Negative: TTSA - bad idea

By “Coach Vance” Trefethen

Case Summary: The AFF plan passes a bill currently pending in Congress but not yet enacted, the Transatlantic Telecommunications Security Act. It provides foreign aid to central and east European countries to upgrade their telecom networks and help them get away from Chinese 5G technology.

Negative: TTSA 3

DEFINITION 3

Definition of what TTSA does 3

INHERENCY 3

1. Status Quo risk management is all we need 3

There are "many" cybersecurity threats, not just China, to be concerned about. Best response is simply apply today's cybersecurity risk management policies 3

2. The "Clean Network Initiative" already solved 4

The US "Clean Network Initiative" in 2019-2020 already did the AFF plan in Central and Eastern Europe 4

3. Western Europe solved with the Prague Proposals and the "EU Toolbox" 4

Western Europe secured its networks from threats, achieving the same results with less confrontation with China 4

4. New European Union security standards and funding 5

European Union has budgeted billions of euros to fund 5G upgrades 5

EU is setting 5G security standards 5

It's working: 13 EU countries already have upgraded their 5G security 5

HARMS / SIGNIFICANCE 5

1. Not a harm until someone gets harmed 5

None of the "harms" in the Affirmative case describe anyone being harmed 5

2. A/T "China influence in Eastern Europe" 6

China and Russia have made themselves unpopular in Europe and hardened opposition against them 6

2. No threat: Chinese 5G will fail on its own 6

Chinese officials admit: China 5G is an expensive failure 6

Huawei 5G founder admits: It's exaggerated, no one needs it 6

3. No threat: Chinese telecom technology isn't dangerous 7

China is less likely to put security risks into telecom technology when we have close commercial ties 7

No secret "back door" surveillance hidden in Huawei telecom software 7

No actual threats have been found - it's just anti-China political posturing 7

SOLVENCY 7

1. More study needed 7

Conventional wisdom about China/5G requires a lot more study, or else we will make policy mistakes 7

Chaotic results may happen if we don't stop and study this more now, before enacting new policies 8

There's no reliable way to know to what degree we should restrict Chinese technology right now. We should preserve our options, study it and move slowly 8

Must have a larger strategy first before enacting specific policies 8

2. Cutting off China won't work 9

Cutting off China/5G for security protection won't work. Instead, we should engage with China but manage the risks 9

3. Can't solve for security risk 9

Singling out any specific telecom system is useless: Hackers can get into any system regardless of country of origin 9

DISADVANTAGES 9

1. Harms US economy 9

Suppressing Chinese technology backfires: 1) Harms US industry 2) Accelerates China's technological independence 9

Suppressing Chinese telecom technology ends up harming US high-tech companies in the long run 10

2. Increased risk of war over Taiwan 10

Link: Strangling Chinese telecom technology increases risk of China invasion of Taiwan 10

Backup Link: China threatens to invade Taiwan because they believe it's already theirs, not a separate country like Russia/Ukraine 10

Backup Link: Mainland China seriously wants to reunify with Taiwan, by force if necessary 10

Brink: US & China must reduce tensions now to avoid a potentially disastrous instability 11

Brink: US / China tensions are increasing and coming to the brink of war 11

Impact: Global economic collapse and nuclear war with China 11

Impact: US/China conflict over Taiwan would escalate and nuclear war is possible 11

Backup: Biden says US will go to war with China over Taiwan 12

3. Distracts us from bigger threats 12

Focus on Chinese network technology risks gives a false sense of security and distracts us from bigger risks 12

Impacts of the bigger risks outweigh Chinese tech threats right now. More important to focus on the bigger threats 12

4. China retaliates 13

Link: US efforts to block Chinese technology will likely trigger retaliation 13

Link: Retaliation spirals and escalates. The US retaliates for Chinese retaliation, which then retaliates for that… 13

Impacts: Multiple ways Chinese retaliation would harm the US economy or educational institutions 13

Negative: TTSA

DEFINITION

Definition of what TTSA does

Dave Nyczepir 2021 (journalist) 21 May 2021 " Lawmakers reintroduce bill to finance 5G projects in 22 European countries" (accessed 13 Nov 2022) https://www.fedscoop.com/house-5g-project-bill-europe/

Under the [Transatlantic Telecommunications Security Act](https://kaptur.house.gov/sites/kaptur.house.gov/files/documents/Kaptur%20117%20TTSA%20Bill%2021.pdf), the U.S. Development Finance Corporation would work with relevant agencies improve the resilience of vulnerable telecommunications networks by providing early- and late-stage project support and replacing potentially compromised equipment.  
**END QUOTE. THEY GO ON LATER IN THE ARTICLE WRITING QUOTE:**

If made law, the act would require the [State Department](https://www.fedscoop.com/tag/state-department) to work with DFC [Development Finance Corporation] and the U.S. Trade and Development Agency to identify 5G projects worth financing. Eligible projects would improve 5G networks with new hardware or software, provide market transparency, avoid or replace potentially compromised equipment, and increase telecom integration in the target region.

INHERENCY

1. Status Quo risk management is all we need

There are "many" cybersecurity threats, not just China, to be concerned about. Best response is simply apply today's cybersecurity risk management policies

Prof. Peter Cowhey and Prof. Susan Shirk 2021. (Prof. Shirk is chair of the 21stCentury China Center at the University of California, San Diego, where Prof. Cowhey is dean of the School of Global Policy and Strategy. Both are members of the Working Group on Science and Technology in U.S.-China Relations) 9 Jan 2021 WALL STREET JOURNAL (accessed 18 Sept 2021) The Danger of Exaggerating China’s Technological Prowess https://china.ucsd.edu/\_files/opinion\_jan2021\_wsj\_shirk-cowhey.pdf

The 5G Internet of Things will connect tens of thousands of suppliers of devices and pieces of software with massive rivers of data flowing across national borders. China will be a major security problem, but only one of many. Think of the challenge posed by the 5G Internet of Things as a massively scaled-up version of the cybersecurity threats that pervade networked computing today. As such, 5G security will need to follow today’s cybersecurity template of carefully designed risk management.

2. The "Clean Network Initiative" already solved

The US "Clean Network Initiative" in 2019-2020 already did the AFF plan in Central and Eastern Europe

Dr. Karsten Friis & Olav Lysne 2021 (Friis - Senior Research Fellow and Head of the Security and Defence Research Group at the Norwegian Institute of International Affairs; PhD from Univ of Groningen. Olav Lysne is Director of Simula Metropolitan, and Professor of Communication Systems at the Oslo Metropolitan Univ., Norway. He headed the national commission on digital vulnerabilities in 2014/2015 and later the commission that evaluated the use of lawful interception of Internet traffic crossing the national borders of Norway) "Huawei, 5G and Security: Technological Limitations and Political Responses" 3 Oct 2021 (accessed 18 Sept 2022) https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680

In addition to diplomatic tools, the aforementioned Clean Network initiative was elevated by the State Department to an international collaboration network, with a number of countries, telecoms companies and suppliers throughout the world listed as participants. In this context, in 2019 and 2020 the US State Department initiated a series of ‘Joint Declarations on 5G Security’ with allies in Eastern and Central Europe. All NATO countries in this part of Europe, except Hungary, signed such agreements (LRT English, 2020; Republic of Slovenia, [2020](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0037); Reuters, [2020b](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0040); [Romania Insider, 2020](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0045); US Department of State, [2020b](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0058), [2020c](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0059), [2020d](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0060); US Embassy in Estonia, [2019](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0063); White House, [2019](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0065)). Furthermore, in the western Balkans, North Macedonia signed a similar declaration, Kosovo signed a Memorandum of Understanding, and in 2020 Albania stated its intention to join the Clean Network initiative (Taylor, [2020](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0051); US Department of State, [2020e](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0061), [2020f](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0062)). Serbia also made a number of pledges related to 5G (Ruge and Vladisavlej, 2020).

3. Western Europe solved with the Prague Proposals and the "EU Toolbox"

Western Europe secured its networks from threats, achieving the same results with less confrontation with China

Dr. Karsten Friis & Olav Lysne 2021 (Friis - Senior Research Fellow and Head of the Security and Defence Research Group at the Norwegian Institute of International Affairs; PhD from Univ of Groningen. Olav Lysne is Director of Simula Metropolitan, and Professor of Communication Systems at the Oslo Metropolitan Univ., Norway. He headed the national commission on digital vulnerabilities in 2014/2015 and later the commission that evaluated the use of lawful interception of Internet traffic crossing the national borders of Norway) "Huawei, 5G and Security: Technological Limitations and Political Responses" 3 Oct 2021 (accessed 18 Sept 2022) https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680

In October 2019, the EU published a report assessing cybersecurity risks in 5G networks (NIS Cooperation Group, [2019](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0030)). It stated that state actors represent the most significant threat and that several EU members had identified ‘certain non-EU countries’ as a particular threat to their national interests. Thus, China is not mentioned in words but, quite clearly, this can be read between the lines. Furthermore, the report emphasized diversification — in that one should not become dependent on only one supplier — to be resistant to errors and disturbances. Then, in January 2020, the European Commission published a so-called ‘toolbox’, the purpose of which was to identify some common measures that could reduce the most severe digital threats to 5G networks (NIS Cooperation Group, [2020](https://onlinelibrary.wiley.com/doi/full/10.1111/dech.12680#dech12680-bib-0031)). China is not mentioned here either, and the toolbox includes all kinds of risks, not just government intrusion. Nevertheless, it states that governments can impose restrictions and exclude suppliers they consider to be a risk to critical functions. Importantly, these are only recommendations, and although the EU member states should report the implementation of the recommendations in the toolbox, this is still voluntary. Thus, the various EU initiatives helped the countries implement adequate security in the new 5G networks but left it to each country how they would handle China and Huawei. However, most seem to have chosen an approach similar to that of the EU; neither countries nor vendors are mentioned explicitly in 5G regulation, but the Chinese company could still be excluded entirely or partially based on security assessments and the need for diversification. The aforementioned East European joint declarations with the US were therefore in line with both the Prague Proposals and the EU toolbox, but these documents may have assisted the Europeans in finding a less confrontational approach towards China. In short, 5G was securitized, but China and Huawei were not.

4. New European Union security standards and funding

European Union has budgeted billions of euros to fund 5G upgrades

European Court of Auditors 2022 (agency of the European Union) 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved (accessed 13 Nov 2022) https://www.eca.europa.eu/Lists/ECADocuments/SR22\_03/SR\_Security-5G-networks\_EN.pdf

During the 2014-2020 period, the EU supported 5G development with over €4 billion, both directly from the EU budget and through the European Investment Bank (EIB) financing. The EU budget funded projects related exclusively to research, while the EIB supported both research and deployment. The EIB has been the biggest provider of EU financing for 5G related projects. As of August 2021, it provided loans for a total of €2.5 billion for nine 5G projects in five Member States. Furthermore, around €1.9 billion was made available from the EU budget for the 2014-2020 period.

EU is setting 5G security standards

European Court of Auditors 2022 (agency of the European Union) 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved (accessed 13 Nov 2022) https://www.eca.europa.eu/Lists/ECADocuments/SR22\_03/SR\_Security-5G-networks\_EN.pdf

In January 2020, the NIS Cooperation Group adopted an EU toolbox on 5G cybersecurity, which specifies a number of strategic, technical and support measures to deal with 5G security networks threats and identifies the relevant actors for each of these measures. This toolbox, endorsed by the Commission and the European Council, was adopted only nine months after the European Parliament and the Council had raised their concerns about 5G security for the first time. More recently, the EU toolbox on 5G cybersecurity has been mentioned in the new European Strategy to boost smart, clean and secure links in digital systems across the world, as a tool to guide investments in digital infrastructure. The soft law approach put in place by the Commission contributed to putting into motion rapidly measures to deal with security threats also at EU level and to facilitate Member States’ cooperation on this crossborder topic.

It's working: 13 EU countries already have upgraded their 5G security

European Court of Auditors 2022 (agency of the European Union) 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved (accessed 13 Nov 2022) https://www.eca.europa.eu/Lists/ECADocuments/SR22\_03/SR\_Security-5G-networks\_EN.pdf

The toolbox has been developed to avoid fragmentation and promote consistency in the internal market. The criteria in the toolbox offer an operational framework that is useful for assessing the risk profile of suppliers in a coordinated manner across all Member States. It also allowed the Commission to react swiftly to emerging 5G security concerns, together with Member States. At the same time, it remains the national authorities’ responsibility to apply these criteria when assessing the risks related to specific suppliers. By October 2021, taking account of this framework, 13 Member States have enacted or amended legislation on 5G security (see paragraph 75 and Figure 6).

HARMS / SIGNIFICANCE

1. Not a harm until someone gets harmed

None of the "harms" in the Affirmative case describe anyone being harmed

1) "Huawei gives info to Chinese intel services" - so what? Maybe this is a good thing because they can fight terrorism better. If they disclose that my grandmother and I talked about her apple pie recipe, so what? Until the Affirmative tells us what info is being disclosed and whose life is affected or harmed by it, this isn't a harm.

2) "China is an increasing threat to 5G" - so what? What's the threat? Who gets harmed by it? If the threat comes true and completely happens… until there is evidence describing dollars lost, human rights lost, lives lost, or some other impact to someone, this isn't a harm. It's not a harm until someone gets harmed.

2. A/T "China influence in Eastern Europe"

China and Russia have made themselves unpopular in Europe and hardened opposition against them

Dr. Stephen Blank 2021 (PhD; Senior Fellow at the American Foreign Policy Council. Former member of the U.S. Army War College faculty) 25 Aug 2021 " Europe’s Threat Assessments of Russia and China" <https://theasanforum.org/europes-threat-assessments-of-russia-and-china/> (accessed 20 Aug 2022)

The European Round Table for Industry, a trade lobby comprised of almost 60 CEOs and chairpersons of major Europe-based multinationals, has just called on EU leaders to push for better business terms with China and not turn away due to US pressure, despite the fact that China will almost certainly not improve terms for foreign business.This attests to the efficacy of Sino-Russian pressure in achieving the decoupling of Europe from the US. Fortunately for the West, China’s “Wolf Warriors” and Russia’s aggression have hardened opposition to their demands in most European capitals, revealing growing European disaffection with both states, even as the divisions are there for a more supple diplomacy to exploit.

2. No threat: Chinese 5G will fail on its own

Chinese officials admit: China 5G is an expensive failure

John Xie 2020 (journalist) 10 Oct 2020 (accessed 18 Sept 2022) Voice of America News "Chinese 5G Not Living Up to Its Hype" https://www.voanews.com/a/east-asia-pacific\_voa-news-china\_chinese-5g-not-living-its-hype/6196962.html

Another former official warned in a recent speech that China’s 5G push could become a failed investment. "The existing 5G technology is very immature, hundreds of billions of investment have been deployed, and the operating cost is extremely high, no application scenarios can be found, and it is difficult to digest the cost in the future," former finance minister Lou Jiwei reportedly warned in a recent speech last month. "It is difficult for ordinary consumers and industry users to see the long-term benefits and rewards of 5G," a white paper titled "The 2020 China 5G Economic Report" released by China Academy of Information and Communications Technology said.

Huawei 5G founder admits: It's exaggerated, no one needs it

John Xie 2020 (journalist) 10 Oct 2020 (accessed 18 Sept 2022) Voice of America News "Chinese 5G Not Living Up to Its Hype" https://www.voanews.com/a/east-asia-pacific\_voa-news-china\_chinese-5g-not-living-its-hype/6196962.html

With all the expectations and the investment, 5G is “actually exaggerated,” and it is not something that the societies need anyway, according to the man who leads a company that dominates the technology. "In fact, human societies do not have an urgent need for 5G," said Huawei's founder and CEO, Ren Zhengfei, "What people need now is broadband, and the main content of 5G is not broadband."

3. No threat: Chinese telecom technology isn't dangerous

China is less likely to put security risks into telecom technology when we have close commercial ties

Scott Kennedy 2020 (senior adviser and Trustee Chair in Chinese Business and Economics at the Center for Strategic and International Studies) 27 July 2020 "Washington’s China Policy Has Lost Its Wei" (accessed 18 Sept 2022) https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

The United States’ openness to global talent, including from China, to work in the U.S. high-tech community has facilitated the country’s innovation enterprise in both commercial markets and military applications in absolute terms and relative to China. Hundreds of thousands of Chinese students have obtained advanced degrees in U.S. universities; the [great majority of them](https://macropolo.org/digital-projects/the-global-ai-talent-tracker/) remain and help the United States maintain its advantage. In addition, having Huawei and other Chinese firms integrated into U.S.-led ecosystems is not just smart business, it also makes the United States safer. China is less likely to make radical advancements or place backdoors in its silicon when its products are rooted in our foundational technologies. And because of close commercial ties, the United States has greater visibility into the progress China does make.

No secret "back door" surveillance hidden in Huawei telecom software

Associated Press 2019. (journalist Frank Bajak) 28 Feb 2019 (accessed 19 Sept 2022) "Experts: US anti-Huawei campaign likely exaggerated" https://apnews.com/article/74070ddc51ef475b9e7af0cec35d4cf6

One of the most common U.S. fears — that Huawei might install software “backdoors” in its equipment that Chinese intelligence could use to tap into eavesdrop on or interrupt data transmissions -- strikes many experts as highly unlikely. Priscilla Moriuchi, who retired from the U.S. National Security Agency in 2017 after running its Far East operations, said the risk of Huawei backdoors is “almost zero because of the chance that it would be discovered,” thus exposing Huawei’s complicity. Moriuchi, now an analyst at the U.S. cybersecurity firm Recorded Future, said that she and other NSA employees were tasked with searching for Huawei hardware and software backdoors created by Chinese intelligence, but never found any.

No actual threats have been found - it's just anti-China political posturing

Associated Press 2019. (journalist Frank Bajak) 28 Feb 2019 (accessed 19 Sept 2022) "Experts: US anti-Huawei campaign likely exaggerated" https://apnews.com/article/74070ddc51ef475b9e7af0cec35d4cf6

The U.S. has provided no evidence of China planting espionage backdoors in Huawei equipment despite a [2012 congressional report](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf) that led the U.S. government and top domestic wireless carriers to ban it and other Chinese manufacturers from their networks. “The backdrop for this is essentially the rise of China as a tech power in a variety of domains” said Paul Triolo, tech lead [at the Eurasia Group](https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g) risk analysis consultancy. Now, he said, “there is a big campaign to paint Huawei as an irresponsible actor.”

SOLVENCY

1. More study needed

Conventional wisdom about China/5G requires a lot more study, or else we will make policy mistakes

Prof. Peter Cowhey and Prof. Susan Shirk 2021. (Prof. Shirk is chair of the 21stCentury China Center at the University of California, San Diego, where Prof. Cowhey is dean of the School of Global Policy and Strategy. Both are members of the Working Group on Science and Technology in U.S.-China Relations) 9 Jan 2021 WALL STREET JOURNAL (accessed 18 Sept 2021) The Danger of  Exaggerating China’s  Technological Prowess https://china.ucsd.edu/\_files/opinion\_jan2021\_wsj\_shirk-cowhey.pdf

The conventional wisdom about China’s supposed advantages in AI and 5G shows how easy it is for incomplete understanding of technologies to lead to misjudgments and policy mistakes. Balancing economic and security considerations requires considerable knowledge of specific technologies—not just a current snapshot but also a sense of how the fundamentals will shape their evolution. We believe that the most effective U.S. policies will pair openness to China with scrupulous efforts to manage the risks posed by specific technologies.

Chaotic results may happen if we don't stop and study this more now, before enacting new policies

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 U.S.-CHINA TECHNOLOGICAL “DECOUPLING” A STRATEGY AND POLICY FRAMEWORK (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

The U.S. technology base—foundational to national well-being and power—is thoroughly enmeshed with China in a larger, globe-spanning technological web. Cutting many strands of this web to reweave them into new patterns will be daunting and dangerous. Without a clear strategy, the U.S. government risks doing too little or—more likely—too much to curb technological interdependence with China. In particular, Washington may accidentally set in motion a chaotic, runaway decoupling that it cannot predict or control. Sharper thinking and more informed debates are needed to develop a coherent, durable strategy.

There's no reliable way to know to what degree we should restrict Chinese technology right now. We should preserve our options, study it and move slowly

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 "Choosing a Strategy" (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

The very existence of a heated debate among restrictionists, cooperationists, and centrists is itself an argument for the careful incrementalism that centrists espouse.  We are still in the early years of a radically new phase in U.S.-China relations, and we are only at the cusp of far-reaching global transformations promised by AI and other emerging technologies. These coming changes, while undoubtedly significant, remain difficult for present-day observers to assess. How will China’s strategic intentions and technological capabilities change as the country further develops? How will cross-border data flows, new energy tech, or quantum computing reshape the global economy and security environment? How will countries of the world (and multinational companies) align themselves in a more fractured geo-technological landscape? How will the familiar costs and benefits of U.S.-China technological interdependence shift in the coming decades? There is simply no reliable way to answer these questions today. Policymakers should therefore play for time—preserving and expanding American options while the future comes into sharper focus.

Must have a larger strategy first before enacting specific policies

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 U.S.-CHINA TECHNOLOGICAL “DECOUPLING” A STRATEGY AND POLICY FRAMEWORK (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

A U.S. strategy for decoupling should envision the kind of technology relationship that America hopes to have with China, provide a rationale for this vision, and explain how it can be made into reality. A sound strategy would start with a multidimensional assessment of U.S.-China tech ties and their wide-ranging effects on diverse American interests. In fact, a strategy for technological decoupling should consider more than just tech-specific or China-specific concerns. It should be rooted in a larger U.S. grand strategy that reconciles decoupling with other national priorities, from international trade to domestic political stability to global climate change, that might be impacted directly or indirectly. Washington still lacks such a decoupling strategy, even as it continually imposes new tech controls on China.

2. Cutting off China won't work

Cutting off China/5G for security protection won't work. Instead, we should engage with China but manage the risks

Prof. Peter Cowhey and Prof. Susan Shirk 2021. (Prof. Shirk is chair of the 21stCentury China Center at the University of California, San Diego, where Prof. Cowhey is dean of the School of Global Policy and Strategy. Both are members of the Working Group on Science and Technology in U.S.-China Relations) 9 Jan 2021 WALL STREET JOURNAL (accessed 18 Sept 2021) The Danger of  Exaggerating China’s  Technological Prowess https://china.ucsd.edu/\_files/opinion\_jan2021\_wsj\_shirk-cowhey.pdf

As such, 5G security will need to follow today’s cybersecurity template of carefully designed risk management. Weighing such trade-offs is a job for politicians and diplomats with a sophisticated grasp of the underlying technology. A security strategy aimed at eliminating all risks from technological engagement with China would fail, and as we have seen, even many U.S. allies won’t join us in breaking such ties. Tech-savvy policy leaders must find more productive ways of managing the risks of engagement with China while boosting America’s innovation ecosystem and competitiveness.

3. Can't solve for security risk

Singling out any specific telecom system is useless: Hackers can get into any system regardless of country of origin

Associated Press 2019. (journalist Frank Bajak) 28 Feb 2019 (accessed 19 Sept 2022) "Experts: US anti-Huawei campaign likely exaggerated" https://apnews.com/article/74070ddc51ef475b9e7af0cec35d4cf6

Since last year, the U.S. has waged a vigorous diplomatic offensive against the Chinese telecommunications giant Huawei, claiming that any nation deploying its gear in next-generation wireless networks is giving Beijing a conduit for espionage or worse. But security experts say the U.S. government is likely exaggerating that threat. Not only is the U.S. case short on specifics, they say, it glosses over the fact that the Chinese don’t need secret access to Huawei routers to infiltrate global networks that already have notoriously poor security. State-sponsored hackers have shown no preference for one manufacturer’s technology over another, these experts say. Kremlin-backed hackers, for instance, adroitly exploit internet routers and other networking equipment made by companies that are not Russian. If the Chinese want to disrupt global networks, “they will do so regardless of the type of equipment you are using,” said Jan-Peter Kleinhans of the Berlin think tank Stiftung Neue Verantwortung.

DISADVANTAGES

1. Harms US economy

Suppressing Chinese technology backfires: 1) Harms US industry 2) Accelerates China's technological independence

Scott Kennedy 2020 (senior adviser and Trustee Chair in Chinese Business and Economics at the Center for Strategic and International Studies) 27 July 2020 "Washington’s China Policy Has Lost Its Wei" (accessed 18 Sept 2022) https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

The U.S. federal government is obsessed with the Chinese telecom giant Huawei. It has adopted a multipronged strategy to crush the company and decouple the Western world from China’s telecom and semiconductor industries. Although well-intentioned, this effort could seriously harm the United States’ economy and national security. The U.S. semiconductor industry, which is the bedrock of the U.S. economy, has thrived like never before in a globalized industry. The campaign to isolate Huawei and the greater technology decoupling enterprise threatens this historic success and accelerates China’s technological independence.

Suppressing Chinese telecom technology ends up harming US high-tech companies in the long run

Scott Kennedy 2020 (senior adviser and Trustee Chair in Chinese Business and Economics at the Center for Strategic and International Studies) 27 July 2020 "Washington’s China Policy Has Lost Its Wei" (accessed 18 Sept 2022) https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

Despite progress by Huawei and other Chinese firms, they are still dependent on U.S. and Western firms higher up the food chain. Many elements of this hierarchy have endured, with the semiconductor industry as its most crucial cog. The campaign to isolate Huawei and the greater technology decoupling enterprise threatens all of this. As the United States leads an effort to close off global markets to Huawei and other Chinese firms, Beijing will certainly respond in kind, locking out U.S. firms in favor of their counterparts from Europe, South Korea, and Japan, partly out of spite, partly out of a need to have reliable suppliers. Moreover, as a result of these restrictions, China is accelerating its infamous “indigenous innovation” strategy like never before. China’s chip industry is still [several generations behind](https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence), but it is more likely to advance when deprived of external supplies. Rather than crushing China’s high-tech designs, U.S. actions are fueling them. The consequence will be slower global sales and a gradual loss of dominance for the U.S. chip industry.

2. Increased risk of war over Taiwan

Link: Strangling Chinese telecom technology increases risk of China invasion of Taiwan

Scott Kennedy 2020 (senior adviser and Trustee Chair in Chinese Business and Economics at the Center for Strategic and International Studies) 27 July 2020 "Washington’s China Policy Has Lost Its Wei" (accessed 18 Sept 2022) https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

Close cross-strait economic ties are also vitally important to China. Not only do Taiwanese firms, such as Foxconn, employ millions of Chinese workers, but the island also plays a crucial role in China’s tech sector. In chip production, even with the emergence of manufacturers such as Shanghai-based Semiconductor Manufacturing International Corporation ([SMIC](https://www.caixinglobal.com/2020-07-15/in-depth-chinas-chip-dreams-power-smics-mega-ipo-101580331.html)), TSMC is irreplaceable. This economic reality is a huge disincentive for China to openly use force against the island. A U.S. policy to strangle China’s semiconductor and telecom sectors, thereby decoupling China and Taiwan’s economies, [raises the security risks for Taipei](https://nationalinterest.org/feature/could-donald-trump%E2%80%99s-war-against-huawei-trigger-real-war-china-162565), and hence, for the United States as well.

Backup Link: China threatens to invade Taiwan because they believe it's already theirs, not a separate country like Russia/Ukraine

CNN 2022. (journalist Michelle Toh, CNN Business) 23 Mar 2022 " Russia's invasion of Ukraine has foreign investors fleeing Taiwan. Here's why[" (accessed 15 Sept 2022) https://www.cnn.com/2022/03/23/investing/taiwan-investment-jitters-russia-ukraine-intl-hnk/index.html](%22%20(accessed%2015%20Sept%202022)%20https://www.cnn.com/2022/03/23/investing/taiwan-investment-jitters-russia-ukraine-intl-hnk/index.html)

China's ruling Communist Party has repeatedly vowed to "reunify" with the island — using force if necessary. "Ukraine is a sovereign state, while Taiwan is an inseparable part of China's territory," Qin Gang, China's ambassador to the United States, wrote in a [Washington Post op-ed](https://www.washingtonpost.com/opinions/2022/03/15/china-ambassador-us-where-we-stand-in-ukraine/) published last week. "These are totally different things."

Backup Link: Mainland China seriously wants to reunify with Taiwan, by force if necessary

Dr. Ted Galen Carpenter 2018 (contributing editor to both the National Interest and American Conservative, serves on the editorial boards of Mediterranean Quarterly and the Journal of Strategic Studies. Ph.D. in U.S. diplomatic history from Univ of Texas.) 20 Feb 2018 “Will the U.S. Go to War with China over Taiwan?” (accessed 16 Sept 2022) https://www.cato.org/publications/commentary/will-us-go-war-china-over-taiwan

Chinese officials are hypersensitive about any Taiwanese trappings of independence, even though the island has never been under the PRC’s control. Australian scholar Andrew Tan aptly summarizes Beijing’s attitude: “For China, Taiwan represents unfinished business from the Chinese civil war and an emotionally charged nationalist issue that far outranks tensions in North Korea, the Senkaku Islands and the South China Sea. For a rising great power that is increasingly confident, assertive and nationalistic, the reunification of Taiwan with the mainland is its top, non‐negotiable national priority.” Indeed, the PRC passed its Anti‐Secession Law in 2005, emphasizing that China would use force if necessary to prevent any move by Taiwan toward formal independence.

Brink: US & China must reduce tensions now to avoid a potentially disastrous instability

Dr. David Keegan 2021 (Ph.D. in Chinese History; adjunct lecturer in China Studies at Johns Hopkins School of Advanced International Studies; retired from the Department of State in 2012. He was Deputy Director of the American Institute in Taiwan in Taipei and served as Director of the Office of Taiwan Policy in the Bureau of East Asian and Pacific Affairs) "Strengthening Dual Deterrence on Taiwan: The Key to US-China Strategic Stability" 6 July 2021 https://www.stimson.org/2021/strengthening-dual-deterrence-on-taiwan-the-key-to-us-china-stra

As stated at the beginning, the U.S. and China have been here before, although both sides are threatening the other’s interests and values with an intensity seldom seen before. China is proclaiming its rise to great power status, co-equal or almost co-equal with the United States; President Biden has made outcompeting China the measure of his administration. The militaries on both sides have ramped up their capabilities to deter and defeat the other. The two nations have gone beyond competition to confrontation, and both have repeatedly made determining Taiwan’s future the center of that confrontation. Whether you call Taiwan a pawn or not, it is entrapped by this clash. For that very reason, reducing tensions over Taiwan could be the initial step away from a potentially disastrous instability and perhaps toward building a restrained confidence on both sides that other outstanding conflicts can be successfully addressed.

Brink: US / China tensions are increasing and coming to the brink of war

Kevin Rudd 2020. (former Prime Minister of Australia and President of the Asia Society Policy Institute in New York) 3 Aug 2020 “Beware the Guns of August—in Asia” (accessed 16 Sept 2022) https://asiasociety.org/policy-institute/beware-guns-august-asia

Unmoored from the strategic assumptions of the previous 50 years but without the anchor of any mutually agreed framework to replace them, the world now finds itself at the most dangerous moment in the relationship since the Taiwan Strait crises of the 1950s. The question now being asked, quietly but nervously, in capitals around the world is, where will this end? The once unthinkable outcome—actual armed conflict between the United States and China—now appears possible for the first time since the end of the Korean War. In other words, we are confronting the prospect of not just a new Cold War, but a hot one as well.

Impact: Global economic collapse and nuclear war with China

Prof. Hugh White 2015 (Professor of Strategic Studies in the School of International, Political & Strategic Studies at the Australian National Univ. Served as an intelligence analyst with the Office of National Assessments; from 1995 to 2000 he was Deputy Secretary for Strategy and Intelligence.) 5 May 2015 “Will America defend Taiwan?” (accessed 16 Sept 2022) <https://www.lowyinstitute.org/the-interpreter/will-america-defend-taiwan>

US leaders must therefore ask what happens if Beijing does not back down as a crisis escalates. At what point would they back down instead? What would be the damage to US global leadership if Washington brought on a confrontation with China and then blinked first? What could happen if Washington didn't blink first? Is Taiwan's status quo worth a global economic collapse? It is worth a real risk of nuclear war with China?

Impact: US/China conflict over Taiwan would escalate and nuclear war is possible

Prof. Hugh White 2015 (Professor of Strategic Studies in the School of International, Political & Strategic Studies at the Australian National Univ. Served as an intelligence analyst with the Office of National Assessments; from 1995 to 2000 he was Deputy Secretary for Strategy and Intelligence.) 5 May 2015 “Will America defend Taiwan?” <https://www.lowyinstitute.org/the-interpreter/will-america-defend-taiwan>

Militarily, America can no longer expect a swift and certain victory in a war over Taiwan. China's anti-access/area-denial capabilities would preclude direct US intervention unless those capabilities had first been degraded by a sustained and wide-ranging strike campaign against Chinese bases and forces. China would very likely respond to such a campaign with attacks on US and allied bases throughout Asia. The US has no evident means to cap the resulting escalation spiral, and no one could be sure it would stop below the nuclear threshold. The possibility of nuclear attacks on US cities would have to be considered.

Backup: Biden says US will go to war with China over Taiwan

Associated Press 2022 (journalists Josh Boak, Aamer Madhani and Zeke Miller) 23 May 2022 "Biden: US would intervene with military to defend Taiwan" (accessed 15 Sept 2022) https://apnews.com/article/russia-ukraine-biden-taiwan-china-4fb0ad0567ed5bbe46c01dd758e6c62b

President Joe Biden said Monday the U.S. would intervene militarily if China were to invade Taiwan, declaring the commitment to protect the island is “even stronger” after [Russia’s invasion of Ukraine](https://apnews.com/hub/russia-ukraine?utm_source=apnewsnav&utm_medium=featured). It was one of the most forceful presidential statements in support of Taiwan’s self-governing in decades. Biden, at a news conference in Tokyo, said “yes” when asked if he was willing to get involved militarily to defend Taiwan if China invaded. “That’s the commitment we made,” he added.

3. Distracts us from bigger threats

Focus on Chinese network technology risks gives a false sense of security and distracts us from bigger risks

Scott Kennedy 2020 (senior adviser and Trustee Chair in Chinese Business and Economics at the Center for Strategic and International Studies) 27 July 2020 "Washington’s China Policy Has Lost Its Wei" (accessed 18 Sept 2022) https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

Banning Huawei components from U.S. networks may reduce the risks to Chinese surveillance, but a singular focus on the supply chain may provide a false sense of security and result in the United States letting its guard down to other cyber risks. Instead, there is a school of thought that effective cybersecurity begins with the assumption of “[zero trust](https://www.nextgov.com/ideas/2020/06/gov-clouds-during-covid-19-end-digital-fortress-era/166151/),” viewing threats as possible from everyone and everywhere, regardless of the equipment. Having only U.S. or “trusted” suppliers will not on its own eliminate cyber risks. As a result, the benefits of building a “fortress” for safe networks may be overstated, especially if doing so distracts the United States from continuous monitoring and protection of networks and other emerging challenges.

Impacts of the bigger risks outweigh Chinese tech threats right now. More important to focus on the bigger threats

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 U.S.-CHINA TECHNOLOGICAL “DECOUPLING” A STRATEGY AND POLICY FRAMEWORK (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

Domestically, the U.S. political system is floundering, its social cohesion fraying, and its economic promise hollowing for too many people. These trends have complex, multi-decadal causes but have dangerously accelerated in recent years. It was only a year ago that the United States suffered an abortive insurrection, and most experts believe that American democracy remains unstable. U.S. policymakers must therefore focus much of their attention on the home front, even at some risk to traditional national security priorities such as addressing Chinese tech threats. For example, the U.S. government’s ongoing crackdown on Chinese graduate students and researchers cannot be allowed to trigger a mass exodus of Chinese undergraduates, who pose little security risk yet pay billions of tuition dollars, in effect subsidizing educational opportunity for many Americans. In sum, an overaggressive technological decoupling can set back other national priorities that may matter more or come to a head sooner. This does not negate the risks of U.S.- China technological interdependence, which are real and will likely grow in years ahead. But the United States must balance the troubling possibilities of tomorrow against the lethal dangers of today. This means buying additional time for U.S. leaders to assess geo-technological developments, juggle domestic and global crises, and implement long-term investments in American technological strength. Select defensive measures can extend these timelines—helping to lay the groundwork for greater technological independence in the future, should it become needed, even as most U.S.-China tech ties are allowed to endure for now. Balancing in this way can help hedge against multiple scenarios, from full-scope decoupling to relative technological integration.

4. China retaliates

Link: US efforts to block Chinese technology will likely trigger retaliation

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 U.S.-CHINA TECHNOLOGICAL “DECOUPLING” A STRATEGY AND POLICY FRAMEWORK (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

Another feedback loop stems from Beijing’s retaliation against U.S. technology controls aimed at China, which creates a risk of lengthy tit-for-tat reactions or escalatory spirals. So far, Beijing’s responses have generally been reciprocal. For example, it established an “unreliable entities list” following increased U.S. use of the Entity List, and Beijing imposed new technology export controls after related moves by Washington. But future responses could be more damaging. Many in Beijing believe that the United States is intent on destroying the Chinese technology ecosystem, and Chinese domestic narratives about tech competition have become increasingly nationalistic. A particularly harsh U.S. restriction, or the overall accumulation of controls, may cause China to step up its responses or broaden them into new areas. Alternatively, Beijing might overreact due to misperceived U.S. intentions.

Link: Retaliation spirals and escalates. The US retaliates for Chinese retaliation, which then retaliates for that…

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 U.S.-CHINA TECHNOLOGICAL “DECOUPLING” A STRATEGY AND POLICY FRAMEWORK (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

Retaliation by China could put pressure on Washington to respond in kind, risking a repetitive cycle that takes decoupling further or faster than the United States initially envisioned. For example, the U.S. order for ByteDance to divest from TikTok was followed, less than a year later, by China’s pressure on ride-hailing company DiDi to de-list from the New York Stock Exchange. Although Beijing probably had multiple motivations for reining in DiDi, it publicly cited data security concerns, mirroring Washington’s main justification for the TikTok order. Beijing’s abrupt exercise of power over DiDi aggravated U.S. leaders’ worries that Chinese companies fail to disclose regulatory (and other) risks and are in Beijing’s thrall. Several senators seized upon the episode to promote an accelerated timeline for de-listing all Chinese companies from American exchanges under the Holding Foreign Companies Accountable Act. These moves and countermoves illustrate how easily escalatory spirals could be set in motion.

Impacts: Multiple ways Chinese retaliation would harm the US economy or educational institutions

Jon Bateman 2022. (fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace; former senior intelligence analyst, policy adviser, and speechwriter in the U.S. Dept of Defense, former special assistant to the Chairman of the Joint Chiefs of Staff) 25 Apr 2022 U.S.-CHINA TECHNOLOGICAL “DECOUPLING” A STRATEGY AND POLICY FRAMEWORK (accessed 18 Sept 2022) https://carnegieendowment.org/files/Bateman\_US-China\_Decoupling\_final.pdf

China has many cards to play if it chooses to step up its retaliation for U.S. tech restrictions. For example, it could dissuade or bar Chinese undergraduates from attending U.S. universities, depriving the United States of billions of dollars in tuition revenue at a time when many American institutions of higher learning are struggling financially. It could impose controls on the rare earth metals required for many important technologies, which China nearly monopolizes. It could further limit the activities of U.S. tech companies operating in China, bar or unwind U.S. investments and joint ventures, or ban the purchase of certain U.S. tech products.