Great Decisions 2019

Class #6: Cyber Conflict & Geopolitics

Joe Coffey
joecoffey@outlook.com

Website Coffeynotes.com

1. Cyber conflict - foreign interference in elections, industrial & infrastructure sabotage
2. Russia accused of interfering in 2016 elections
3. US & China use cyberspace as policy tool
4. Cyber involves new means of warfare
5. Is US prepared to respond to such threats?

The way to get a cat to eat hot pepper is to grind it up, place it on its fur and let him lick it off of his own accord. - Mao

1

Problem: US dependence on vulnerable Internet

- Everything increasingly dependent upon Internet
- Internet has progressively greater foreign cyber risks and new vulnerabilities to catastrophic cyber incidents
- Increased Internet-connected devices and reliance on global supply chains expands risk
- Challenge: Benefit from Internet while minimizing vulnerability to malicious cyber threats, lessen their consequences and effectively respond

2

2

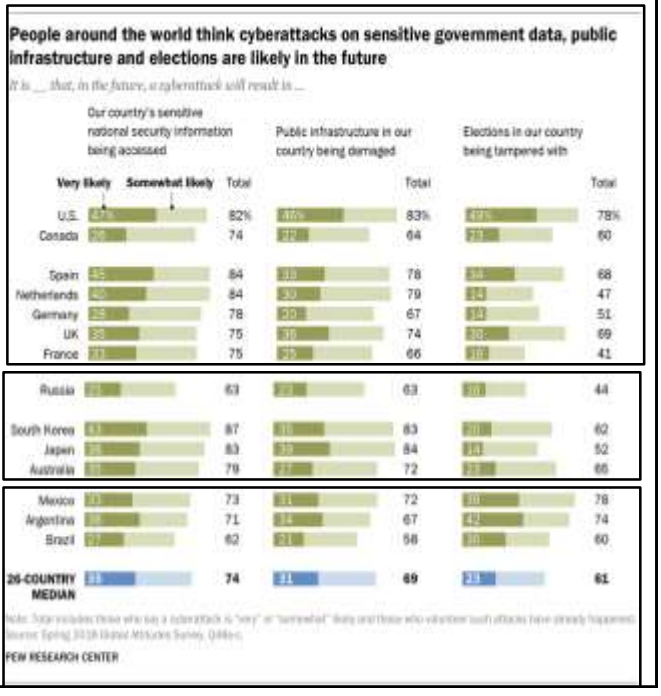
What is Cyber Warfare?

- Use or targeting computers and networks for espionage and sabotage
- 100 countries engage in cyberwarfare
- Using Internet as a weapon to target financial markets, computer systems and utilities
- Defensive cyber policies include prevention, reduce vulnerability and minimize damage and recovery time
- Multiple threats - supporting traditional warfare such as tampering with air defenses, spreading espionage and propaganda, and disruption

3

3

Cyberattacks in deemed 80% likely in US and others worldwide



4

Why Cyber warfare? From bricks to chips

- Virtually everything is linked to computer networks
- How wealth is generated & stored: changed from tangible to intangible goods – Intellectual Property (IP)
- This makes them vulnerable to cyber piracy

***Uber**, the world's largest taxi company, owns no vehicles. **Facebook**, the world's most popular media owner, creates no content. **Alibaba**, the most valuable retailer, has no inventory. And **Airbnb**, the world's largest accommodation provider, owns no real estate. The battle is for the customer interface.*

techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface

5

5

Intellectual property (IP) theft $1 tril. business

- Digital age prompted expanded cyber theft
- China hacks into every major US company
- China signed agreement with US that wouldn't support theft - but may now be greater than ever
- China now using better less detectable techniques
- Many US companies can't protect themselves

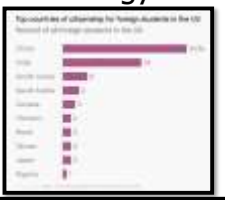
Notes on Video 6 "Made in China," Great Decisions 2019

6

6

US Intellectual Property vulnerable

- US firms must store data inside China which makes them more vulnerable to IP theft
- China limits US firms unless joint venture which enables access to technology
- Many Chinese arrested for theft in US – e.g. snatching corn plants to access advanced genetic technology
- Many US firms go along with China's rules hoping they can out-innovate, but can they?
- Concern about Chinese graduate students in US learning and taking home cutting-edge technology

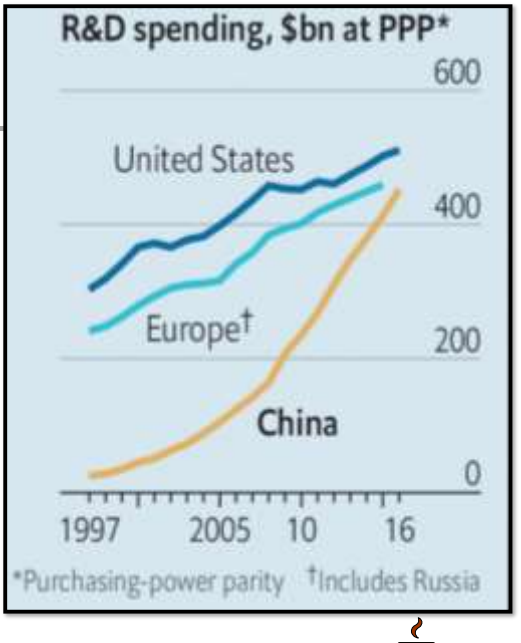


7

7

China is catching up with US in R&D

- **Impressive achievements:** landing on far side of moon, gene-editing …
- **But can China excel?** Can scientific research directed from top down to serve a one-party system excel?
- Perhaps but unproven



economist.com/science-and-technology/2019/01/12/can-china-become-a-scientific-superpower?

8

8

US - an early user of cyber technology

- Cyber - million times more efficient at data collection than traditional spying
- In 2010, Stuxnet "worm" a malicious software used to destroy Iran's centrifuges
- Edward Snowden CIA employee leaked highly classified information from National Security Agency (NSA) in 2013
- Revealed US global surveillance with cooperation of telecommunication companies and European governments
- US tapped phones of leaders such as Angela Merkel of Germany and prompted others to accelerate cyberwarfare

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

9

9

Cyber attacks on US worsen

- US targeted by Iranian and Chinese hackers
- Dozens of corporations & agencies hit, prompting a emergency order by Homeland Security
- Iranian attacks coincide with a renewed Chinese target of Boeing, GE Aviation and T-Mobile
- Cyber allows adversaries to attack below threshold of armed attack or war
- Hackers from China and Iran pile on to Russia's, US's top hacker of trade and military secrets and sowing mayhem

Nicole Perlroth, Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies, NY Times, Feb. 18, 2019

10

10

Cyber provides asymmetric advantage to potential attackers

- Offensive cyber capabilities provide an asymmetric advantage to potential attackers who may not have capacity—or desire—to launch a conventional attack against US
- Cyber tools can provide states like China, Iran, North Korea, and Russia ability to seriously disrupt the U.S. economy, government, and services.
- Cyberattack on U.S. critical infrastructure and networks is a top threat

https://www.cfr.org/blog/top-conflicts-watch-2019-cyberattack>

11

11

Russian strategy: attack infrastructure & democracy

- Russia used cyber warfare to increase anti-US, anti-EU and anti-NATO sentiment in Europe
- Encouraged nationalist movements in Spain, Italy & UK
- May be able to "flip switch on US power grid"
- Electrical infrastructure around world may be infested with Russian malware
- Used cyber to intimidate countries - Estonia & Georgia
- Russia has better means to protect itself than an open society such as the US against cyber warfare

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

12

12

Cybersecurity charges against Huawei

- $ 100 bil. Chinese multinational telecommunications and consumer electronics firm - 180,000 employees
- Founded by former engineer in China's Army in 1987
- Huawei networks reach 1/3rd world's population
- Overtook Apple in 2018 as 2nd in smartphones
- Faces allegations in US that equipment may contain backdoors to enable surveillance by China
- In Dec 2018, Huawei's exec arrested in Canada on US charges of fraud, obstruction of justice, and theft of trade secrets

https://en.wikipedia.org/wiki/Huawei

13

13

How to protect US firms & intellectual property?

- Most don't want a US great firewall, but more aggressive action and technical support
- 2018 Foreign Investment Risk Review Modernization Act (FIRRMA) - which can block or revise transactions in defense and high tech
- Needed to ensure foreigners don't steal our technology or compromise our security
- But must balance trade-off: benefit from foreign investments when they create jobs in US vs. compete with US firms and more easily access technology

Notes on Video 6 "Made in China," Great Decisions 2019

14

14

Trump's cybersecurity strategy

- More aggressive against hacking and overseas sources of cyber attacks
- Increasing participation by private companies
- "Name and shame" more cyber criminals & countries
- Decrypt communications of suspected criminals
- Space Force - enhance protection of "space assets" such as global positioning, navigation and timing; intelligence gathering, surveillance and reconnaissance; satellite communications; and weather monitoring

www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html>

15

15

Chinese use cyber capabilities to undermine US primacy

- Cyber policy based on deception and reflexive control
- Since can't overcome US technology directly, take advantage of US freedom of information & openness
- Verizon reported 96% of state-affiliated cyber espionage attempts against its IP originated in China
- FBI: "Two kinds of big companies - those who have been hacked by Chinese and those who don't know it"

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

16

16

Biggest single threat facing US may be cyber threat

- May allow China and Russia, increasingly working together, to challenge US led liberal world order
- Cyber meddling in social media and elections along with Iran's increasing cyber espionage, posing increasing danger to US
- Americans generally see the US global leadership as permanent and not threatened
- But new technologies in past (e.g. warships, trains, and nuclear weapons have caused geopolitical pivots

China's cyber warfare persists

- May have 100,000 hackers
- Spends billions on "thought control" public relations techniques for infiltrating and fostering self-censorship
  - For example, Hollywood profits depend upon revenue from China, so self-censor to avoid banning
- Trump placed tariffs on Chinese imports in retaliation of cyber theft – may have provoked more cyber theft

Cyber could aid Russia and China reshape world order

- China-Russia Axis: Most aligned since 1950s
- 1950s – Soviets sent equipment & 1000s to assist China industrialize and nuclear weaponize
- Rivals after Sino-Soviet split in 1961 - danger of war
- Enmity lessened after Mao's 1976 death, but relations poor until fall of Soviet Union in 1991
- In 2001, closer relations, implicitly a military treaty
- Both hold grievances and suspicion against US and seek to reshape world order
- China is Russia's largest market, bilateral trade $100 bil.

The New Beijing-Moscow Axis, by Yaroslav Trofimov, Feb. 1, 2019, *WSJ*

19

Despite Russia's limitations, Putin has re-established it as global player

- Putin has played a weak hand well - exploited US ambivalence of post-9/11 presence in Middle East
- Trump's focus on Iran has given opening to Putin
- Russia is only big foreign power that talks to all of region's key actors: Iran, Sunni Arab states, Israel, Turkey, Kurds, Palestinian Authority, Hamas, Hezbollah and Syria
- Russia's growing regional influence is a Putin achievement, alongside stronger ties with Xi Jinping's China, despite Russian GDP only 1/8th China's

Source: Vladimir Putin's Big Push Into the Middle East, By Angela Stent, *WSJ*, Feb. 15, 2019

20

20

China: Existential threat to US and the World Order

- China has been positive for world affairs - lowered cost of living and expanded prosperity worldwide
- But things have changed:
  1) Instead of liberalizing, has become more repressive
  2) Focuses on dominating high-tech industries - not competing but stealing US IP ~ $600 bil.
  3) Trying to infiltrate tech economy & penetrate our society
  4) No longer just economic but existential - geopolitical
- **China won't democratize, liberalize, and join free democratic world – rather is an existential threat to liberal international order**

Source: David Brooks, How China Brings Us Together - An existential threat for the 21st century, NY Times, Feb. 14, 2019, www.nytimes.com/2019/02/14/opinion/china-economy.html>

21

21

Summary: Cyber Conflict & Geopolitics

- Everything interconnected and rise of intangible assets makes cyber attacks more possible and powerful
- Cyber is changing nature of 21st century warfare
- Cyber attacks may give autocrats advantage over US & EU democracies
- West holds technological lead, for now, and therefore has more to be stole by cyberattacks
- China's economic success and Putin's cleverness is shrinking US image
- Unlikely China and Russia will democratize or Internet to decline, so greatest threat of US may be cyber

22

22

China and U.S are battling for tech supremacy

- US worries Chinese equipment infiltrating for espionage and theft of intellectual property
- China is shifting from being world's factory for low-cost goods to technology such as Huawei become a major player in telecoms undercutting rivals like Cisco and Nokia
- Congress proposing to ban sale of chips and components to Huawei and other Chinese telecom companies
- Chinese encouraged to buy local - hurting Apple's revenue
- China's investments in U.S. fell to $5 bil. in 2018 from $46 bil. in 2016
- Risk US and China tech conflict could undermine tech ecosystem along with all its innovation

Source: The Cold War in Tech Is Real and Investors Can't Ignore It, By Reshma Kapadia, *Barron's*, February 22, 2019

23

23

Intensified cyber to weaken democracies

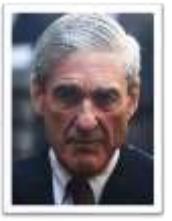
- Iran hackers implicated in breach of Australia's Parliament and political parties
- Global espionage against US and allies likely retaliation for Trump's withdrawal from Iran nuclear agreement
- US indicted Iranian group for hacking universities, companies, & governments
- Experts warn that China, Iran, North Korea and Russia are intensifying cyber operations to weaken Western democracies

Source: Australia's Parliament hacked this month, *WSJ*, By Rob Taylor, Feb. 21, 2019

24

24

Political import of social media?



- Facebook is vulnerable to bad actors and lacks safeguards on personal information of users
- Tech giants profit by selling information on their users
- Political influence of cyber in elections debatable: some think Russians stole election from Hillary, whereas others believe she was bad candidate and needed no help from Russians to lose an election
- It's argued that social media rarely change users' political opinions but intensify those already held

Source: Politics: The Government We 'Like' By Barton Swaim, WSJ, Feb. 22, 2019

25

25

Kissinger on cyber technology and world order

- Internet has outstripped strategy or doctrine - the very definition of state authority is becoming ambiguous
- It's easier to mount a cyber attack than to defend against it - possibly encouraging an offensive bias
- Cyberspace has become strategically indispensable- and the next war may begin in cyberspace and raises the question whether "virtual" aggression warrants "kinetic" response
- Internet focuses on information whose overabundance may paradoxically inhibit the acquisition of knowledge
- We must be concerned about information-especially who controls it
- We risk being driven less by reasoned arguments than by what catches the mood of the moment
- Despite the limitless possibilities of new technologies, we must recognize the dangers of societies driven by mass consensus and deprived of context and foresight in a historical context

Source: Henry Kissinger, *World Order*, 2014, Chapter 9

26

26

Highlights of Video #6: "Made in China"

- China aiming to be powerhouse by 2049 equal to US
- Restricts US market access and technology
- Requires US to joint venture enabling easier access to technology
- Agreed not to support IP theft, but now greatest ever
- New 2018 US law enables blocking or revising transactions of US defense and high-tech firms
- Difficult to balance security vs economic interests: Foreign investments create jobs in US vs. compete with US firms
- China complains unfairly targeted, but doesn't reciprocate and millions of students take home high tech expertise

27

27

What is cyber warfare?

- Virtually everything in economy and national security are linked to computer networks
- How wealth is generated and stored has changed-in the 1980s 80% of industrial wealth was stored in tangible assets today 80% is stored in intangible goods-trade secrets and intellectual property
- This makes them vulnerable to cyber piracy
- A sophisticated and strong cyber attack has a potential to damage the US
- Such information crosses borders and incentivizes states to manipulate them

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

28

28

US - an early user of cyber technology

- Cyber arrested for knowledge much, maybe a milli
more efficient at data collection than traditional sp
- In 2010, this.net "worm" a malicious software was used to attack and destroy Iran's centrifuges at its nuclear facility
- China has hacked into Google in order to track down dissidents
- Infamous case of Edward Snowden former CIA employee who leaked highly classified information from National Security Agency (NSA) in 2013 that revealed global surveillance programs with cooperation of telecommunication companies and European governments that US tapped phones of leaders such as Angela Merkel of Germany

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

29

29

Rushes criminal connections for cyber espionage in US

Time Magazine runner-up 2018 perso

- Cyber use by US gave wake-up call to China, Russia, Iran and others who are now also using it to attack the US
- Russia used cyber against Estonia in 2007 and Georgia in 2008 and after 2011 stepped up its cyber attacks
- In 2014 Russia's military doctrine rewritten to include cyber exploiting of popular protests and decreasing civilian patriotism
- Russia developed cyber for "systematic manipulation of public opinion through social media" to spread pro-Russian posts, to foment dissension and undermine legitimacy
- Robert Mueller investigation of Russian influence is still unfolding

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

30

30

Cyber warfare can attack electrical infrastructure around the world

- Russia has used cyber warfare to increase anti-US and anti-EU and anti-NATO sentiment in Europe
- Has also encouraged nationalist movements in Spain, Italy, and UK Brexit boat
- Also uses cyber to affect US infrastructure
- Presumably has capability to "flip the switch on the US power grid"
- It's thought most electrical infrastructure around the world is infested with Russian malware
- Russia has better means to protect itself than an open society such as the US against cyber warfare

Chinese cyber warfare strategy

- Use information and cyber capabilities to push back against US primacy
- Adopt a cyber policy based on deception and reflexive control
- Since China cannot overcome US technology directly, can dominate the information arena by taking advantage of US freedom of information and openness
- Verizon reported that 96% of Allstate-affiliated cyber espionage attempts against its IP originated in China
- FBI indicated that there are "two kinds of big companies-those who have been hacked by the Chinese and those who don't

The way to get a cat to eat hot pepper is to grind it up, place it on its fur and let him lick it off of his own accord. - Mao

Cyber warfare may trigger geopolitical conflict

- May allow China and Russia, who are increasingly working together, to challenge the US led liberal world order
- Cyber operations using social media and meddling in election campaigns, along with Iran's increasing cyber espionage, posing increasing danger to US government and business
- Some say that the biggest single threat facing US economy is the cyber threat
- Americans generally see the US global leadership as permanent and not threatened, especially by such indirect attacks as cyber warfare
- But new technologies in the past, such as warships, trains, and nuclear weapons have caused geopolitical pivots in the past

China's cyber warfare persists

- China targets cyber warfare on commercial IP to foster his continued growth and may have upwards of 100,000 hackers
- China also spends billions on "thought control" public relations techniques for infiltrating and fostering self-censorship
- For example, Hollywood film profits and TV shows depend upon revenue from China and self-censor to avoid censorship or rejection
- Despite the Obama-Xi Jinping 2015 agreement to limit official cyber warfare, its current level is greater than ever
- Trump placed tariffs on some Chinese imports in retaliation of cyber theft
- Cyber theft economic espionage costs range from $200-$600 billion per year

conclusions

- Cyber warfare is likely to continue and escalate.
- US is especially vulnerable in China, Russia and Iran use it to attack US economy and institutions to steal valuable technology and sow discord

Notes on Topic 6 "Cyber conflict and geopolitics" by Richard B Andres, Great Decisions 2019

35

35

China aggressively planning to become a global powerhouse

- US criticizes China because of its theft of intellectual property rights, cyber spying, forced joint-ventures and trade barriers
- Since 2015 China has an aggressive made in China 2025 plan
- It's a strategic plan for industrial policy and economic development
- Longer-term plans:
  - 2035- Plan to become comparable to South Korea's economy
  - 2049- Plan to become equal to Germany or US economy
- China wants to avoid the middle income trap – stagnation like other middle-income countries
- Labor costs are rising and they recognize continued rapid growth is not possible

Notes on Video 6 "Made in China," Great Decisions 2019

36

36

China has made technological progress

- China's most impressive innovation is in the financial sector – e.g. mobile payments
- They also capture (way too?) much data from the users
- Advanced in telecommunication and healthcare- especially advanced in genetic testing
- Genetic testing programs have attracted foreign investors and questionable ethics as they have lax regulations

37

Can Chinese companies innovate?

- China's government has a heavy hand which normally would limit innovation
- They also target industries - although such efforts in Japan and elsewhere have been of dubious value
- They are also emphasizing artificial intelligence
- Despite great strides - many are skeptical because difficult to innovate in a communist society and they still lag behind US

38

China may successfully innovate and we shouldn't ignore

- Since 1980s, China has restricted access of US companies to their market
- US exports to China are $120 bil. per year – our 4th largest export market, but would be much bigger if had freer access
- China limits the use of US technology
- China requires our firm's to store all their data inside China - which forces companies that wish to do business in China to do so but it makes them vulnerable to theft of intellectual property

Difficult decision-access their large market for lose intellectual property

- China limits firms unless they form a joint venture with a Chinese firm which enables them to access the technology
- Many foreign companies went along because they thought they could innovate faster than China and keep ahead-but now that is questionable
- But how to stop that? The difficulty in limiting the transfer because companies want to do business in China
- And the US government hasn't sufficiently defended or protected US companies
- There have been arrests for out right theft by China in the US- for example pulling up corn plants out of fields to access advanced genetic technology

Theft is big business: Obama estimated cyber theft worldwide at $1 trillion

- China isn't the only country to steal intellectual property - US in early years stole textile and other technology from Britain
- But digital age has prompted an expanded cyber theft
- China hacks into every major US company
- China's President Xi Jinping eventually signed an agreement that China's government wouldn't support theft-but it took a long time to get him to do it
- Afterwards cyber theft initially declined, but may now be greater than it was
- China simply started using better less detectable techniques
- Use very advanced techniques from which many US companies can't protect themselves

41

How to protect US firms and intellectual property?

- Most firms don't want US government to create a great firewall, but they want more aggressive action and technical support
- In 2018 Congress passed the United States Foreign Investment Review Act -which can block or revise investment transactions
- Especially in defense and in high-tech firms
- Such protection is needed to ensure they don't steal our technology or compromise our security
- But it's difficult to balance security with economic interests
- There's a trade-off: We benefit from foreign investments when they create jobs in US, but compete with US firms and more easily access technology

42

China feels unfairly targeted

- China complains they are unfairly targeted and are investment laws lacked transparency
- But what to do when China does not reciprocate
- China can sell all their products in US, but US is limited in China
- Was substantial worry when China bought the IBM PC division
- There is also concern about the millions of Chinese graduate students in the US-much of the IT graduate programs are dominated by Chinese graduate students
- They obviously are learning the cutting-edge technology

Conclusion:

- China will continue to pursue their leadership
- But how can US protect our security and proprietary technology
- How can we level the playing field of trade with China
- There's an old Chinese saying: when winds of change blows, some build walls while some build wind mills