The Evolution of Cyberspace – Competing Ideologies of Cybersecurity

Samuel S. Visner

Director, National Cybersecurity Federally Funded Research and Development Center

Adjunct Professor, Cybersecurity Policy, Operations, and Technology, Georgetown University

My viewpoint

My viewpoint is formed by my journey

- From intelligence officer
  - To businessman
    - To government executive
      - To university professor
        - and, back to being a businessman
          - And now, an FFRDC Director

The story I want to tell

- Changes in the global environment
- Changes in what we do in that environment

In other words, we need

to make strategic

decisions in a very different place

First, my day job …
as an FFRDC Director

Mission


Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

What we do

Develop, publish, and reach out to stakeholder and adopters - cybersecurity architectures - comprised of commercial cybersecurity technologies – that can be applied to the "verticals" comprising the United States private sector and critical infrastructures …

- Drive innovation
- Support standards

… in support of US economic competitiveness and security

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Open and transparent

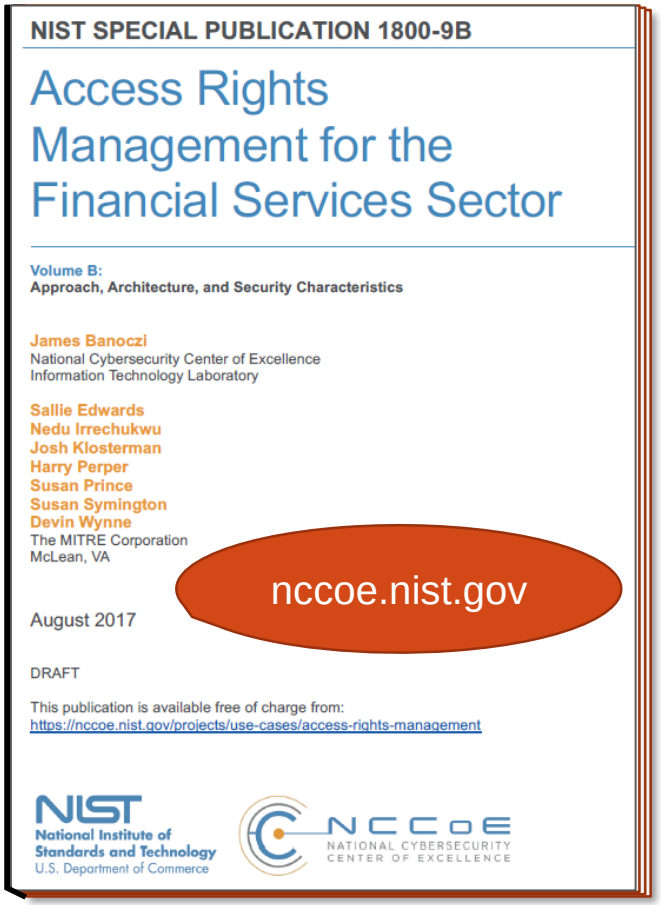
Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

Portfolio

- Attribute Based Access Control (SP 1800-3)
- Consumer/Retail: Multifactor Authentication for e-Commerce (SP 1800-17)
- Data Integrity: Identifying and Protecting
- Data Integrity: Detecting and Responding
- Data Integrity: Recovering (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Email Security (SP 1800-6)
- Energy: Asset Management
- Energy: Identity and Access Management (SP 1800-2)
- Energy: Situational Awareness (SP 1800-7)
- Financial Services: Access Rights Management (SP 1800-9)
- Financial Services: IT Asset Management (SP 1800-5)
- Financial Services: Privileged Account Management (SP 1800-18)
- Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
- Healthcare: Securing Picture Archiving and Communication Systems
- Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
- Hospitality: Securing Property Management Systems
- Mitigating IoT-Based DDoS
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems (NISTIR 8219)
- Mobile Device Security: Cloud and Hybrid Builds (SP 1800-4)
- Mobile Device Security: Enterprise Builds
- Mobile Threat Catalogue
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Mobile Application SSO (SP 1800-13)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Mgmt (SP 1800-16)
- Transportation: Maritime: Oil & Natural Gas
- Trusted Cloud (SP 1800-19)

NIST NCCoE SP 1800 Series

- Practice Guide Publication
- Volume A: Executive Summary
  - High-level overview of the project, including summaries of the challenge, solution, and benefits
- Volume B: Approach, Architecture, and Security Characteristics
  - Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards
- Volume C: How-To Guide
  - Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance



National Cybersecurity Excellence Partnership

The evolution of the global environment

By which I mean

- Cyberspace
- And the societies and cultures affected by cyberspace

Tough questions

- How do we characterize and undertake meaningful analysis in an environment we barely understand?
- How do other countries understand this environment

Let me start by viewing these questions through my current discipline - Cybersecurity

Concepts vary

- For some, cybersecurity is about safeguarding information
- Others take a more expansive view:
  - Safeguarding information systems
  - Safeguarding IT-intensive information infrastructures
- Cybersecurity is viewed by some as gaining the outcome in cyberspace you desire, and not the outcome someone else would impose
- Even more expansive view: cyberspace is a portion of sovereign space – cybersecurity is about governance – cyber in an instrument of state power

In this context

I mean the exercise of influence in cyberspace – as an instrument of national power

Defining Cybersecurity

- Today, we consider cybersecurity as
  - Computer Network Defense
  - Computer Network Exploitation
  - Computer Network Attack
- *What is a "**computer network**"*
- The concept of "computer network" is important to today's concept of cyberspace – in fact, it's core to understanding today's cyberspace

Cybersecurity as a digital concept

- The term "computer network" presupposes that cyberspace lives principally in the digital universe
- Not always true:
  - We have attempted to exploit, disrupt, and attack information systems prior to the digital age
  - Cyberspace can be said to exist whenever we transmit and process information using electro-magnetic energy
- So, why is "cybersecurity" a big deal now?

The scope of cybersecurity

- The scope of cybersecurity is a reflection of the scope of information technology – the changing conception of a 'computer network"
- A progression:
  - Point to point communication devices and connectivity
  - Auxiliary devices (printers, phones, encipherment devices, fax machines, etc.) attached to each end
  - Automated switching systems to route communication
  - Devices to store and process information
  - Networks to handle transactions
  - Databases
  - Data warehouses; advanced analytics
  - More advanced endpoints (tablets, smartphones)
  - Converged devices (data, voice, video, media, social networking)
  - Virtualization and clouds
  - Embedded programmable logical devices
  - Industrial control systems
  - Supervisory control and data acquisition systems
  - The "internet of things"
  - Global cloud – cloud storage on orbit
  - AI
  - IPv6
  - 5G Internet … convergence of 5G, IPv6, AI

What makes these things possible?

- Digital technology (information and signal processing)
- Low cost
- Ubiquity
- Interoperability
- Combination of information-in-motion and information-at-rest
- Other things?

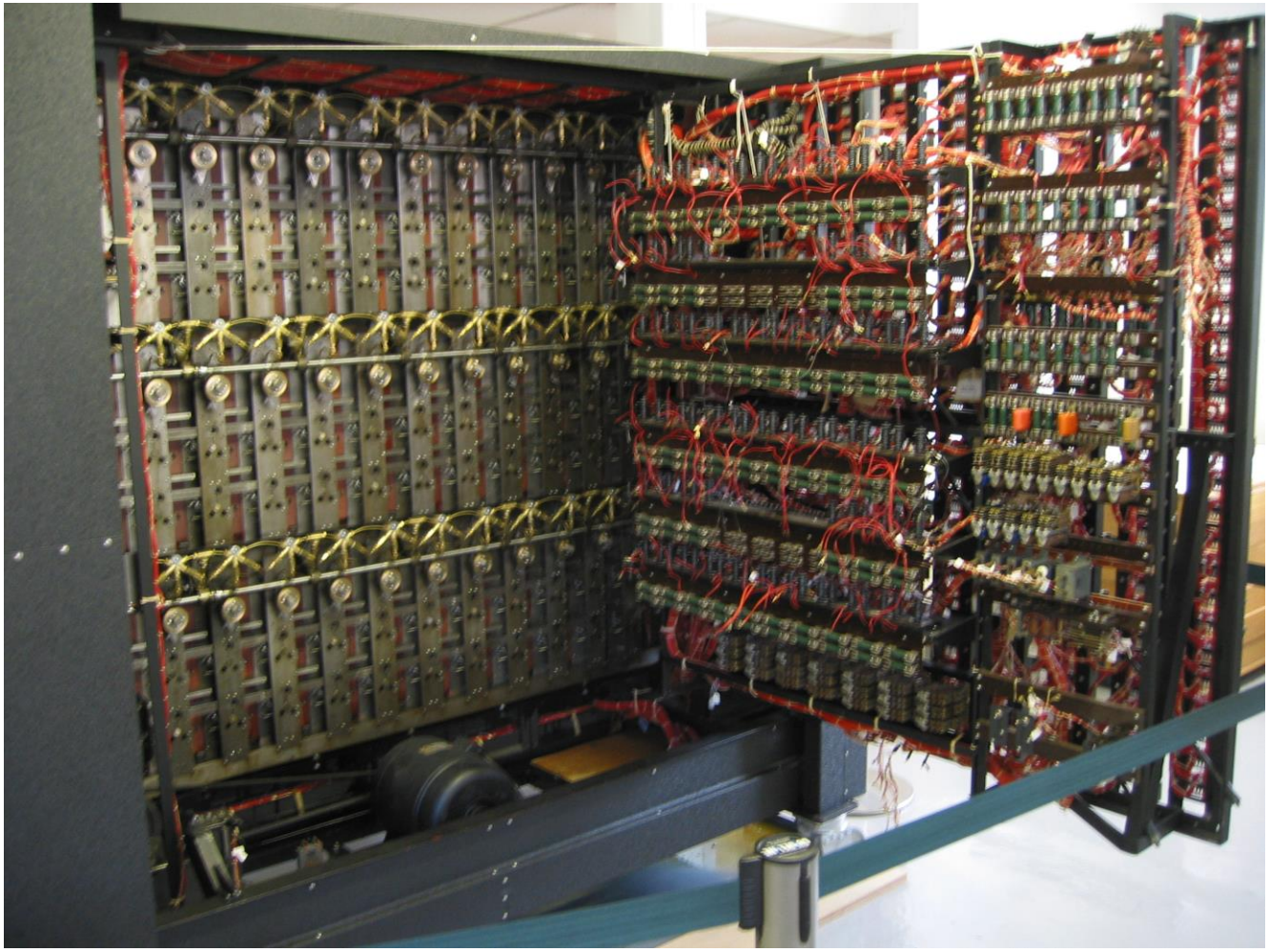
The rise of cybersecurity

- Aspect of cybersecurity have existed for many years
- US Civil War – Communication technology used to coordinate vast campaigns
- WWI efforts to:
  - Encipher communication
  - Intercept communication
  - Decrypt communication
  - Exploit communication
- WWII saw efforts to build integrated information systems

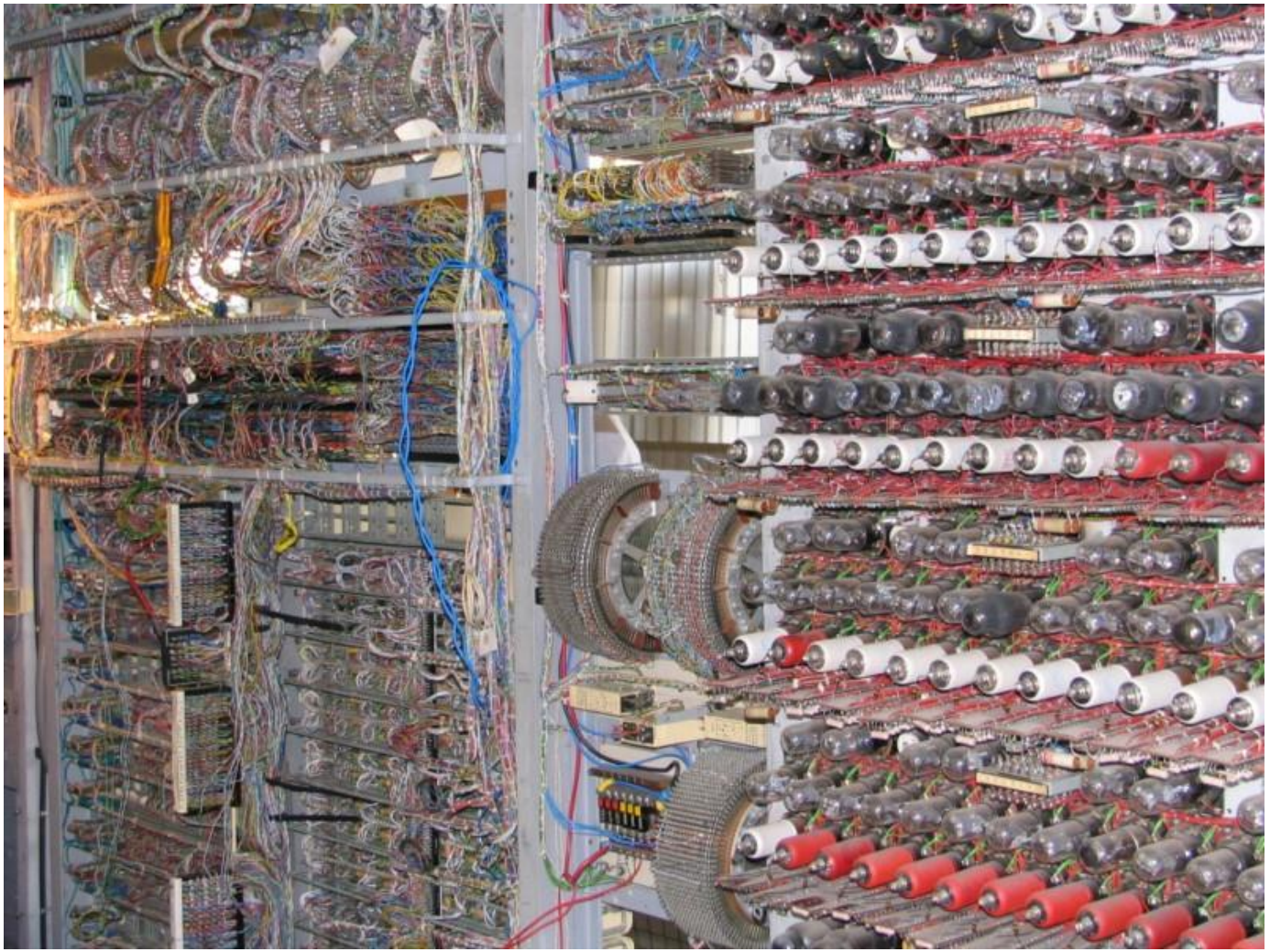
WWII

- Germany relied in its ability to safeguard its communication to achieve military advantage
- Defeating that ability allowed the Allies to in the Battle of the Atlantic
- The exploitation by the US of Japanese communications (and breaking their codes) provided the warning necessary to succeed at Midway
- The course of the Pacific War was changed only six months after Pearl Harbor

Bletchley Park – The Bombe – Performing Turing's Logic Tests



Bletchley Park – Colossus – Breaking the German Leadership Cyphers



Allied Communication Security – SIGSALY – Voice Encipherment for Franklin Roosevelt and Winston Churchill

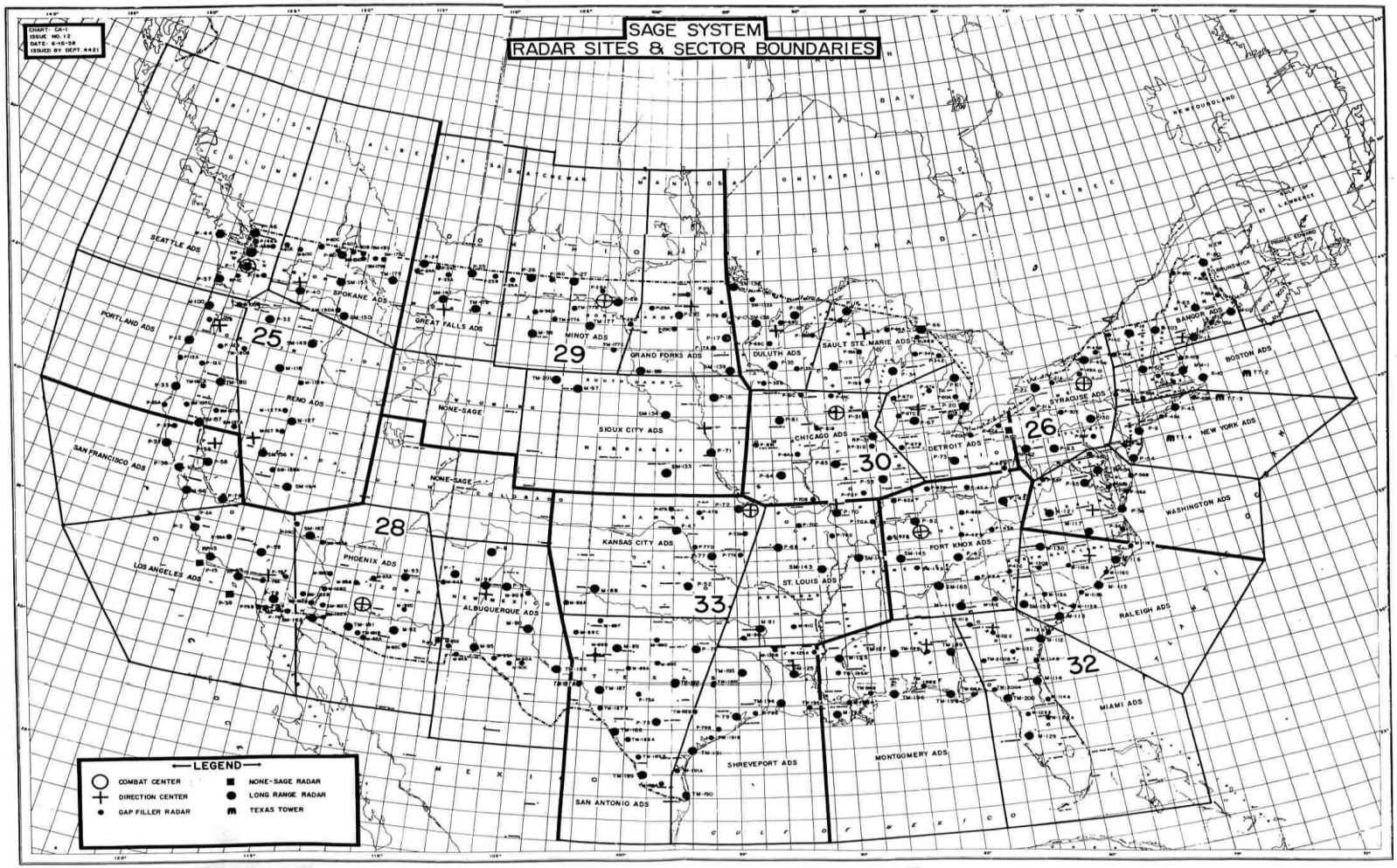
Information was important, but …

- These systems were not digital, cheap, or ubiquitous
- These systems focused on protecting, or compromising "information in motion"
- "Information at rest"
  - Was only beginning to be subject to modern means of analysis used to support operations
  - Was not the subject of electronic exploitation
  - Was not processed using inexpensive and ubiquitous technology

The stage was being set

- The 1950s saw rapid advances in digital information processing
- Digital information processing was tied to large networks creating true cyberspace environments
  - By 1957, the Semi-Automatic Ground Environment (SAGE) was deployed to automate air defense of North America
    - Important – Keeping adversaries from exploiting or disrupting processing
    - Important – using information at rest alongside information in motion (databases, processing, communication)

SAGE - a cyberspace environment along side physical space



We also needed a common format for the transmission of digital information

- Advanced Research Projects Agency Network (ARPANET)
  - Telecommunication Communications Protocol/Internet Protocol (TCP/IP) starts to gain ground
  - By 1969, four nodes connected
  - By 1973, Europe was connected
  - ARPANET is the Internet's progenitor
  - Not "just" communication, but a network that connected systems that processed information at rest

As ARPANET faded and the Internet took over ...

- The Internet spread around the world
- Internet-like architectures were deployed for specific and sensitive environments (DISN, NIPRNet)
- As the sun set on ARPANET, we recall the words of Vint Cerf:

It was the first, and being first, was best,
but now we lay it down to ever rest.
Now pause with me a moment, shed some tears.
For auld lang syne, for love, for years and years
of faithful service, duty done, I weep.
Lay down thy packet, now, O friend, and sleep.

Key Point

- Cyberspace is not "just" an environment in which information is transmitted
- Cyberspace includes the systems that process information
- "Networks" are more than connectivity
- Networks make possible the distributed processing of information

Thus, the transition from "communication" to "computer network," the core of today's global cyberspace environment

The other key point

- As Lenin is reported to have said: "Quantity has a quality all its own."
- While we have used electro-magnetic energy to communicate since the middle of the 1850s, cyberspace, as an environment that mediates and affects almost every aspect of human experience is relatively new
- Cyberspace is certainly a domain
- Consider:
  - Approximately 7.5B people on earth
  - Several tens of millions on the earth's oceans and seas (not at the same time, of course)
  - Almost 1B airline passengers in 2017 (not at the same time, of course)
  - A handful (less than 10) in space at any moment (maybe a few more, if Jeff Bezos and Elon Musk get their way)

The world online: almost 3.9B

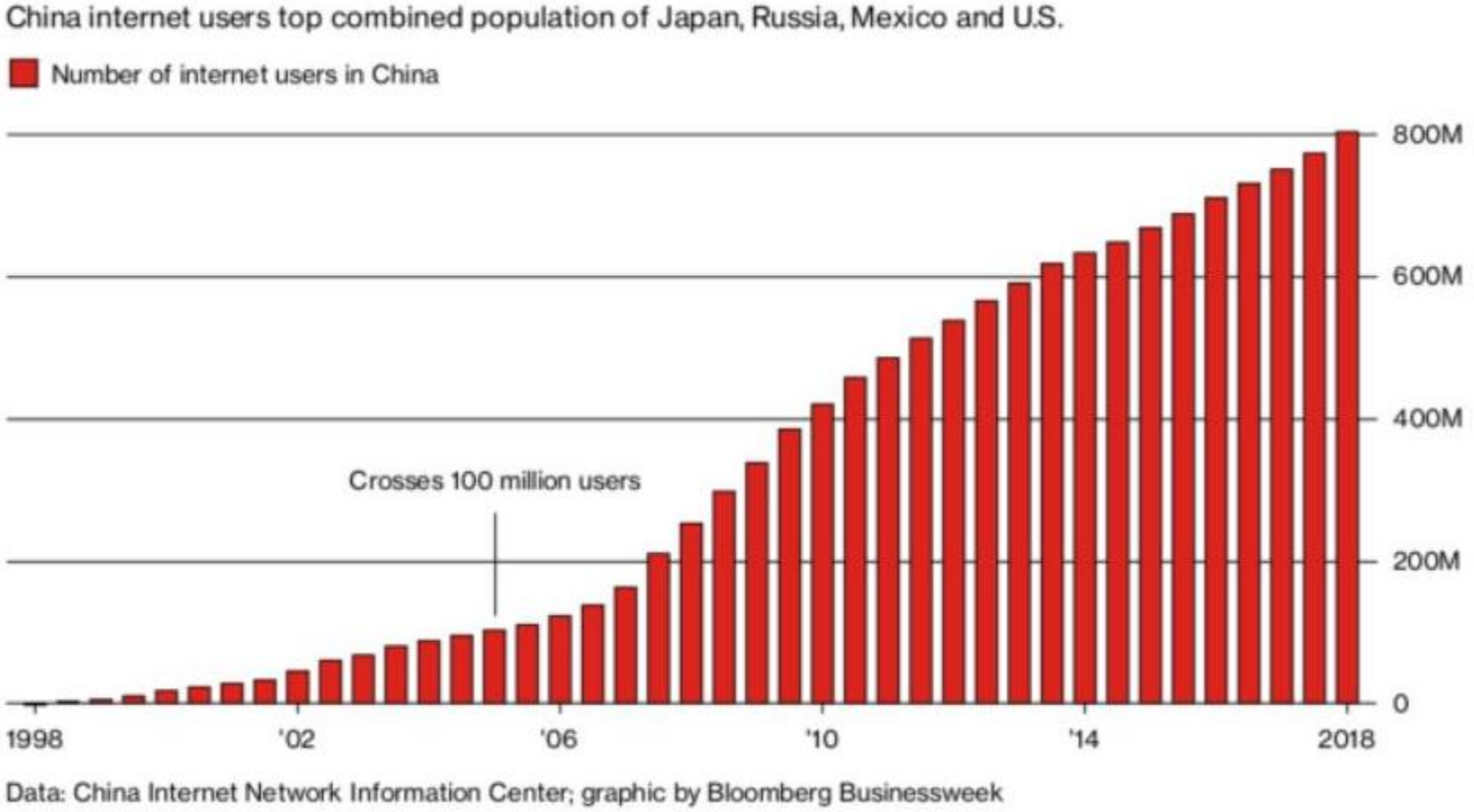
TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - JUNE 30, 2017						
#	Country or Region	Population, 2017 Est.	Internet Users 30 June 2017	Internet Penetration	Growth (*) 2000 - 2017	Facebook 30 June 2017
1	China	1,388,232,693	738,539,792	53.2 %	3,182.4 %	1,800,000
2	India	1,342,512,706	462,124,989	34.4 %	9,142.5 %	241,000,000
3	United States	326,474,013	286,942,362	87.9 %	200.9 %	240,000,000
4	Brazil	211,243,220	139,111,185	65.9 %	2,682.2 %	139,000,000
5	Indonesia	263,510,146	132,700,000	50.4 %	6,535.0 %	126,000,000
6	Japan	126,045,211	118,453,595	94.0 %	151.6 %	26,000,000
7	Russia	143,375,006	109,552,842	76.4 %	3,434.0 %	12,000,000
8	Nigeria	191,835,936	91,598,757	47.7 %	45,699.4 %	16,000,000
9	Mexico	130,222,815	85,000,000	65.3 %	3,033.8 %	85,000,000
10	Bangladesh	164,827,718	73,347,000	44.5 %	73,247.0 %	21,000,000
11	Germany	80,636,124	72,290,285	89.6 %	201.2 %	31,000,000
12	Vietnam	95,414,640	64,000,000	67.1 %	31,900.0 %	64,000,000
13	United Kingdom	65,511,098	62,091,419	94.8 %	303.2 %	44,000,000
14	Philippines	103,796,832	57,607,242	55.5 %	2,780.4 %	69,000,000
15	Thailand	68,297,547	57,000,000	83.5 %	2,378.3 %	57,000,000
16	Iran	80,945,718	56,700,000	70.0 %	22,580.0 %	17,200,000
17	France	64,938,716	56,367,330	86.8 %	563.1 %	33,000,000
18	Turkey	80,417,526	56,000,000	69.6 %	2,700.0 %	56,000,000
19	Italy	59,797,978	51,836,798	86.7 %	292.7 %	30,000,000
20	Korea, South	50,704,971	47,013,649	92.7 %	146.9 %	17,000,000
TOP 20 Countries		5,038,740,614	2,818,277,245	55.9 %	944.1 %	1,326,000,000
Rest of the World		2,480,288,356	1,067,290,374	43.0 %	1,072.2 %	653,703,530
Total World Users		7,519,028,970	3,885,567,619	51.7 %	976.4 %	1,979,703,530

One year later – another ½ billion – penetration rises another 3 ½ percent

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2018 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 30 June 2018	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,199 %	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,704 %	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570 %	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,325 %	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,894 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,066 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics estimates in June 30, 2018. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) The information from this website may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2018, Miniwatts Marketing Group. All rights reserved worldwide.

Velocity of China's on-line growth is phenomenal



What's happening right now?

- IPv4 give us 2^{32} addresses, or 4,294,967,296
- IPv6 gives us (potentially) 2^{128} addresses, or 340,282,366,920,938,463,463,374,607,431,768,211,456 (or approximately 3.4 x10^{38} (i.e., a big number)
- Just about "everything" can be connected
- 5G will provides for
  - Higher speed connection
  - Direct connection of Internet of Things (and IPv6) devices
- 5G deployment is starting – look for more general availability later this year

The World Economic Forum says

"We believe 5G will change the world even more profoundly than 3G and 4G; that it will be as revolutionary as electricity or the automobile, benefitting entire economies and entire societies.

"Developing nations have rivalled or surpassed their industrialized counterparts in benefiting from the deployment of mobile technology, and there's every reason to think 5G will have an even bigger levelling effect than its predecessors.

"Economists estimate the global economic impact of 5G in new goods and services will reach $12 trillion by 2035 as 5G moves mobile technology from connecting people to people and information, towards connecting people to everything."

Back to thinking about the evolution of cybersecurity
Computer Network Defense

- Defending a network from intrusion and damage
- Defending a network from the proliferation of malware
- Defending information from being "exported" from a network without authorization
- Defending information from being altered, or from having its authenticity questioned
- Defending the integrity of the analysis on which we depend
- Defending the integrity of the systems that depend on information

Computer Network Exploitation

- Efforts to infiltrate a network to steal information
- Done without the network owner's knowledge
- Information of many types can be exploited
  - Data
  - Metadata

Computer Network Attack

- Efforts to gain access to a network and information to alter, damage, destroy, or otherwise undermine the integrity of information
- Make it worthless (or worth less) to its owner
- Damage information systems (computer networks); "CNA Sub 1"
- Damage infrastructures that rely on computer networks; "CNA Sub 2"
  - Energy systems
  - Manufacturing systems
  - Transportation systems
  - Other systems in the "Internet of things"

And now

- Weaponized Exploitation – what I call "*Computer Network Influence*" (think of US elections, French elections)

- Big Data Analytics applied to exploitation – what I call "*Computer Network Correlation*" ("What do we *do* with 400 million records?")
- And now … *Computer Network Persistent Surveillance* (using computer networks to observe society - and to govern it)

And now …

- What about electoral systems?
  - Now a "critical infrastructure subsector" (under Government facilities)
- *What about the media* – which affects thinking and behavior?
  - Facebook
  - Twitter
  - "Fake news"
  - "LikeWar"

The new normal

- Computer Network Exploitation = a form of espionage: adjacent to diplomacy
  - Not acknowledged
  - Accepted by the international system– up to a point
- Computer Network Attack = perhaps a form of covert action, i.e., force applied by one state to another, short of a state of war; adjacent to special operations and covert action
  - Not acknowledged
  - Accepted by the international system – up to a point

Tough questions

- Can we develop normative behavior in the international system relating to cybersecurity?
- How do we constrain the behavior of non-state actors, given low barriers to entry?
- What do we do about state-sponsored, non-state actors (e.g., “cyber patriots?”)

Let's talk about sovereignty

- For the US and western democracies, cyberspace is a global commons
  - We operate in cyberspace
  - We defend cyberspace – personal information, intellectual property, business, research, infrastructure, our military operations
  - We even fight in cyberspace (DoD Cyber Strategy, 2015)
  - We don't "own" cyberspace
    - Think of the Law of the Sea – in this instance, we control cyber assets in our physical space
    - Beyond territorial waters – universal jurisdiction
- For China, Russia, and possibly others:
  - Cyberspace is territory in which the government has sovereign prerogatives
  - Cybersecurity is about defending the state's legitimacy and the government's sovereign prerogatives

Implications

- If cyberspace is sovereign territory, can a state acquire more of it?
- Can cyberspace be governed and controlled?
- How can it be acquired? By force?
- We know Russia tried to influence US elections
- If Russia was successful in influencing US elections by "seizing" cyberspace, was that a military victory? What has Russia gained? What have we lost?

What do other countries think?

- Draft treaty circulated as early as 2009 by China, Russia, and several other states (Appendix 2, Section 5) extends the definition of cybersecurity as follows:

  " Distribution of information harmful to political and social and economic systems, to the spiritual, moral and cultural circle of other states. Source of threat are the states, the organizations, the group of persons or the individual using information infrastructure for distribution of information harmful to political and social and economic systems, the spiritual, moral and cultural circle of other states. Its signs are emergence and replication in electronic (radio and television) and other mass media, on the Internet and other networks of information exchange of information: distorting idea of political system, the social order, foreign and domestic policy, important political and public processes in the state, cultural, moral and cultural values of its population; propagandizing idea of terrorism, separatism and extremism; kindling international, interracial and interconfessional hostility."

What do other countries think?

- Researchers at the People's Liberation Army (PLA) Academy of Military Sciences, Ye Zheng and Zhao Baoxian, have called for the international com-munity to establish "cyber territory" and defend "cyber sovereignty
- Min Jiang, Assistant Professor of Communication at the University of North Carolina, notes that the discussion at the World Conference on International Telecommunications (WCIT-12) of the International Tele-communications Union (ITU) focused in part on the Internet governance divide between, on the one hand, liberal democracies such as the United States, and on the other hand, authoritarian regimes such as China, Russia, and many Arab nations. Jiang describes China's approach, as well as that of other states in the "Global South," as a "state-centric model of Internet governance," one "that that favors the authority of a nation-state over its netizen."

Another way of thinking

- Dr. Joseph Nye, former Chairman of the National Intelligence Council, describes the world as a three-level chessboard
  - *First Level*: IT is applied the *military power*; the US remains the dominant (though not unchallenged) leader; barriers to entry are high
  - *Second Level*: IT is used to enable a multi-polar *world of commerce; barriers to entry are surmountable by middle-range powers*
  - *Third Level:* IT connects *parties, constituencies, religious affiliates, social groups, ideologues* – No one is dominant; barriers to entry are low
- Nye argues that US policy- and decision-makers need to understand the use of power at the second and third levels
- He notes: Conventional wisdom has always held that the state with the largest military prevails, but in an information age it may also be the state -- or nonstate actor -- *with the best story that wins*."

The stakes are rising

- Electoral politics:
  - Can they be influenced?
  - How they been influenced?
- Cyber exploits and attacks from state sponsors and well equipped cybercriminals
  - How do enterprises defend themselves?
  - How do individuals?
- More important – How do we model and understand our national interests in this new environment?
- How do we defend and advance them?

How do other countries act?

Mark Gagliotti writes in Foreign Policy" that Russia is combatting the west:

"(b)y turning its democratic norms and institutions against itself, by opening existing fault lines, and by taking every opportunity to neutralize the West. This is a textbook case of what George Kennan called political war: "the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures … and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."

"The point is this: If the subversion is not the prelude to war, but the war itself, this changes our understanding of the threat. The point is this: If the subversion is not the prelude to war, but the war itself, this changes our understanding of the threat, and therefore our best responses. Maintaining serious armed forces as a deterrent is still necessary, but perhaps more emphasis ought to go on counterintelligence and media literacy, on fighting corruption (always a boon for the political warriors) and healing the social divisions the Russians gleefully exploit."

Where do we undertake "counterintelligence and media literacy," if not in cyberspace

Foreign Policy, March 5, 2018

Has the time come to redefine cybersecurity?

- Perhaps in a world in which defense, exploitation, attack, correlation, and influence are practiced simultaneously …
- … to achieve governance, control, and sovereignty …
- … we should redefine cybersecurity as …
- … *Computer Network Control = achieving the outcomes we desire in cyberspace as a component of national power*

So, an alarming vision

- For us, cyberspace is an domain of electromagnetic energy
- For China and others, cyberspace is a domain of human behavior
- We secure information; others govern human behavior; for others, cyberspace is sovereign space – like land
- As China moves forward:
  - A sovereign ideology
  - Economics and investment- One Belt/One Road
  - Global deployment of 5G, AI, and persistent surveillance
  - Belt/Road becomes a new "digital silk road"
  - If China owns the digital infrastructure along the Belt/Road, is China wresting sovereignty from other countries?
  - What would happen if that model were extended to our doorstep?

Which takes us to ...

- Cybersecurity as an aspect of "great power competition"
- Great powers using cybersecurity to influence and undermine competitors and adversaries
- Great powers vying for influence in cyberspace as a domain of human governance

Parting shots

- How do we understand the changing global environment?
- What instruments of power are available?
- What normative behavior constrains us – or our adversaries?
- How do we decide what outcomes to achieve, and how to achieve them?

That is your challenge

MITRE

GEORGETOWN UNIVERSITY

Thank you for your kind attention.

svisner@mitre.org

ssv@georgetown.edu

CHESAPEAKE LARGE-SCALE ANALYTICS CONFERENCE