Digital Power and EMP

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Cyber Espionage

Before getting into “Digital Power” here is a short review of Cyber Espionage

Watch: *Essential Geopolitics China's Cyber Espionage Strategy*

- https://www.youtube.com/watch?v=o3X3scDlUWc
- Goes into some details on industrial espionage

Cyber Exercises

The U.S. government runs regular cyber exercises to prepare for cyber events. These scenarios can include:

- Destructive/disruptive cyber attacks in isolation (only digital attacks)
- Destructive/disruptive cyber attacks in conjunction with physical attacks
- Non-destructive cyber attacks (ex. Information collection)

One major program for these kind of exercises is Cyber Flag, run by U.S. Cyber Command

Cyber Flag

Read: *US Cyber Command exercise will help shape new tactics for changing threats* by Mark Pomerleau

- https://www.c4isrnet.com/cyber/2021/06/23/us-cyber-command-exercise-will-help-shape-new-tactics-for-changing-threats/

Read: Exercise Focuses on Collective Defense by U.S. Cyber Command Public Afairs

- https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense/

You are responsible for knowing the content of these articles

Cyber Flag

Some key points from the articles:

Cyber Flag exercises include international partners:

- *…over 430 individuals from 17 teams from the U.S., UK, Canada, National Guard, House of Representatives and U.S. Postal Service and is taking place across eight time zones.*

The scenarios evolve to properly address real-world threats:

- *Cyber Flag 21-1 is a U.S. response to the exploitation of SolarWinds to strengthen collective defense in cyberspace and affirm the importance of an open, reliable and secure internet.*

The U.S. has invested huge resources into cyber training

- They have built the National Cyber Range which is accessible all over the world
- There is also the Persistent Cyber Training Environment
  - Allows for growing the cyber range
  - Maintains a library of scenarios that can be quickly deployed

The exercises are also used to evolve tactics, responses, and team composition and structure

National, Military, and Cyber Power

Military Power:

From: *Information as Power: China's Cyber Power and America's National Security* by Colonel Jason M. Spade:

- *IN TERMS OF MILITARY CAPABILITIES, the United States has been the world's only superpower since 1991. In future conflicts, adversaries who cannot match U.S. military capabilities will necessarily look for asymmetric means to counter America's strength.*
- *As demonstrated in the 1991 Gulf War and the 2003 invasion of Iraq, information technology is critical to America's military superiority in areas such as command, control, and communications; intelligence gathering, surveillance, and reconnaissance; logistics, transportation, and administration. This reliance on information technology might prove to be America's asymmetric Achilles' heel.*
- *Cyber power, the employment of computer network attack and computer network exploitation, is a relatively inexpensive but potentially effective means by which an adversary might counter U.S. military power. And the potential for cyber power is not limited to use in a direct fight with America's military.*
- *Military power is one facet of national power, which also includes the economy as well as political and national will.*
- *The United States as a whole – the government and civil sector – is dependent on cyberspace and information systems for many routine and daily functions. America's highly networked society, using an Internet designed for open and easy information exchange, could be subject to cyber attack in 21st century cyber warfare.*

Notice the reference to “asymmetric” in the previous quotes

- This is an important concept when it comes to cybersecurity
- Make sure you have a good understanding of this concept

Reference: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

Military Power

China's Cyber Capability:

China and Russia are going to be referred to often in this class

In order to protect our national cyber infrastructures, we need to understand what they are doing and what they are capable of

From: *Information as Power: China's Cyber Power and America's National Security* by Colonel Jason M. Spade:

- *The People's Republic of China (PRC) is prominent among countries employing cyber attacks and intrusion against other nations. Taiwan is a perennial favorite for PRC-based cyber attacks. The first 'Taiwan/China Hacker War' erupted in 1999 when the President of Taiwan suggested state-to-state relations between the island and mainland. Chinese hackers responded by defacing Taiwan government, university and commercial sites. In 2003, mainland hackers penetrated networks in 30 Taiwan government agencies, including the Defense Ministry, Election Commission, National Police Administration, and many Taiwan companies. In 2004 hackers infiltrated the Ministry of Finance and Kuomintang Party. In 2005, the Taiwan National Security Council was targeted with socially engineered emails containing malicious code.*
- *China's cyber activities are not limited to Taiwan; they are global. In May 2007, Trojan horse programs sent terabytes of information from government networks at the German Chancellery and their foreign, economic and research ministries to what officials believe were PLA-supported servers in Lanzhou and Beijing. Security officials estimate 40 percent of all German companies have been targeted by state-sponsored Internet espionage, most coming from either China or Russia. In November 2007, the United Kingdom's Director-General of MI5 sent a confidential letter warning 300 chief executives and security chiefs at banks, accounting and legal firms of electronic espionage by "Chinese state organizations." These attacks used Trojans customized to defeat the firms' IT security systems and exfiltrate confidential data. In March 2009, the University of Toronto's Munk Center for International Studies exposed a cyber espionage ring that had penetrated more than 1,200 computer systems in 103 countries. Targets included news media, government ministries and embassies, and nongovernmental and international organizations. Dubbed 'Ghostnet' by the investigating team, these computer network exploitations (CNE) used Chinese malware and three of the four control servers were in Chinese provinces.*

These kinds of number show the scope of these operations and the broad kinds of organizations targeted.

Reference: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

Military Power

From: *Information as Power: China's Cyber Power and America's National Security* by Colonel Jason M. Spade:

- *China has repeatedly targeted the United States. In 2004, a CNE exfiltrated terabytes of data from Sandia Laboratories, the National Air and Space Administration, and several U.S. defense contractors. Code-named **Titan Rain**, this CNE routed the data through servers in South Korea, Hong Kong, and Taiwan before sending it to China. In August 2006, a CNE originating from China infiltrated computer systems belonging to Members of Congress and the House Foreign Affairs Committee. Congressman Frank Wolf (R-VA) maintains that "critical and sensitive information about U.S. foreign policy and the work of Congress" was exfiltrated. In October 2006, computer network attacks launched from Chinese servers forced the Commerce Department's Bureau of Industry and Security (BIS) to block Internet access for over a month. BIS replaced hundred computers to expunge their network of all malicious code. Between 2007 and 2009, a CNE exfiltrated data on Lockheed Martin's F-35 fighter program. Forensics found that the intruders searched for data on the plane's design, performance statistics, and electronic systems. Investigators traced the CNE to Chinese Internet protocol addresses used in previous network intrusions.*

Reference: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

National Defense and National Power

From: *Information as Power: China's Cyber Power and America's National Security* by Colonel Jason M. Spade:

- *For national defense and national power, nation-states have developed military capabilities for each of the natural domains: sea power (navies), land power (armies), air power (air and air defense forces), and space power (spacecraft and satellites).*
- *The purpose of these powers is for the nation-state to establish control and exert influence within and through the domains, control and influence being steps toward the state achieving its national goals and objectives.*
- *States create armies to control, defend, and extend their borders; navies to protect their coasts, control sea lanes, and attack others' by sea; air and outer space forces to attack through the sky, defend against like attacks, and conduct observation. Each of these powers is intended to use a domain to the advantage of the state. And each of these powers can support and reinforce the powers dominant in the other domains.*

National Defense and National Power

From: *Information as Power: China's Cyber Power and America's National Security* by Colonel Jason M. Spade:

- *Cyber power is the ability of a nation-state to establish control and exert influence within and through cyberspace, in support of and in conjunction with the other domain-elements of national power.*
- *Attaining cyber power rests on the state's ability to develop the resources to operate in cyberspace. Cyber power as a nation-state capability is no different than land, sea, air, or space power. Instead of tanks, ships, and airplanes, the state needs networked computers, telecommunication infrastructure, programs and software, and people with the requisite skills.*
- *As with the land, sea, air, and space domains, the state can produce effects within cyberspace or into another domain through cyberspace. A cyber attack could corrupt an adversary's logistics database, degrading the adversary's rapid deployment capabilities; bring down an air defense network, enabling an air attack; or jam the signals of a global positioning satellite, interfering with a warship's ability to navigate or target its weapons systems.*

In the description of Cyber Power:

- ***Consider***: How many different ways can a nation-state *'establish control and exert influence within and through cyberspace'*?
- ***Consider***: How has Russia and China used these techniques to exert their influence?

Problem: How do we determine or evaluate the "Cyber" or "Digital" Power of a nation?

Digital Power

The concept of digital power or cyber power can be hard to quantify

- With military power, it is relatively easy to count planes, tanks, and ships – and still relatively easy to compare their capabilities
  - Speed
  - Armaments
  - Range
- However, cyber power is not nearly as straightforward
  - This is especially true since many aspects of cyber power may not be know
  - For example, how many zero-day exploits does a country have in its arsenal?

Over the years there have been many different attempts to quantify this value

The first we will look at is from 2011

Composite Index of National Capabilities (CINC) Score

From: *Information as Power: China's Cyber Power and America's National Security* by Colonel Jason M. Spade (ch 4):

- *The ability to influence, 'power,' is a fundamental concept that underpins international relations theory.*
- *Power is an ambiguous concept. Power in the traditional sense is imagined as a brute force strength that overwhelms a potential adversary. Or as Jeffrey Hart explains, the definition of power contains the common threads of 'control, influence, and legal authority.'*
- *In politics and international relations in particular, there is one primary type of power, the ability to get one's way. This can be linguistically construed as [the] ability for a person to influence others. Simply put, a weak person is forced, whereas a powerful person forces.*

- *To create a single robust measure of cyber power, the next step in the process is to develop an index variable of power. This index variable is similar to the Composite Index of National Capabilities (CINC) score.*

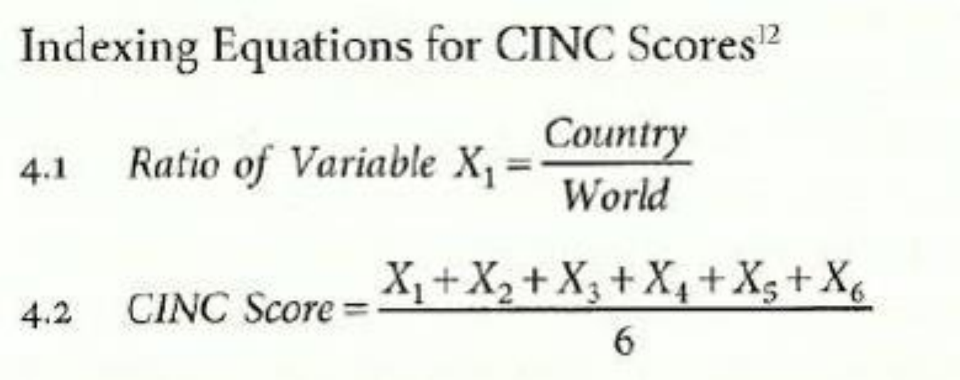
- *J. David Singer and colleagues, the creators of CINC scores, incorporate variables of conventional power ranging from total population to military personnel within a country, create an additive model, and then divide the summation of the power scores by the number of variables. Each of the variables included in their indexed variable is a country to world ratio, used to represent the finite number of resources presently available to engage in conflict.*

Reference: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

CINC Score

The variables for this equation are:

- Military Unit Designation
- Economic and Social Context
- Technological Infrastructure & Industrial Application
- Legal and Regulatory Frameworks
- Military Budget Allocation



Indexing Equations for CINC Scores[12]

4.1 $$\text{Ratio of Variable } X_1 = \frac{\text{Country}}{\text{World}}$$

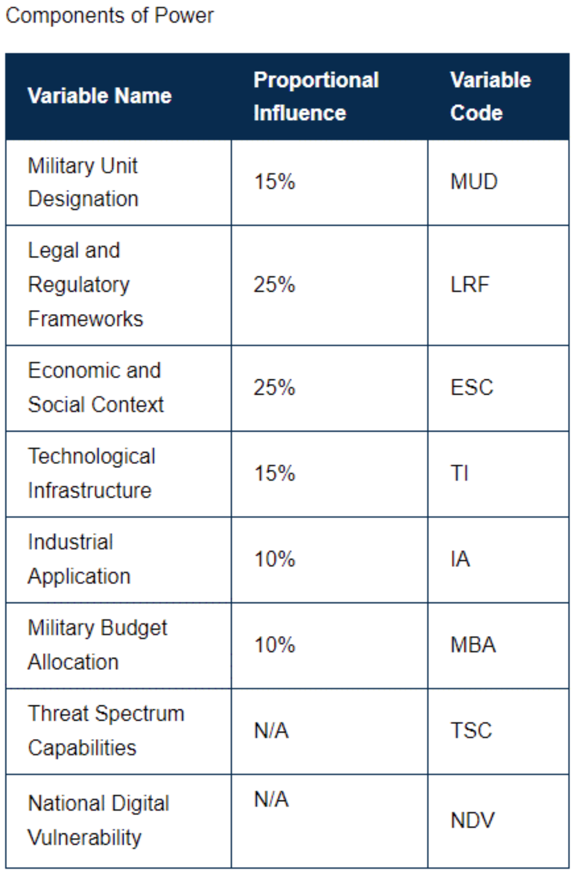
4.2 $$\text{CINC Score} = \frac{X_1 + X_2 + X_3 + X_4 + X_5 + X_6}{6}$$

In addition, there are these factors:

- ***Threat Spectrum Capabilities***
  - *the demonstrated capabilities of a state within cyber offense or defense*
- ***National Digital Vulnerability***
  - *In 1990 Saddam Hussein had an enormous military with nearly half a million active-duty military personnel. If power were to rely on numbers alone, the first Gulf War should not have been won as quickly as it was. The relative power based on aggregate numbers was not such that it should have facilitate a speedy American victory. However, the Iraqi military had strategic vulnerabilities and command and control vulnerabilities that, when exploited, made it difficult for Iraqi commanders to communicate with deployed divisions. This indicates that power is not a pure numbers game even in conventional conflict; in the cyber world it is even less so.*

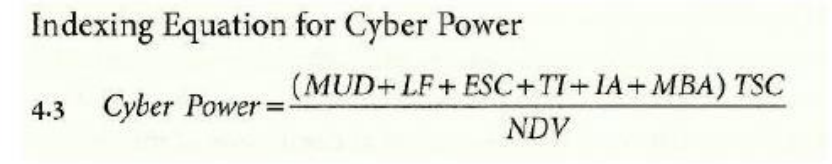
Image and references from: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

CINC Score Variables



Components of Power

Variable Name	Proportional Influence	Variable Code
Military Unit Designation	15%	MUD
Legal and Regulatory Frameworks	25%	LRF
Economic and Social Context	25%	ESC
Technological Infrastructure	15%	TI
Industrial Application	10%	IA
Military Budget Allocation	10%	MBA
Threat Spectrum Capabilities	N/A	TSC
National Digital Vulnerability	N/A	NDV

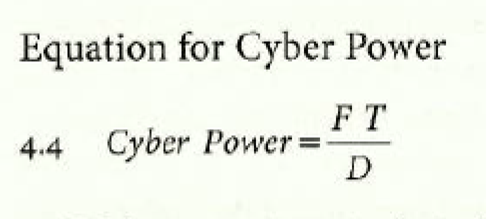


Indexing Equation for Cyber Power

$$4.3 \quad Cyber\ Power = \frac{(MUD + LF + ESC + TI + IA + MBA)\ TSC}{NDV}$$

Images from: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

Cyber Power



Equation for Cyber Power

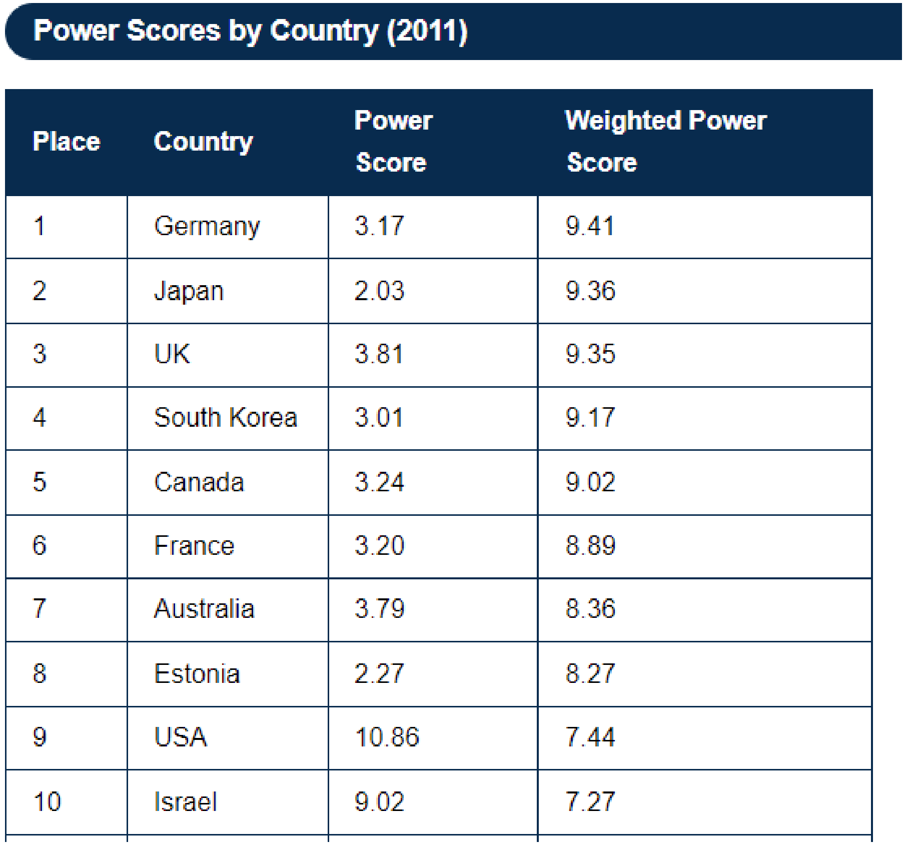
$$4.4 \quad \text{Cyber Power} = \frac{F\ T}{D}$$

F= Theoretical cyber force

T= Demonstrated Threat Spectrum Capability

D= National Digital Dependence Vulnerabilities

(The unweighted power score assumes an equal weight for all variables)



Power Scores by Country (2011)

Place	Country	Power Score	Weighted Power Score
1	Germany	3.17	9.41
2	Japan	2.03	9.36
3	UK	3.81	9.35
4	South Korea	3.01	9.17
5	Canada	3.24	9.02
6	France	3.20	8.89
7	Australia	3.79	8.36
8	Estonia	2.27	8.27
9	USA	10.86	7.44
10	Israel	9.02	7.27

Images from: Colonel Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security*

Cyber Power

Note that in the ranking from 2011, the U.S. ranks behind Estonia in cyber power

Since Estonia does not have a reputation of being a “top tier” cyber power, there are probably a few areas where this could have been improved

Another attempt at ranking Cyber Power was undertaken in 2020 by the Harvard Kennedy School

- They published the *National Cyber Power Index 2020* (NCPI)
- https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf
- The objective of the NCPI was to: *provide a more complete measure of cyber power than existing indices*

Cyber Power

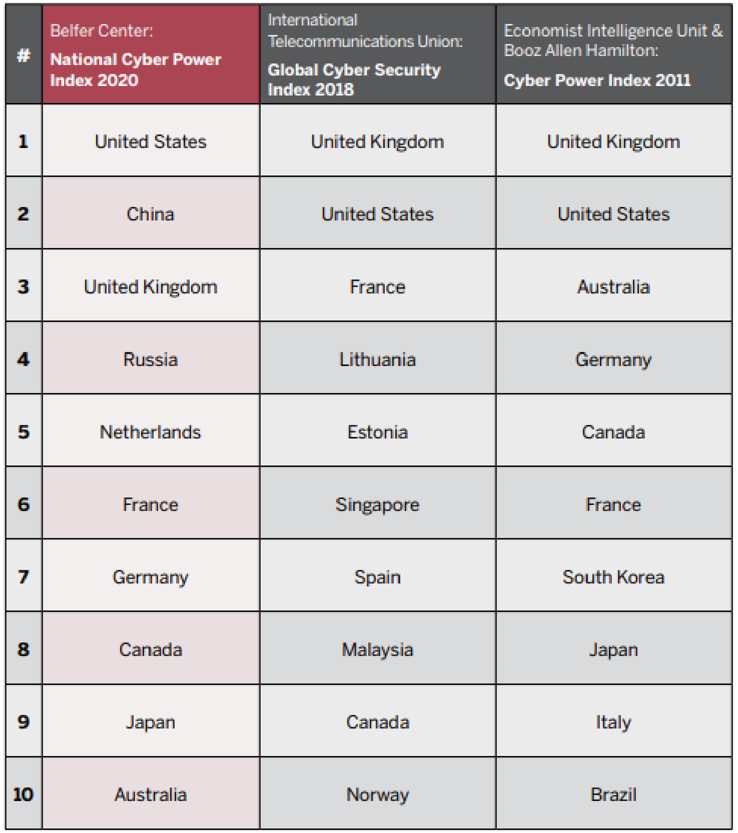
The NCPI provides a comparison of the Top-10 countries according to different indices that have been developed

This included:

- Cyber Power Index 2011
- Global Cyber Security Index 2018
- NCPI

From this table, we can see that there are many disagreements on where countries are regarding their cyber power

- China, Russia, and Estonia only appear on one list each

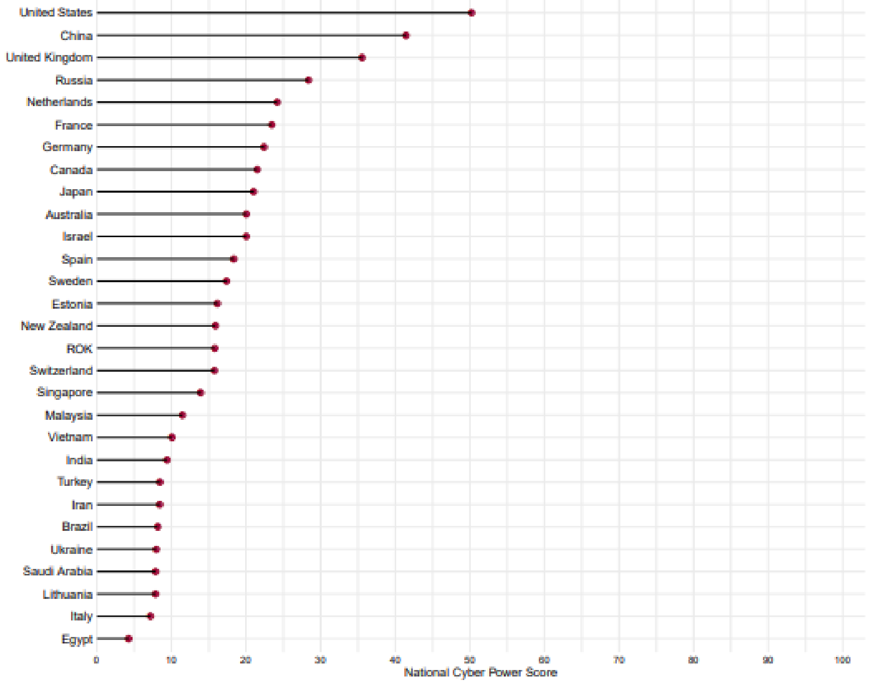


#	Belfer Center: **National Cyber Power Index 2020**	International Telecommunications Union: **Global Cyber Security Index 2018**	Economist Intelligence Unit & Booz Allen Hamilton: **Cyber Power Index 2011**
1	United States	United Kingdom	United Kingdom
2	China	United States	United States
3	United Kingdom	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 from: Harvard Kennedy School, *National Cyber Power Index 2020*

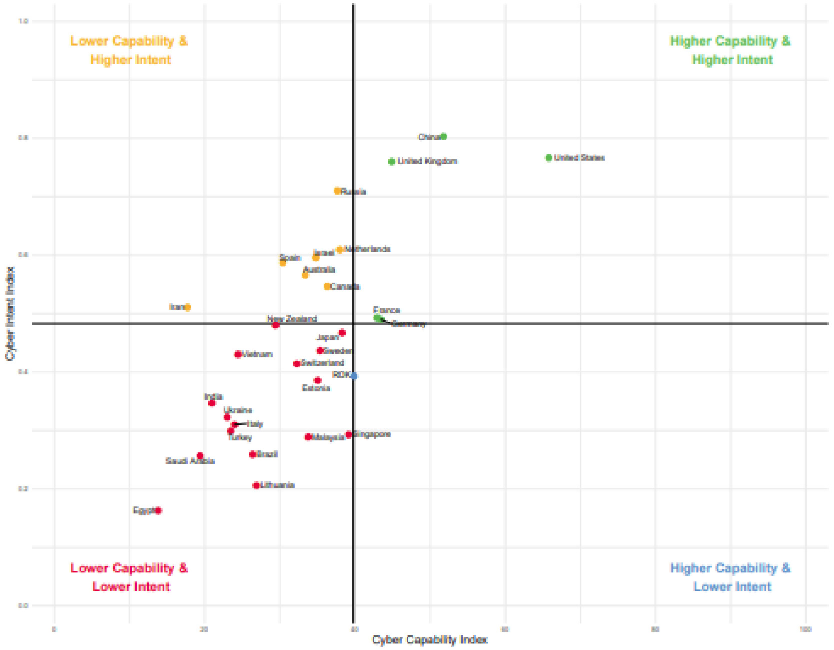
Cyber Power

Graph 1: NCPI 2020: Most Comprehensive Cyber Powers



Belfer Center for Science and International Affairs | Harvard Kennedy School

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



Belfer Center for Science and International Affairs | Harvard Kennedy School

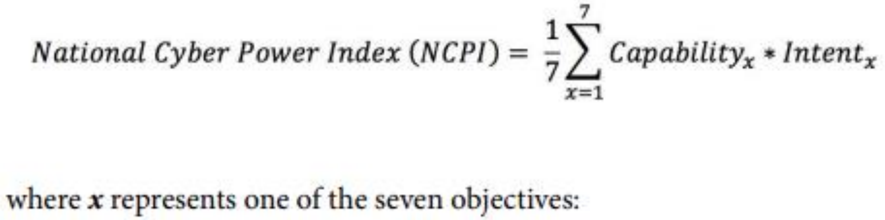
Images from: Harvard Kennedy School, *National Cyber Power Index 2020*

NCPI Index Formula

The NCPI index formula is based on capability and intent of 7 areas.

The 7 areas are:

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



$$\textit{National Cyber Power Index (NCPI)} = \frac{1}{7}\sum_{x=1}^{7} \textit{Capability}_x * \textit{Intent}_x$$

where *x* represents one of the seven objectives:

Images from: Harvard Kennedy School, *National Cyber Power Index 2020*

Some Other Thoughts

From: *Cyberpower and National Security: Policy Recommendations for a Strategic Framework* by FranklinD.Kramer (ch 1):

- https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-01.pdf
- *Daniel Kuehl defines cyberspace as an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructures.*

- As one looks at different elements of cyberpower, the Kuehl definition provides a common base for analysis, but other aspects will tend to be added or emphasized, and the technical definition will be less critical to the development of policy and strategy. By way of examples:
  - cyber ***influence*** activities will include the Internet as well as radio, television, communications such as cell phones, and applications for all
  - cyber ***military activities*** will include network-centric operations, computer network attack and exploitation, geopolitical influence operations, and security
  - cyber ***security*** will include not only technical issues such as viruses and denial-of- service attacks, but also human matters—such as insider deception as well as normal human mistakes—and the problems of governance, both national and international.
- ***Emphasis (bold) are my edits.***

Some Videos Related Cyber Power

Watch: *Cyber War - US vs China: Has the US Already Lost?* by the Covert Cabal

- https://www.youtube.com/watch?v=I1T1WD2B_TA

Watch: *'Every Organization In The U.S. Is At Risk' Of A Russian Cyber Attack, Warns DHS* by MSNBC

- https://www.youtube.com/watch?v=WaaFTtiYnaU

Electromagnetic Pulse (EMP)

On March 29, 2019 President Trump issued Executive Order 13865 *Coordinating National Resilience to Electromagnetic Pulses*.

The purpose of the order is:

- *An electromagnetic pulse (EMP) has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs.*

EO 13865 also defined three key terms:

- *"**Electromagnetic pulse**" is a burst of electromagnetic energy. EMPs have the potential to negatively affect technology systems on Earth and in space.*
- ***A high-altitude EMP** (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of Earth.*
- *A **geomagnetic disturbance** (GMD) is a type of natural EMP driven by a temporary disturbance of Earth's magnetic field resulting from interactions with solar eruptions. Both HEMPs and GMDs can affect large geographic areas.*

It has been known for decades that electromagnetic energy can damage or destroy electronic components and equipment

Additionally, if it occurs at a high altitude some believe it could result in bringing down the U.S. energy grid as well as other critical infrastructures such as telecommunications, emergency services and hospitals

Electromagnetic Pulse (EMP)

Watch: *EMP Risk is 'Not a Sideshow': Why One Cyber Attack Could Wipe Out 90% of US Population* by CBN News

- *https://www.youtube.com/watch?v=1_2EkvEzvr4*

The video is somewhat sensationalist, but still has several interesting points.

The key question to ask is:

- How likely is such an attack on the U.S.?
- Given that a nuclear attack on the U.S. would likely result in a counterstrike against those who launched the attack, how likely is such an event?
- Is this a possibility for a terrorist group?
- What about EMP through natural occurring events?

Another question to ponder is what can we as individuals do about EMP?

Is there something an individual can do to protect their own electronic devices?

Watch*: How To Prepare for an EMP - With PREPSTEADERS.com* by PREPSTEADERS

- https://www.youtube.com/watch?v=BpRHvctF20E

Consider the recommendations in this video

- Are they reasonable?
- If the U.S. were to lose its critical infrastructures, would these precautions have benefit?

Geomagnetic Disturbance

Solar activity can result in geomagnetic storms that can impact electronics and the power grid

Some notable geomagnetic disturbances – and the impact of a solar storm:

- Carrington Event:
  - https://en.wikipedia.org/wiki/Carrington_Event
- March 1989 Geomagnetic Storm (Quebec Event):
  - https://en.wikipedia.org/wiki/March_1989_geomagnetic_storm
- Feb 2022, SpaceX lost 40 of 49 freshly launched satellites from a solar storm:
  - https://www.smithsonianmag.com/smart-news/solar-storm-knocks-40-spacex-satellites-out-of-orbit-180979566/

This is a serious enough threat that NASA, Space Force, and the Air Force monitor space weather

- In serious events, satellites need to shut down to protect their sensitive electronics