## 5G Aff

### 2AC – Military Adv – NC3 Internal

#### Domestic Huawei networks compromise NC3 and military movements.

Katie Lillis 22, reporter for CNN covering intelligence and national security, 7/23/2022, "CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications," https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html, RMax

On paper, it looked like a fantastic deal. In 2017, the Chinese government was offering to spend $100 million to build an ornate Chinese garden at the National Arboretum in Washington DC. Complete with temples, pavilions and a 70-foot white pagoda, the project thrilled local officials, who hoped it would attract thousands of tourists every year.

But when US counterintelligence officials began digging into the details, they found numerous red flags. The pagoda, they noted, would have been strategically placed on one of the highest points in Washington DC, just two miles from the US Capitol, a perfect spot for signals intelligence collection, multiple sources familiar with the episode told CNN.

Also alarming was that Chinese officials wanted to build the pagoda with materials shipped to the US in diplomatic pouches, which US Customs officials are barred from examining, the sources said.

Federal officials quietly killed the project before construction was underway.

The canceled garden is part of a frenzy of counterintelligence activity by the FBI and other federal agencies focused on what career US security officials say has been a dramatic escalation of Chinese espionage on US soil over the past decade.

Since at least 2017, federal officials have investigated Chinese land purchases near critical infrastructure, shut down a high-profile regional consulate believed by the US government to be a hotbed of Chinese spies and stonewalled what they saw as clear efforts to plant listening devices near sensitive military and government facilities.

Among the most alarming things the FBI uncovered pertains to Chinese-made Huawei equipment atop cell towers near US military bases in the rural Midwest. According to multiple sources familiar with the matter, the FBI determined the equipment was capable of capturing and disrupting highly restricted Defense Department communications, including those used by US Strategic Command, which oversees the country's nuclear weapons.

While broad concerns about Huawei equipment near US military installations have been well known, the existence of this investigation and its findings have never been reported. Its origins stretch back to at least the Obama administration. It was described to CNN by more than a dozen sources, including current and former national security officials, all of whom spoke on condition of anonymity because they were not authorized to speak publicly.

It's unclear if the intelligence community determined whether any data was actually intercepted and sent back to Beijing from these towers. Sources familiar with the issue say that from a technical standpoint, it's incredibly difficult to prove a given package of data was stolen and sent overseas.

The Chinese government strongly denies any efforts to spy on the US. Huawei in a statement to CNN also denied that its equipment is capable of operating in any communications spectrum allocated to the Defense Department.

But multiple sources familiar with the investigation tell CNN that there's no question the Huawei equipment has the ability to intercept not only commercial cell traffic but also the highly restricted airwaves used by the military and disrupt critical US Strategic Command communications, giving the Chinese government a potential window into America's nuclear arsenal.

"This gets into some of the most sensitive things we do," said one former FBI official with knowledge of the investigation. "It would impact our ability for essentially command and control with the nuclear triad. "That goes into the 'BFD' category."

"If it is possible for that to be disrupted, then that is a very bad day," this person added.

Turning doves into hawks

Former officials described the probe's findings as a watershed moment. The investigation was so secret that some senior policymakers in the White House and elsewhere in government weren't briefed on its existence until 2019, according to two sources familiar with the matter.

That fall, the Federal Communications Commission initiated a rule that effectively banned small telecoms from using Huawei and a few other brands of Chinese made-equipment. "The existence of the investigation at the highest levels turned some doves into hawks," said one former US official.

In 2020, Congress approved $1.9 billion to remove Chinese-made Huawei and ZTE cellular technology across wide swaths of rural America.

But two years later, none of that equipment has been removed and rural telecom companies are still waiting for federal reimbursement money. The FCC received applications to remove some 24,000 pieces of Chinese-made communications equipment—but according to a July 15 update from the commission, it is more than $3 billion short of the money it needs to reimburse all eligible companies.

Absent more money from Congress, the FCC says it plans to begin reimbursing approved companies for about 40 percent of the costs of removing Huawei equipment. The FCC did not specify a timeframe on when the money will be disbursed.

In late 2020, the Justice Department referred its national security concerns about Huawei equipment to the Commerce Department, and provided information on where the equipment was in place in the US, a former senior US law enforcement official told CNN.

After the Biden administration took office in 2021, the Commerce Department then opened its own probe into Huawei to determine if more urgent action was needed to expunge the Chinese technology provider from US telecom networks, the former law enforcement official and a current senior US official said.

That probe has proceeded slowly and is ongoing, the current US official said. Among the concerns that national security officials noted was that external communication from the Huawei equipment that occurs when software is updated, for example, could be exploited by the Chinese government.

Depending on what the Commerce Department finds, US telecom carriers could be forced to quickly remove Huawei equipment or face fines or other penalties.

Reuters first reported the existence of the Commerce Department probe.  
"We cannot confirm or deny ongoing investigations, but we are committed to securing our information and communications technology and services supply chain. Protecting US persons safety and security against malign information collection is vital to protecting our economy and national security," a Commerce Department spokesperson said

US counterintelligence officials have recently made a priority of publicizing threats from China. This month, the US National Counterintelligence and Security Center issued a warning to American businesses and local and state governments about what it says are disguised efforts by China to manipulate them to influence US policy.

FBI Director Christopher Wray just traveled to London for a joint meeting with top British law enforcement officials to call attention to the Chinese threats.

In an exclusive interview with CNN, Wray said the FBI opens a new China counterintelligence investigation every 12 hours. "That's probably about 2,000 or so investigations," said Wray. "And that's not even talking about their cyber theft, where they have a bigger hacking program than that of every other major nation combined, and have stolen more of Americans' personal and corporate data than every nation combined."

Asked why after years of national security concerns raised over Huawei, the equipment is still largely in place atop cell towers near US military bases, Wray said that, "We're concerned about allowing any company that is beholden to a nation state that doesn't adhere to and share our values, giving that company the ability to burrow into our telecommunications infrastructure."

He noted that in 2020, the DOJ indicted Huawei with racketeering conspiracy and conspiracy to steal trade secrets.

"And I think that's probably about all I can say on the topic," said Wray.

Critics see xenophobic overreach

Despite its tough talk, the US government's refusal to provide evidence to back up its claims that Huawei tech poses a risk to US national security has led some critics to accuse it of xenophobic overreach. The lack of a smoking gun also raises questions of whether US officials can separate legitimate Chinese investment from espionage.

"All of our products imported to the US have been tested and certified by the FCC before being deployed there," Huawei said in its statement to CNN. "Our equipment only operates on the spectrum allocated by the FCC for commercial use. This means it cannot access any spectrum allocated to the DOD."

"For more than 30 years, Huawei has maintained a proven track record in cyber security and we have never been involved in any malicious cyber security incidents," the statement said.

In its zeal to sniff out evidence of Chinese spying, critics argue the feds have cast too wide a net — in particular as it relates to academic institutions. In one recent high-profile case, a federal judge acquitted a former University of Tennessee engineering professor whom the Justice Department had prosecuted under its so-called China Initiative that targets Chinese spying, arguing "there was no evidence presented that [the professor] ever collaborated with a Chinese university in conducting NASA-funded research."        
And on Jan. 20, the Justice Department dropped a separate case against an MIT professor accused of hiding his ties to China, saying it could no longer prove its case. In February, the Biden administration shut down the China Initiative entirely.     
The federal government's reticence across multiple administrations to detail what it knows has led some critics to accuse the government of chasing ghosts.

"It really comes down to: do you treat China as a neutral actor — because if you treat China as a neutral actor, then yeah, this seems crazy, that there's some plot behind every tree," said Anna Puglisi, a senior fellow at Georgetown University's Center for Security and Emerging Technology. "However, China has shown us through its policies and actions it is not a neutral actor."

Chinese tech in the American heartland

As early as the Obama administration, FBI agents were monitoring a disturbing pattern along stretches of Interstate 25 in Colorado and Montana, and on arteries into Nebraska. The heavily trafficked corridor connects some of the most secretive military installations in the US, including an archipelago of nuclear missile silos.

For years, small, rural telecom providers had been installing cheaper, Chinese-made routers and other technology atop cell towers up and down I-25 and elsewhere in the region. Across much of these sparsely populated swaths of the west, these smaller carriers are the only option for cell coverage. And many of them turned to Huawei for cheaper, reliable equipment.

Beginning in late 2011, Viaero, the largest regional provider in the area, inked a contract with Huawei to provide the equipment for its upgrade to 3G. A decade later, it has Huawei tech installed across its entire fleet of towers, roughly 1,000 spread over five western states.

As Huawei equipment began to proliferate near US military bases, federal investigators started taking notice, sources familiar with the matter told CNN. Of particular concern was that Huawei was routinely selling cheap equipment to rural providers in cases that appeared to be unprofitable for Huawei — but which placed its equipment near military assets.

Federal investigators initially began "examining [Huawei] less from a technical lens and more from a business/financial view," explained John Lenkart, a former senior FBI agent focused on counterintelligence issues related to China. Officials studied where Huawei sales efforts were most concentrated and looked for deals that "made no sense from a return-on-investment perspective," Lenkart said.

"A lot of [counterintelligence] concerns were uncovered based on" those searches, Lenkart said.

By examining the Huawei equipment themselves, FBI investigators determined it could recognize and disrupt DOD-spectrum communications — even though it had been certified by the FCC, according to a source familiar with the investigation.

"It's not technically hard to make a device that complies with the FCC that listens to nonpublic bands but then is quietly waiting for some activation trigger to listen to other bands," said Eduardo Rojas, who leads the radio spectrum lab at Embry-Riddle Aeronautical University in Florida. "Technically, it's feasible."

To prove a device had clandestine capabilities, Rojas said, would require technical experts to strip down a device "to the semi-conductor level" and "reverse engineer the design." But, he said, it can be done.

And there was another big concern along I-25, sources familiar with the investigation said.

Weather camera worries

Around 2014, Viaero started mounting high-definition surveillance cameras on its towers to live-stream weather and traffic, a public service it shared with local news organizations. With dozens of cameras posted up and down I-25, the cameras provided a 24-7 bird's eye view of traffic and incoming weather, even providing advance warning of tornadoes.

But they were also inadvertently capturing the movement of US military equipment and personnel, giving Beijing — or anyone for that matter — the ability to track the pattern of activity between a series of closely guarded military facilities.

The intelligence community determined the publicly posted live-streams were being viewed and likely captured from China, according to three sources familiar with the matter. Two sources briefed on the investigation at the time said officials believed that it was possible for Beijing's intelligence service to "task" the cameras — hack into the network and control where they pointed. At least some of the cameras in question were running on Huawei networks.

Viaero CEO Frank DiRico said it never occurred to him the cameras could be a national security risk.

"There's a lot of missile silos in areas we cover. There is some military presence," DiRico said in an interview from his Colorado office. But, he said, "I was never told to remove the equipment or to make any changes."

In fact, DiRico first learned of government concerns about Huawei equipment from newspaper articles — not the FBI — and says he has never been briefed on the matter.

DiRico doesn't question the government's insistence that he needs to remove Huawei equipment, but he is skeptical that China's intelligence services can exploit either the Huawei hardware itself or the camera equipment.

"We monitor our network pretty good," DiRico said, adding that Viaero took over the support and maintenance for its own networks from Huawei shortly after installation. "We feel we've got a pretty good idea if there's anything going on that's inappropriate."

### 2AC – Eurasia DA – UQ

#### Tech influence is failing now.

Marta Makowska 22, Senior Research Fellow at the Polish Institute of International Affairs, Guest Contributor to Council on Foreign Relations, 5/19/2022, "China’s Digital Authoritarianism vs. EU Technological Sovereignty: The Impact on Central and Eastern Europe," Council on Foreign Relations, https://www.cfr.org/blog/chinas-digital-authoritarianism-vs-eu-technological-sovereignty-impact-central-and-eastern, RMax

What is Next for China in the Region After the War in Ukraine?

China’s support for Russia’s invasion of Ukraine may be a defining moment for the future of EU-China relations. For most Central and Eastern European states, the war, and Beijing’s embrace of Moscow, will result in a further political decoupling from China. This will have an impact on economic relations as well: The reception of Chinese tech companies in these countries, already under severe pressure, will suffer even further scrutiny. Perhaps, more Chinese firms will be banned from Central and Eastern European markets.

What’s more, China’s cooperation with Russia will further mobilize Central and Eastern European policymakers, particularly those from the Baltics and Poland, to advocate for deepening strategic cooperation on security infrastructure with the United States and other like-minded governments across the world, beyond already existing NATO cooperation.

### 1AR – Eurasia DA – AT: CCP Instability

#### CCP’s resilient – western academics are biased.

Tang 18 Wenfang Tang, Political Science Professor at the University of Iowa. [The “Surprise” of Authoritarian Resilience in China, American Affairs, 2(1), 101–117]//BPS

The information explosion based on public opinion surveys in China in the past thirty years has left a few cracks in the empirical foundation of some of the classic theories of political science that were first developed in the West with limited firsthand evidence. For example, the classic theory of civic culture was developed from survey data in only five countries—the United States, the United Kingdom, Germany, Italy, and Mexico. Today, the World Values Surveys cover more than eighty countries in all continents with human inhabitation. Among these countries, China stands out as an outlier and does not fit the theoretical predictions of Western political science. As discussed in the above mentioned “surprises”: (1) the Tiananmen protest in 1989 was an anti-reform movement, but it was expected to be a pro-democratic movement; (2) the Chinese regime enjoys strong public support even though many in the West expected it to have collapsed already; (3) social capital in China is among the highest in the world, despite political science’s expectation that its authoritarian political system would produce public distrust; (4) the authoritarian government is (perceived to be) highly responsive while the theory of democracy predicts otherwise; and (5) Chinese citizens are politically active and enjoy a strong feeling of political efficacy even if they are expected to be politically apathetic. One problem in the existing political science literature is the rigid (and black-and-white) definition of democracy. For example, in the rankings of democracy and freedom by Polity25 and Freedom House,26 both highly respected organizations whose annual rankings are widely used in political science teaching and research, China has been consistently ranked at the very bottom in terms of freedom and democracy. Yet in the World Values Survey in 2012, more than 60 percent of Chinese respondents said they felt free, which was higher than in many democracies. Yes, the Chinese may have extremely low expectations, but they do feel free, and that feeling matters because unhappy citizens can cause political disruption. The problem of measurement error is not only limited to China. In fact, when comparing the subjective feelings in public opinion surveys with the “objective” measures of democracy in the rankings assigned by Polity and Freedom House, public opinions throughout the world show a negative correlation with the democracy rankings. This negative relationship between the subjective and the “objective” measures of democracy can be clearly seen in the chart below, based on the Global Barometer Surveys (2010–2015) covering more than seventy countries and regions. The respondents in these surveys were asked about their opinions regarding the following six questions related to the levels of subjective democracy in their societies: (1) The level of democracy is very high in my country; (2) The democratic system in my country is functioning very well; (3) Ordinary people in my country can freely express their opinions; (4) I trust the media in my country; (5) My government responds to what people need; and (6) I am satisfied with my government’s performance. These six items are combined into a single index of subjective democracy. When this index is compared to the Polity scores of “objective” democracy in these same countries and regions, the correlation coefficient is a statistically significant –0.51! In other words, democratic citizens feel less democracy and freedom in their societies than authoritarian citizens. One way to solve the inconsistency between the subjective and “objective” measures is to slightly stretch the concepts in the political science literature. Concept stretching may carry a negative meaning because it may result in the diluted explanatory power of a theory. Yet overly rigid definitions can limit the scope and effectiveness of political analysis. Some of the key concepts in political science can be stretched (or enriched) by the available public opinion surveys. For example, the traditional study of authoritarian politics can include both elites and masses, and formal and informal politics;27 social capital can incorporate both civic trust (trusting strangers) and community-based interpersonal trust. More importantly, the traditional definitions of democracy, freedom, government responsiveness, and political legitimacy that are derived from institutional designs (objective measures) can be enriched by including public (not elite) perceptions of these concepts (subjective measures). Those who only focus on the institutional design of democracy but discount the importance of public perception of democracy run the risk of political arrogance. Finally, a further barrier to understanding China’s authoritarian resilience is ideological bias. While people outside China take it for granted that academic research in China is ideologically limited, it is also true that China is frequently judged with ideologically tinted glasses by some media organizations and scholars in the West. According to these ideologically tinted views, the authoritarian political system in China is inherently bad; supporting such a system is unhealthy; civic trust is the only type that can qualify as interpersonal trust and social capital; government responsiveness is due to Chinese citizens’ “extremely low expectations,” and so on. These value judgements prevent researchers from understanding what is working and what is not working in the Chinese political system, regardless of whether it is good or bad.

### 1AR – Eurasia DA – AT: China Diversionary War

#### No diversionary war under Xi.

Yin 19 George Yin, government PhD from Harvard, political economy MSc from the London School of Economics, Dickey Fellow in U.S. Foreign Policy and International Security at Dartmouth College. [Domestic repression and international aggression? Why Xi is uninterested in diversionary conflict, 1-22-2019, https://www.brookings.edu/articles/domestic-repression-and-international-aggression-why-xi-is-uninterested-in-diversionary-conflict/]//BPS

Crucially, diversionary war theory rests on a number of assumptions, two of which do not hold for Xi today. Assumption 1: Leaders prefer foreign adventure over addressing domestic troubles. As discussed earlier, in the realm of domestic policies, Xi has been criticized for primarily two things: his promotion of his cult of personality and a slowing Chinese economy overly focused on inefficient SOEs. It is easy for Xi to dial back his cult of personality, and he has already done so. Reverting his policy of guo jin min tui (“as the state advances, the private sector retreats”) is not going to be easy and would entail important financial system and legal reforms (see discussions from the 2018 Chinese Economists 50 forum), but is quite doable. There is little reason why Xi would want to create international tension to distract his critics when it is much more straightforward to directly address the domestic issues. Furthermore, a diversionary skirmish involving Vietnam or the Philippines over one of the South China Sea islands would hardly be significant enough for diversion. To rally the nation behind him, Xi must pick on Taiwan, Japan, or even the United States. The problem is that a confrontation with either Taiwan or Japan is highly risky. The Chinese military, which has not fought a war since the Sino-Vietnamese conflict in 1979 and is embroiled in corruption scandals, might well suffer defeat. Perhaps China could take on the United States in the economics arena, but China has been unable to react effectively to the ongoing trade war with the United States. CCP elites do not want international conflict, especially one involving the United States. Assumption 2: Key domestic political players want conflict. Most importantly, the CCP elites do not want international conflict, especially one involving the United States. This is not because the CCP elites like the United States, which is still seen by many as an imperial power that supports Japanese militarism and secessionism in Taiwan, Hong Kong, Tibet, and Xinjiang. However, in Fan’s words, it is important “to deal with domestic issues before pacifying the barbarians” (an nei rang wai). In the eyes of his critics, any foreign adventure would indicate that Xi was getting the priorities wrong and further deviate from Deng’s grand strategy of fostering a favorable foreign environment to promote development. A diversionary conflict is therefore likely to further galvanize Xi’s opposition. In conclusion, the Xi administration’s performance since 2012 has been attacked by a wide range of groups that constitute China’s governing elites; Xi can do little to eliminate rival factions who are waiting for the opportune moment to strike back. Xi is unlikely to be interested in a foreign adventure that would at best distract him from domestic power struggles, and at worst provide more political ammunition for his opponents to use against him. Instead, Xi actually faces a lot of pressure to improve China’s relations with the U.S. in his second term, which could help him deal with his domestic troubles or at least not exacerbate them.

#### Diversionary War Theory is wrong.

Wang 18 Yaping Wang, Politics PhD Candidate at the University of Virginia, M.A. at both George Washington University and the National University of Singapore. [The Dog That Barks: Understanding Propaganda Campaigns on Territorial Disputes, Dissertation for the University of Virginia]//BPS

The logic of the diversionary argument is summarized in Figure 2.5. The limitation with this argument is that resorting to nationalism for regime legitimacy is a dangerous venture. For one, it increases the chance of unwanted conflicts that might eventually wear off the nationalist sentiments. The audience cost theory argues that diversions are too risky because they tie a government's hands. Two, the anger of the mass might turn inward and backfire to threaten regime survival.100 State leaders are aware of these risks. Existing literature on state-instigated nationalism has not reached a conclusion on why and when states would overcome such trade-offs and deliberately pursue such a risky policy. Managing nationalism within control is, after all, a delicate game. Besides, for authoritarian states where domestic stress is a constant concern and governing legitimacy is always a valued good given the non- democratic nature of the government, it remains a puzzle as why stoking nationalism through hiking up territorial disputes is not a constant effort. It also does not explain why states choose some disputes but not others to attract the public eye for regime consolidation purposes. Despite these shortcomings, diversionary war theory has often been used to explain authoritarian international behaviors because of its emphasis on domestic politics and regime survival at home, which are critical in understanding authoritarian foreign policy. So it deserves our attention here.

### 2AC – Russia CP – Intrinsic Perm

#### Russia doesn’t care about 5G.

Ian Morris 20, international editor for LightReading, 11/19/2020, "Russia's long 5G wait goes on," Light Reading, <https://www.lightreading.com/5g/russias-long-5g-wait-goes-on/d/d-id/765563>, RMax

As 5G hurtles through China and goes live in the West, it has been stopped in its tracks like Napoleon's army in the vast expanse of Russia.

None of the mobile operators looks close to launching a mainstream 5G mobile service. If there is such a thing as a 5G "race" between different countries, Russia is merely a spectator.

While bad weather halted 19th-century Frenchmen, a lack of spectrum has bogged down 5G. Most other countries have settled on 3.4-3.8GHz as the optimal frequency real estate for the rollout of 5G services.

In Russia, those bands are still occupied by government agencies and the military. A discussion about freeing them up for the telecom sector has so far been fruitless.

"What we are getting from the government is that regulators are unwilling to allocate in the 3.4-3.8GHz range, which is the bandwidth for 5G in most countries," says Andrey Kamensky, the chief financial officer of MTS, Russia's biggest mobile operator.

"The discussion is happening, but we do not see a willingness from the regulator to come up with this."