“National Cyber Power Database”

Version 1.0, released 9 September 2020

Description

The “National Cyber Power Database” includes information on cyber capabilities, cyber intent and cyber power of 30 countries in 2020 (annual updates are planned for the future). It includes three indices - the National Cyber Power Index (NCPI), the Cyber Capability Index (CCI) and the Cyber Intent Index (CII) – as well as 32 intent indicators and 27 capability indicators.
Cyber power is measured along seven 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 of cyber power, destroying, or disabling an adversary’s infrastructure commonly referred to as offensive cyber operations is only one of seven objectives countries pursue using cyber means.
For each objective, separate scores are featured in the database that allow to rank a country’s cyber capability, intent and power specific to that objective.

Keywords: Cyber Power, Cyber Capability, Cyber Intent, Surveillance, Defense, Offense, Information Control, Intelligence, Commerce, Norms

Authors: Julia Voo;
Irfan Hernani;
Simon Jones;
Winnona DeSombre;
Daniel Cassidy;
and Anina Schwarzenbach

Publication:
Voo, Julia; Irfan Hernani; Simon Jones; Winnona DeSombre; Daniel Cassidy; and Anina Schwarzenbach (2020). National Cyber Power Index 2020. Methodology and Analytical Considerations. China Cyber Power Initative. Report, Harvard Kennedy School’s Belfer Center for Science and International Affairs.

General

VARIABLE	DESCRIPTION		SOURCE	YEAR	SCORING METHOD
country	country name				

Capability Scores

VARIABLE	DESCRIPTION		SOURCE	YEAR	SCORING METHOD
score_capabilities	Overall Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_surveillance	Surveillance Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_defense	Defense Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_control	Information Control Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_intelligence	Intelligence Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_commercial	Commerce Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_offense	Offense Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)
score_norms	Norms Cyber Capability Score		Harvard Belfer Cyber Power Project	2020	0 (very low capability) to 1 (very high capability)

Intent Scores

VARIABLE	DESCRIPTION		SOURCE	YEAR	SCORING METHOD
score_intent	Overall Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_offense	Surveillance Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_commercial	Defense Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_intelligence	Information Control Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_control	Intelligence Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_defense	Commerce Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_surveillance	Offense Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)
intent_norms	Norms Cyber Intent Score		Harvard Belfer Cyber Power Project	2020	0 per cent (very low intent) to 100 per cent (very high intent)

Cyber Power Scores

VARIABLE	DESCRIPTION		SOURCE	YEAR	SCORING METHOD
score_capint	National Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_surveillance	Surveillance Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_defense	Defense Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_control	Information Control Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_intelligence	Intelligence Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_commercial	Commerce Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_offense	Offense Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)
capint_norms	Norms Cyber Power Score		Harvard Belfer Cyber Power Project	2020	0 (very low cyber power) to 1 (very high cyber power)

Capability Indicators

VARIABLE	DESCRIPTION		SOURCE	YEAR	SCORING METHOD
laws	Cyber related Laws	Measurement of how active a country has been in implementing content, privacy, and cyber crime laws	Harvard 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)
state_attack	State-backed Cyber Attacks	Number of publicly attributed notably sophisticated cyber attacks	CSIS	2018/2019	Count of cyber attacks attributed to state sponsored actors
attack_surveillance	State-backed Surveillance Cyber Attacks	Number of publicly attributed notably sophisticated cyber attacks for the surveillance objective	CSIS	2018/2019	Count of cyber attacks attributed to state sponsored actors
attack_control	State-backed Information Control Cyber Attacks	Number of publicly attributed notably sophisticated cyber attacks for the information control objective	CSIS	2018/2019	Count of cyber attacks attributed to state sponsored actors
attack_intelligence	State-backed Intelligence Cyber Attacks	Number of publicly attributed notably sophisticated cyber attacks for the intelligence objective	CSIS	2018/2019	Count of cyber attacks attributed to state sponsored actors
attack_commercial	State-backed Commerce Cyber Attacks	Number of publicly attributed notably sophisticated cyber attacks for the commerce objective	CSIS	2018/2019	Count of cyber attacks attributed to state sponsored actors
attack_offense	State-backed Offense Cyber Attacks	Number of publicly attributed notably sophisticated cyber attacks for the offense objective	CSIS	2018/2019	Count of cyber attacks attributed to state sponsored actors
bilat_agreement	Bilateral Cyber Agreements	Number and quality of bilteral formal and/or informal agreements signed by the national government in cyberspace, scored by recency.	Harvard Belfer Cyber Power Project	2020	For each of the agreements between countries: 1 = meeting, remarks 2 = Joint Statement, cooperation, framework 3 =Agreement / MOU
multi_agreement	Multilateral Cyber Agreements	Number and quality of multilateral formal and/or informal agreements signed by the national government in cyberspace, scored by recency.	Harvard Belfer 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
military_strategy	Cyber Miltary Doctrine	Cyber Strategies detailing offensive or defensive military capabilities in cyberspace	Harvard 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
tech_firm	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
tech_export	High Tech Exports	Percentage of high tech exports as total of manufactuing exports	World Bank	2018	Higher values indicate more technology exports.
human_capital	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
cybermil_people	Cyber Military Staffing	Number of individuals in staff positions for military's cyber forces	Harvard Belfer Cyber Power Project	2020	Number of individuals that are reported in the open source that are working on cyber forces.
cyber_command	Centralized Cyber Command	The existence and age of a national cyber command.	Harvard 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)

VARIABLE	DESCRIPTION		SOURCE	YEAR	SCORING METHOD
cyber_firm	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.
computer_infection	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
mobile_infection	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
socials_use	Social Media Users	Percentage of active social media accounts	Statista	2020	Share of internet users visiting social networking sites.
internet_use	Internet Users	Internet penetration rate within a country.	World Bank	2017-2018	Higher the more individuals use the internet
surveillance_firm	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
web_alexa	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
news_alexa	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
removal_google	Content Removal Requests	Number of takedown requests to Google from a government entity	Google	2018-2019	Number of requests
freedom_net	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.
patent_application	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.
patent_app_capita	Patent Applications (per capita value)	Number of domestic patent filings by residents of that country	World Development Indicators	2018	Number of domestic patent filings (residents only). Per capita measure.
broadband_speed	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.
mobile_speed	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.
ecommerce	E-Commerce	National E-commerce sales as a percentage of GDP	UNCTAD	2017 and 2020	Higher the more e-commerce sales.
ecommerce_capita	E-Commerce (per capita value)	National E-commerce sales as a percentage of GDP	UNCTAD	2017 and 2020	Higher the more e-commerce sales.
CERTS	CSIRT	Existence of a Cyber Security Incidence Response Team	Harvard 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
shodan	Vulnerabilities	Cumulative percentage of the vulnerabilities listed for a country's infrastructure in the Shodan database	Harvard Belfer Cyber Power Project	2020	Cumulative percentage of the Shodan search results.
softpower	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.

Intent Scores Construction

VARIABLE	OBJECTIVE	DESCRIPTION	MEANING	SOURCE DESCRIPTION	YEAR	SCORING METHOD
intent_offense	Destroying or Disabling an Adversary's Infrastructure and Capabilities	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	Acknowledgement that the country's intelligence agency has a cyber	Analysis of the online presence of each country's intelligence agency to	2020	Yes/No
		Consistency of objective: is it pursued in >1	Countries that have pursued a particular objective over multiple	Compare the objectives listed in the most recent strategy with those listed	2020	Objective present in >1 strategy: Yes/No
		Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent	Use CFR Cyber Operations Tracker figures to assess whether a country has	2020	Observed in 1 or more attack: Yes/No
		If destructive activity is acknowledged in the	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
		If destructive activity is acknowledged in the	The country is sufficiently committed to deliver its strategy to	The country has announced increased cyber funding since the publication of	2020	Yes/No
intent_commercial	Growing National Cyber and Technology Competence	What is the rate of participation in ISO/IEC	The International Organization for Standardization (ISO) and the	https://www.iso.org/technical-committees.html	2020	# of ISO/IEC Joint Technical Committees X is
		What is the quality of participation across	The International Organization for Standardization (ISO) and the	https://www.iso.org/technical-committees.html	2020	Each country was given a score for each
		Does the country have a public-private	Private-sector organisations represent a source of capability to boost	Analysis of the online presence of each country to find evidence of public-	2020	Yes/No
		Is there evidence the country has invested in	Investment in R&D is an essential component of growing cybersecurity	Analysis of the online presence of each country to find evidence of specific	2020	Yes/No
		Consistency of objective: is it pursued in >1	Countries that have pursued a particular objective over multiple	Compare the objectives listed in the most recent strategy with those listed	2020	Objective present in >1 strategy: Yes/No
		Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent	Use CFR Cyber Operations Tracker figures to assess whether a country has	2020	Observed in 1 or more attack: Yes/No
		If national growing national cyber and	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
		If growing national cyber and technology	The country is sufficiently committed to deliver its strategy to	The country has announced increased cyber funding since the publication of	2020	Yes/No
intent_intelligence	Intelligence Gathering and Collection in other Countries for National Security Objectives	Does the country's cyber military planning or	Like all large bureaucracies, militaries rely on clear hierarchies and	Analysis of the online presence of each country's Ministry of Defence (MOD)	2020	Yes/No
		Does the country's military cyber unit or	Having a dedicated military cyber unit or command shows that a	Analysis of the online presence of each country's military cyber force to	2020	Yes/No
		Does the country's signals intelligence	Acknowledgement that the country's intelligence agency has a cyber	Analysis of the online presence of each country's intelligence agency to	2020	Yes/No
		Consistency of objective: is it pursued in >1	Countries that have pursued a particular objective over multiple	Compare the objectives listed in the most recent strategy with those listed	2020	Objective present in >1 strategy: Yes/No
		Observed in attributed cyber attack	Unlike the other intent indicators, which demonstrate specific intent	Use CFR Cyber Operations Tracker figures to assess whether a country has	2020	Observed in 1 or more attack: Yes/No
		If intelligence activity is acknowledged in	See Strategy Score table	See Strategy Score table	2020	See Strategy Score table
		If intelligence activity is acknowledged in	The country is sufficiently committed to deliver its strategy to	The country has announced increased cyber funding since the publication of	2020	Yes/No
intent_control	Controlling and Manipulating the Information Environment	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	Like all large bureaucracies, militaries rely on clear hierarchies and	Analysis of the online presence of each country's Ministry of Defence (MOD)	2020	Yes/No
		Does the country's military cyber unit or	Having a dedicated military cyber unit or command shows that a	Analysis of the online presence of each country's military cyber force to	2020	Yes/No
		Does the country's signals intelligence	Acknowledgement that the country's intelligence agency has a cyber	Analysis of the online presence of each country's intelligence agency to	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

VARIABLE	OBJECTIVE	DESCRIPTION	MEANING	SOURCE DESCRIPTION	YEAR	SCORING METHOD
intent_defense	Strengthening and Enhancing National Cyber Defenses	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
intent_surveillance	Surveilling and Monitoring Domestic Groups	Does the country have at least one police or law enforcement agency with specialist cyber-crime expertise or that encourages citizens to report cyber-crime?	Shows that the country has given its law enforcement agencies the ability to prosecute cyber-crime and conduct cyber-based surveillance	Analysis of the online presence of each country for references to law enforcement expertise. Also looked for public comments by national politicians and senior police officers.	2020	Yes/No
		Does the country's domestic intelligence agency acknowledge surveillance cyber capabilities?	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
		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?	Shows the country is exploring cyber activity through the lens of CT and homeland security	Analysis of the online presence of each country's Minstry for the Interior or Homeland Security-focused department for national counter-terrorism or homeland security strategies, plans, and laws and whether it refers to cyber-based activities.	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 surveillance 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 surveillance 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

VARIABLE	OBJECTIVE	DESCRIPTION	MEANING	SOURCE DESCRIPTION	YEAR	SCORING METHOD
intent_norms	Defining International Cyber Norms and Technical Standards	How many of the past five UN Cyber Government Group of Experts (GGE) consultations has the country participated in?	The UN General Assembly First Committee on Disarmament and International Security, which, through its successive Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security, has facilitated some of the first efforts to reach global consensus on the binding and non-binding norms that apply to the digital environment and the behaviour of States in their uses of ICT. A higher score in this indicator demonstrates that the country has been party to the UN GGE consultations.	Figures taken from: https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf	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
		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