country 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.	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	Objective present in >1 strategy: Yes/No
If Strengthening and Enhancing National Cyber Defenses activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If Strengthening and Enhancing National Cyber Defenses activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No
If national growing national cyber and technology competence activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If growing national cyber and technology competence activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No

Intelligence

Indicator	Meaning	Source Description	Year	Scoring Method
Does the country's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the country 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 country'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 country's cyber capabilities.	2020	Yes/No
Does the country's military cyber unit or command acknowledge that the country has a cyber intelligence-gathering capability?	Having a dedicated military cyber unit or command shows that a country 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 countries 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 country'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.	2020	Yes/No
Does the country's signals intelligence agency or foreign intelligence service acknowledge that the country has a cyber intelligence capability?	Acknowledgement that the country's intelligence agency has a cyber mission	Analysis of the online presence of each country'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.	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	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 country.	Use CFR Cyber Operations Tracker figures to assess whether a country has been attributed as conducting 1 or more attack	2020	Observed in 1 or more attack: Yes/No
If intelligence activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If intelligence activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No

Information Control

Indicator	Meaning	Source Description	Year	Scoring Method
Data protection law strength	How well defined and articulated each country's data protection regime is	Using DLA Piper's Data Protection rating for each country: https://www.dlapiperdataprotection.com/	2020	Heavy/ Robust/ Moderate/ Limited/ No information
Does the country's cyber military planning or strategy documents, or wider military planning or strategy documents, acknowledge that the country 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 country'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 country's cyber capabilities.	2020	Yes/No
Does the country's military cyber unit or command acknowledge that the country has cyber capabilities to control and manipulate the information environment?	Having a dedicated military cyber unit or command shows that a country 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 countries 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 country'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.	2020	Yes/No
Does the country's signals intelligence agency or foreign intelligence service acknowledge that the country has cyber capabilities to control and manipulate the information environment?	Acknowledgement that the country's intelligence agency has a cyber mission	Analysis of the online presence of each country'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.	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	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 country.	Use CFR Cyber Operations Tracker figures to assess whether a country has been attributed as conducting 1 or more attack	2020	Observed in 1 or more attack: Yes/No
If Controlling and Manipulating the Information Environment activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If Controlling and Manipulating the Information Environment activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No

Financial

Indicator	Meaning	Source Description	Year	Scoring Method
Is the country 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 countries to export and import products and services to one another without re-evaluation.	Figures taken from: https://www.commoncriteriaportal.org/ccra/members/	2020	Yes/No
Is the country 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 countries, allowing them to export and import cyber security and techology products	Figures taken from: https://www.iecee.org/dyn/www/f?p=106:40:0	2020	Yes/No
Has the country published a plan or strategy on attracting inward investment towards cyber firms or growing its cyber exports?	The country 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	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	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 country.	Use CFR Cyber Operations Tracker figures to assess whether a country has been attributed as conducting 1 or more attack	2019	Observed in 1 or more attack: Yes/No
If amassing Wealth and/or Extracting Cryptocurrency activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If amassing Wealth and/or Extracting Cryptocurrency activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No

Commercial

Indicator	Meaning	Source Description	Year	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 country. The higher the score the more active said country 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	2020	# 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 country.
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 country. The higher the score the more formal authority it has had on average in the technical committees and the more that country and its industry shapes the international standards agenda in ICT.	https://www.iso.org/technical-committees.html	2020	Each country 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 country 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 countries engage their private sectors and partner with them to tackle threats and meet national cyber objectives.	Analysis of the online presence of each country to find evidence of public-private partnerships that aim to increase the cyber security knowledge, skills, and focus of the country as a whole.	2020	Yes/No
Is there evidence the country 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 country to find evidence of specific national funding of cybersecurity research, or if the country funds national universities and research establishments with cyber security outputs.	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	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 country.	Use CFR Cyber Operations Tracker figures to assess whether a country has been attributed as conducting 1 or more attack	2020	Observed in 1 or more attack: Yes/No
If national growing national cyber and technology competence activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table

Indicator	Meaning	Source Description	Year	Scoring Method
If growing national cyber and technology competence activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy	2020	Yes/No

Norms

Indicator	Meaning	Source Description	Year	Scoring Method
How many times has the country sponsored UN GGE related resolutions between 2012-2016? Out of a total of five.	A higher score in this indicator demonstrates that the country is committed to taking the recommendations from the UN GGE and taking more formal steps towards shaping international norms around cyber activity .	Figures taken from: https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf	2017	1 = five times; 0.8 = 4 times; 0.6 = 3 times; 0.4 = 2 times; 0.2 = 1 time; 0 = never
How many times has the country 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	2020	1 = five times; 0.8 = 4 times; 0.6 = 3 times; 0.4 = 2 times; 0.2 = 1 time; 0 = none of these times
Has the country 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.' Countries that participate demonstrate a willingness to help share cyber best practice and norms.	Figures taken from: https://thegfce.org/member-overview/	2020	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 country. The higher the score the more active said country 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	2020	# 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 country.
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 country. The higher the score the more formal authority it has had on average in the technical committees and the more that country and its industry shapes the international standards agenda in ICT.	https://www.iso.org/technical-committees.html	2020	Each country 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 country 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 country 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	2020	Each country 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 country's participation across all three groups was taken, and the final range is between 0 and 1.
Has the country participated in bilateral or multilateral cyber defence exercises?	Demonstrates a willingness to share expertise and capacity building efforts with other countries	Internet search of Government websites and reputable sources for references to participation in bi or multi-lat cyber defence exercises	2020	Yes/No
Consistency of objective: is it pursued in >1 Strategy?	Countries 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).	2020	Observed in 1 or more attack: Yes/No
If Defining International Cyber Norms and Technical Standards activity is acknowledged in the country's national cyber strategy: include strategy score	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
If Defining International Cyber Norms and Technical Standards activity is acknowledged in the country's national cyber strategy: include financial score	The country is sufficiently committed to deliver its strategy to appropriate national funds to meet its outputs	The country has announced increased cyber funding since the publication of the most recent strategy		Yes/No

Annex C. **Detailed Explanation of Capability Indicators**

#	Indicator	Meaning	Source	Year	Scoring Method
1	**Cyber related Laws**	Measurement of how active a country has been in implementing content, privacy, and cyber crime laws	Belfer Cyber Power Project	2020	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)
2	**State-backed Cyber Attacks**	Number of publicly attributed notably sophisticated cyber attacks	CSIS	2018 / 2019	Count of cyber attacks attributed to state sponsored actors
3	**Bilateral Cyber Agreements**	Number and quality of bilteral formal and/or informal agreements signed by the national government in cyberspace, scored by recency.	Belfer Cyber Power Project	2020	For each of the agreements between countries: 1 = meeting, remarks 2 = Joint Statement, cooperation, framework 3 =Agreement / MOU
4	**Multilateral Cyber Agreements**	Number and quality of multilateral formal and/or informal agreements signed by the national government in cyberspace, scored by recency.	Belfer Cyber Power Project	2020	For each of the agreements between countries: 1 = informal/ conference / regional 2 = informal / conference / Global 3 = Formal Regional Agreement / Member of Regional Org 4 = Formal multilateral Agreement / Member of Global Org
5	**Cyber Miltary Doctrine**	Cyber Strategies detailing offensive or defensive military capabilities in cyberspace	Belfer Cyber Power Project	2020	0 = no cyber military strategy 1= draft of a cyber military strategy 2 = potentially outdated cyber military strategy (5 years or more) 3 = new cyber military strategy (less than 5 years) / potentially outdated military strategy but consistently pursued 4 = established and refreshed cyber military strategy (strategy less than 5 years old but cyber military strategy consistently followed
6	**Global Top 100 Tech Firms**	Number of Global Top 100 tech firms headquartered in country.	Thomson Reuters	2018	Count of top tech firms per country
7	**High Tech Exports**	Percentage of high tech exports as total of manufactuing exports	World Bank	2018	Higher values indicate more technology exports.
8	**Human Capital**	Measurement of how easy it is to find skilled employees in a given country	World Economic Forum	2019	The measure of interest is based on the question: "In your country, how easy is it for companies to find employees with the required skills for their business needs? (1 = extremely difficult, 7 = extremely easy)". The measure has subsequently been rescaled to a 100 point scale with high values representing high availability of skilled employees
9	**Cyber Military Staffing**	Number of individuals in staff positions for military's cyber forces	Belfer Cyber Power Project	2020	Number of individuals that are reported in the open source that are working on cyber forces.
10	**Centralized Cyber Command**	The existence and age of a national cyber command.	Belfer Cyber Power Project	2014-2020	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)
11	**Top Cybersecurity Firms**	Number of global top cyber security firms headquartered in country	Cybersecurity Ventures	2019	Number of Top 150 cybersecurity firms listed in the ranking.
12	**Computer Infection**	Percentage of computers in country that are infected with malware	Comparitech	Q3 2019	Percentage of users attacked (unauthorized access, destruction, disruption) during this period
13	**Mobile Infection**	Percentage of mobiles in country that are infected with malware	Comparitech	Q3 2019	Percentage of users attacked (unauthorized access, destruction, disruption) during this period
14	**Social Media Users**	Percentage of active social media accounts	Statista	2020	Share of internet users visiting social networking sites.
15	**Internet Users**	Internet penetration rate within a country.	World Bank	2017-2018	Higher the more individuals use the internet
16	**Surveillance Technology**	Number of private sector surveillance companies with offices in/ or operating in state	Privacy Intenational	2016	Count of the number of surveillance companies that operate in a country
17	**Top websites**	Number of websites in the Alexa Top 50 that belong to organizations HQ in that country	Alexa	2019	Number of sites in the Top 50
18	**Top news sites**	Number of news sites in the Alexa Top 50 that belong to organizations HQ in that country	Alexa	2019	Number of sites in the Top 50
19	**Content Removal Requests**	Number of takedown requests to Google from a government entity	Google	2018-2019	Number of requests
20	**Freedom on the Net**	Freedom House's score for how free citizens are online	Freedom House & Freedom of the World	2019	0-100: 3 separate scores aggregated together: a) obstacles to access b) limits on content c) violations of users rights. For seven countries we used freedom of the World rankings because Freedom House did not have the information.
21	**Patent Applications**	Number of domestic patent filings by residents of that country	World Development Indicators	2018	Number of domestic patent filings (residents only). Per capita measure.
22	**Broadband Speed**	Measurement of broadband speed relevant to the fastest broadband rates in the world	Speedtest Global Index	March 2020	10 out of 10 is Singapore which has the highest broadband speed in the world.
23	**Mobile Speed**	Measurement of mobile speed relevant to the fastest mobile rates in the world	Speedtest Global Index	March 2020	10 out of 10 is UAE which has the fastest mobile internet in the world.
24	**E-Commerce**	National E-commerce sales as a percentage of GDP	UNCTAD	2017 and 2020	Higher the more e-commerce sales.
25	**CSIRT**	Existence of a Cyber Security Incidence Response Team	Belfer Cyber Power Project	2020	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
26	**Vulnerabilities**	Cumulative percentage of the vulnerabilities listed for a country's infrastructure in the Shodan database	Belfer Cyber Power Project	2020	Cumulative percentage of the Shodan search results.
27	**Global Soft Power**	Country scores in the Global Soft Power Index	Brand Finance	2019	The scores calculated by Brand Finance's was part of their Soft Power index. These same scores were used for the Belfer Cyber Power Index.

The data collected on capabilities can be categorized into eight themes as presented below:

- Evidence of Attacks
- National Online Content
- Domestic State Cyber structures
- Cyber Vulnerability Mitigation
- Private Sector, Trade, and Innovation
- Connectivity
- Workforce
- Legal and Policy Frameworks

Evidence of Attacks

Indicator used:

- Council on Foreign Relations Cyber Operations Tracker

A country's track record of carrying out cyber operations is a key metric for capability. Where a country has carried out a cyber-attack for one of the seven objectives, it clearly has the capability in that area. However, known operations do not reflect the full picture—not all countries demonstrate their capabilities, and even those that do, may not demonstrate the full range of their capabilities because not only does this make strategic sense, but often it is not needed. For this indicator we analyzed, by objective, publicly attributed cyber operations contained within the Council on Foreign Relations' Cyber Operations Tracker. CFR's data is drawn from pre-existing databases on state-sponsored cyber-attacks[42] and in-house data collection from more recent cases reported in the media and government statements. This indicator also reflects a country's intent as outlined in Section 3.

42 Such as Florian Roth's APT Groups and Operations spreadsheet, CSIS' list of significant cyber events, and Kaspersky Lab's Targeted Cyberattacks Logbook.

National Online Content

Indicators used:

- Top Websites as listed on Alexa
- Top News Sites as listed on Alexa
- Google Content Removal Requests
- Freedom on the Net Rating

A country's ability to create and control online content is relevant to several national objectives. Through the creation of online content, a country can better influence its own citizens and citizens of other countries. Similarly, the more control a country has over online content, which we can measure through an analysis of successful content removal requests a country has submitted to Google, the more it is trying to control its information environment.

Limitations of this indicator include information on the top news- and websites do not take censorship into account. Despite a top global ranking, some websites are completely blocked in certain countries. Our use of Google content removal for example, does not consider other search engines.[43] Additionally, general freedom (used in a sister ranking to Freedom on the Net) does not equate to Internet freedom, which was used as a substitute if the Freedom on the Net ranking did not have a score for one of the thirty countries placed in the NCPI.

Domestic Government Cyber Structures

Indicators used:

- Existence of a National Cyber Command
- Existence of a Computer Security Incident Response Team (CSIRT)

43 According to GlobalStats Statcounter, between May 2019 and May 2020 the search engine market share worldwide was: Google (92.06%), Bing (2.61%); Yahoo (1.79%), Baidu (1.16%), Yandex (0.56%), and Yandex RU (0.52%).

have the value for mobile infection rate. As the two values are strongly related, we took the same value for computer infection rate.

These indicators cover only one aspect of cybersecurity and are only a sample of computer infections and vulnerabilities.

Private Sector, Trade, and Innovation

Indicators used:

- Active E-commerce Market
- Existence of Private Sector Surveillance Companies
- Number of Global Top 150 Cybersecurity Firms Headquartered in Country
- High-tech Exports as a Percentage of Manufacturing Exports
- Number of Global Top 100 Tech Firms Headquartered in Country
- Number of Patent Applications
- An active e-commerce market signals that a given country actively pursues strategies to promote businesses online. Although we consider this indicator to be positively related to cyber power, high activity in e-commerce also puts a country at risk for potentially disruptive actions.

The number of private cybersecurity firms hosted within a specific country contributes to a country's cyber power, depending on the type of private cyber security firm involved. Organizations that provide better defensive, or "blue-team", capabilities, can help bolster government defenses, whereas surveillance organizations can better provide governments with tooling to assist domestic law enforcement.

Manufacturing exports illustrate how developed a country's industrial cyber capability is, and how much influence Country A may have over other Country B's electronic environment through exports of Country A's own technology and standards. The indicator however suffers because it is

not limited to ICT only, and due to complex supply chains, does not reflect where the intellectual property originates from.

The number of top technology firms based in a country indicate to what extent a country has the workforce and knowledge to innovate. By way of a proxy, the project included data on how many of the Top 100 Global Technology and Cybersecurity companies were incorporated in each country.

We used patent applications per resident as a measure of innovation. A large amount of patent applications signal that a country is investing in the research and development that are needed to advance cybersecurity technology.[44]

We attempted to gather data to indicate how much financial resource each government had allocated to developing cyber-related capabilities. For some countries, there were headline figure announcements and for others, some figures were linked to the creation of a new organization or an investment fund for research or collaboration with industry for cybersecurity. Overall, it proved difficult to generate comparable data to allow an assessment of cyber investment across countries. The breadth of cyber activity is not the domain of a single government entity and elements of cyber power e.g., intelligence gathering by an intelligence agency or military costs are not publicly available even in countries with a high degree of transparency due to national security concerns.

44 Patent regimes themselves have experienced major changes that have encouraged an increase in patenting. See http://www.oecd.org/science/inno/24508541.pdf.

Connectivity

Indicators used:

- Percentage of Internet Users Using Social Media
- Percentage of Individuals Using the Internet
- Speed of Broadband and Mobile Internet
- Use of social media and internet within a country indicates how large or small the attack surface of a country is indicating both the level of connectivity of a country as well as the populations' potential vulnerability to influence operation efforts by malicious actors.

We took broadband and mobile speed as additional proxies for good connectivity, which can influence several capabilities and objectives. These indicators suggest that faster internet and mobile speed is linked with a more developed, digitized, and innovative national economy. At the same time, we acknowledge that digital infrastructure with low levels of cybersecurity exposes a country to significant vulnerabilities. In addition, the broadband and mobile speed indicator faces another challenge in that the data was collected only via the users that opted to "test" the speed of their broadband or mobile via Speedtest Global Index's App.[45]

Workforce

Indicators Used:

- Human Capital/ Skilled Employees
- Cyber military personnel
- A country's cybersecurity capability is dependent on countries having access to highly skilled employees. Cyber defense requires a range of skills, from technical programmers and coders, to analysts, project managers, and researchers.

45 Note: March 2020 might not be the best sample due to the global impacts of the novel coronavirus. See Speedtest's article on, "Tracking COVID-19's Impact on Global Internet Performance". Updated May 4, 2020. https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#/

The first metric is based off a measure of human capital from the World Economic Forum to reflect the availability of highly skilled staff that can work in a country's cyber industry—both government and private sector—that contribute to a country's capability. A weakness of this indicator is that it does not measure cybersecurity relevant skills alone.

The second metric is an indicator of a country's cyber military capability. Many countries' cyber offensive and defensive capability lies within their military. This indicator reports absolute counts of individuals working in military cyber roles in the respective country. The data is collected from an in-house search of publicly available information, media reporting and academic assessments. The numbers were difficult to ascertain and our overall confidence in the accuracy is low. Challenges with this indicator include whether a given country included personnel in its military count that are also included in other agency counts which may be exacerbated by national security concerns that increase the lack of transparency around military personnel numbers.

Domestic and International Legal & Policy Frameworks

Indicators used:

- Multilateral and Bilateral Agreements
- Domestic Legislation (i.e. that are online content, privacy and cybersecurity related)
- Global Soft Power Index
- Cyber Military Doctrine
- International norms are not fixed; they move and adjust to cultural, social, and political changes over time.[46] As cyberspace has grown, so have the rules, norms, and conventions of how countries, businesses and individuals operate within it. For many countries—as outlined in their national cyber strategies—working with others to address challenges such as cybercrime, as well as to shape

46 Ann Florini. 1996. 'The Evolution of International Norms'. *International Studies Quarterly*. Vol 40, No.3. pp 363-389).

agreements to determine acceptable conduct within the cyber domain is a priority.[47] We sought to quantify how active a country has been in pursuing international cooperation and influence by measuring how many informal and formal statements of intent for international collaboration have been announced. For this indicator, we used data collected by UNIDIR and published on its' Cyber Policy Portal.

We gave a numerical score to each agreement depending on whether it was an informal statement of cooperation, a formal bilateral agreement, or a multilateral agreement. Greater weighting was given to formal agreements, with multilateral agreements receiving the highest score. A weakness of this indicator is that it is a measure of intent to collaborate rather than an indicator of the realization of a commitment, its scale or regularity. Another challenge is the consistency between governments on the criteria for the level of agreement between countries.

A country's ability to influence other citizens and governments thereby contributing to global norm-setting depends on several elements, including but not limited to, domestic legal frameworks, activity in multilateral fora and other countries' perception of it.

Finally, a country that is seeking to develop its cyber military capability to conduct offensive operations is likely to require a military doctrine or strategy. This measure was based on the existence of the publication of an official government military strategy and expert assessments. If the doctrine in question has been through multiple iterations, we assessed that the cross-government coordination and therefore capability would be better established.

47 As has been established in traditional domains with international law.

Annex D. **Radar Charts of All Capabilities by Country**

Australia

Brazil

Canada

China

Egypt

Estonia

France

Germany

India

Iran

Israel

Italy

Japan

Lithuania

Malaysia

Key:

1. **Commercial** = Growing National Cyber and Technology Competence
2. **Defense** = Strengthening and Enhancing National Cyber Defenses
3. **Intelligence** = Foreign Intelligence Collection for National Security
4. **Information Control** = Controlling and Manipulating the Information Environment
5. **Norms** = Defining International Cyber Norms and Standards
6. **Offense** = Destroying or Disabling Adversary Infrastructure
7. **Surveillance** = Surveilling and Monitoring Domestic Groups

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

www.belfercenter.org/CCPI

Printed in the United States of America