Social Antiaccess/Area-Denial (Social A2/AD)

Colonel Phil Zeman, USMC

Abstract: Social antiaccess/area-denial (A2/AD) describes the threat posed to U.S. and Western security by sociopolitical and socioeconomic means, primarily by China and Russia. This concern focuses on actions by China and Russia designed to fracture American and Western societies through information, disinformation, economic coercion, and creating economic dependencies—in many cases capitalizing on target nation propensities to accomplish strategic ends. Through these ways, China and Russia hope to prevent the will or ability of American or Western states to respond to aggressive acts.
Keywords: national security, antiaccess/area-denial, A2/AD, China, Russia

In the wake of the 1991 Gulf War, America's would-be adversaries took note of the overwhelming power of the U.S. war machine. They recognized the value and impact of our operational reach, technological overmatch (specifically precision targeting), martial proficiency, command and control, and doctrine. Acknowledging U.S. prowess in these areas, they devised strategies and techniques designed not to compete with the United States head-on, but to find weaknesses and opportunities to counter—and avoid—American military strength. To a significant extent, these developments have manifested themselves as antiaccess/area-denial (A2/AD) capabilities, designed to restrict American operational reach—most notably in antiship and antiair systems.[1] Just 10 years after Operation Desert Storm, U.S. and allied forces were again in action. The conflict in Afghanistan, shortly followed by entry into Iraq, was of a different character from Desert Storm, where American firepower and technological

Col Phil Zeman has served in the U.S. Marine Corps for more than 27 years in infantry, reconnaissance, strategy, and planning posts.

prowess was not decisive—they proved only modest enablers. In searching for a viable response to this change in character, U.S. forces introduced the concept of war among the people, stipulating a shift in the conduct of military campaigns.[2] U.S. and allied forces focused campaign objectives on winning the support of the population and not purely the physical elimination of insurgents and terrorists. This population-centric approach appreciated the decisive roles of information, perception, and culture. This revised doctrinal approach recognized that populations—and with them, societies—are the basis of strength and power.[3]

The 2017 *National Security Strategy* returned the U.S. military to consideration of great power conflict.[4] Visions of the never-experienced great tank battles in Germany's Fulda Gap were now fused with twenty-first century weapons and technology.[5] This twenty-first century-remix of great power conflict is more than an update to previous conventional doctrine, as America's adversaries (both nation-state and nonstate) incorporate their observations from 1991, while adding a population-centric focus. This synthesis points to a different battlefield where the immense capability of the U.S. military is greatly reduced—or nullified altogether. While much discussion surrounds Chinese and Russian A2/AD networks and capabilities, the nonmilitary threat to the United States (and the West in general) receives muted attention—even in the face of repeated Chinese and Russian (among others) information and cyberattacks.

This emergent threat is subtle and coercive in nature, targeting not only the military or government but also industry and citizens. It is designed to exploit social dynamics and economic propensities by creating dependencies on foreign capacities. This strategic design is multifaceted; it exploits and expands the seams in democratic politics, degrades societal cohesion, and puts average citizens at risk while using those same citizens to create and expand economic dependencies—unwitting self-perpetuation of their own demise. Further, these actions are conducted simultaneously and comprehensively in a myriad of venues and ways, compounding the effect. This effort is opaque by design, with layers of complexity that inhibit identification and attribution. Indeed, even in the cases where nefarious actions are realized, other mechanisms deny and further obfuscate the actions while applying coercive countermeasures. Potentially the most significant element of this strategic approach is to never provide a casus belli sufficient to mobilize popular sentiment for response. The intent is not to defeat the United States or the West on the battlefield. The goal is to prevent the Unites States and its allies from even arriving on the field of battle by compromising national the socio-political-economic fabric to the point where it is unable, or *unwilling*, to respond to aggression. With voluminous discussion dedicated to penetrating and countering Chinese and Russian physical A2/AD

networks, there needs to be a similar conversation surrounding the comprehensive nonmilitary targeting of America, with the intent to compromise American resolve, capability, and capacity to respond. America and the West need to recognize the threat posed by *social A2/AD*.[6]

Social A2/AD's main effort is to target the civilian population. It achieves this through information/disinformation campaigns as exhibited through its "Three Warfares" approach of public opinion warfare, influence warfare, and legal warfare, creating economic dependency through enticing corporate investment into Chinese markets, and fostering debilitating sociopolitical activity.[7] Notably, all of these disparate operations are interwoven, capitalizing on opportunities (often unwittingly created by the target population), while creating others. Further, it is important to recognize that there are multitudes of mechanisms that can be used to discreetly influence the social, political, and economic activity. Correspondingly, these domains continuously influence each other, compounding effects. As these dynamic influences interact, they also affect other elements, such as military power. Thus, the endgame of social A2/AD is to gain influence within a second or third state sufficient to prevent or restrict action against the instigating (aggressor) state.

Considering that social A2/AD is primarily a nonmilitary challenge, the well-trod dictums of the war theorist Sun Tzu provide valuable insights for defeating an opponent without force of arms: "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[8] Sun Tzu continues this line of thinking, stating, "Therefore I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril'."[9] (Considering Sun Tzu was Chinese, it should be of little surprise that China would implement this approach. This is analogous to the discovery of gambling in a casino.) Further, a cursory understanding of the Chinese concept of *Shih* reinforces a people-centric view of strategy: "Since men and their hearts were critical to Shih-strategy, commanders and rulers needed to understand how to mobilize them."[10] Although Shih is typically in reference to one's own population and internal strength, it can simply be extended in reverse to an adversary; degrading the strength of your opponent's population is to your advantage. Using Sun Tzu's statements and Shih as a baseline, one can design a strategy designed to maximize indirect approaches and achieve victory without open conflict. This readily blends with the West's best-known military theorist, Carl Von Clausewitz, and his concept of center of gravity, by targeting your opponent's center of gravity while protecting your own.[11] Clausewitz explains that "one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends."[12] Simple analysis

and synthesis of these principles provides a strong argument, and they become especially compelling when woven into a competitive, dynamic, strategy.

Elements of Social A2/AD

During the past decade, many of the attacks against the United States and other Western nations targeted populations, not governments. The Russian cyberattack on Estonia, interference in the 2016 U.S. presidential election, and Chinese hacking of the Office of Personnel Management (OPM) and Marriott hotels are a small sampling of such attacks and demonstrate the intent to disrupt and gain influence over civilian populations. Consider the potential effects, implications, and disruption caused by digital attacks targeting the individual finances of Americans (as "shaping" actions prior to a military campaign, or even as the chosen mechanism to alter behavior). What if these attacks came as the culmination of a comprehensive information campaign designed to convince a population that the so-called threat presented by Russia or China was nothing more than the fantastic conjuring of conspiracy theorists? Part of the campaign would include creating an environment hostile to development of preconflict safeguards and protections complete with twenty-first century "useful idiots" to champion China or Russia as misunderstood and wrongly accused. This information campaign would also find mechanisms to pit American versus American and ally against ally. China and Russia are not simply looking to compromise government systems and capabilities; they desire to hold private citizens and corporations at risk to degrade or prevent effective response, regardless of the mechanism, through societal friction, while discrediting and delegitimizing national leadership.[13]

Although American sociopolitical friction has become increasingly common (although few recognize the associated vulnerability), Europe may be even more susceptible to malicious information campaigns. With existing ethnic tensions, rising authoritarianism, and economic challenges (Brexit), increasing inter- and intra-European conflict appears an easy task. A European scenario requires little imagination: digital and information attacks culminate just as Russian forces conducting "exercise" Zapad in western Russia turn toward the Baltic states. As Russian brigades speed through Vilnius, Lithuania, to Kaliningrad, Russia, and occupy Riga, Latvia, and Tallinn, Estonia, something else takes place. The people of Germany, already with a pacifistic outlook, become enraged and disenchanted by information designed to simultaneously discredit national leadership, legitimize Russian actions (propaganda), and fracture social bonds. This leads to calls for immediate peace, with a simultaneous prohibition of North Atlantic Treaty Organization (NATO) forces transiting through Germany to the Baltics. Lacking access through Germany, the NATO response to Russian aggression in the Baltics is stopped cold. Although this scenario may

seem fantastic, a 2015 Pew Research poll (done in the wake of the Russian intervention in Ukraine) found that German popular support for using force to support an ally from Russian military aggression was only 38 percent. Italy polled at 40 percent. Immediately threatened Poland fell in at 48 percent, and America's special ally, the United Kingdom, came in at 49 percent. The only countries to top 50 percent were the United States (56 percent) and Canada (53 percent).[14] The results of this poll indicate that NATO may face as much threat from within as from without. A Russian act that would trigger NATO's article 5, the collective defense article, could fracture the alliance between the nations that would and would not uphold treaty obligations.

The Pew Research findings are not harbingers of the demise of NATO; however, they do indicate opportunity for Russia (or China) to influence Europe. Russia has repeatedly used its dominant position in Europe's natural gas supply as a weapon of coercion.[15] China has lately also inserted itself into Europe's economic affairs:

> In 2016 Chinese investment in the European Union jumped to nearly €36bn ($40bn), up from €20bn the previous year, according to Rhodium Group, an American research firm. The recent purchases of major interest of major European ports such as Antwerp, Rotterdam, and Hamburg, or outright ownership of major ports (Piraeus) illustrate this point. Much of this is state-backed and speaks of the Communist Party's ambitions to keep Europe from helping America to contain China's rise.[16]

Further, through China's Belt and Road Initiative (BRI), the purchase and development of international transportation infrastructure has given rise to concerns about predatory loan practices—with indirect intended results that span physical, financial, and digital spectrums. By dictating the terms and conditions of predatory loans with associated project bidding requirements (prescribed use of Chinese construction and telecom companies), and bribing local officials, China has been able to gain advantage in countries across Asia, Africa, and even Europe. In some cases, China has turned this leverage into forced accommodation on items not previously envisioned. A prime example of this is China's leveraging of unsustainable loans to Sri Lanka into a Chinese People's Liberation Army Navy (PLAN) facility in Hambantota, Sri Lanka.[17] Sri Lanka is not alone in falling victim to predatory loans from China; many countries in the region are seen as debt risks due to Chinese BRI loans.[18] Punctuating the concerns is the extension of China's advanced digital structure, extending the "Digital Silk Road" across Asia—and with it, China's advanced surveillance apparatus.[19]

While China's financial practices have produced physical access abroad for the Chinese military, perhaps the most concerning element of access pertains to information and China's advanced surveillance apparatus. With China's Huawei at the forefront of 5G technology in Europe, the issue of information security has put the United States at loggerheads with two key allies, the United Kingdom and Germany, putting security-sharing agreements at risk.[20] Should Europe be enticed by Huawei's cheap 5G technology, it will serve as another layer of dependency on Chinese goods. Aside from concerns about Chinese surveillance, cost of future extraction would increase—both in terms of financial cost and China's ability to exert coercive power (not unlike Russia's ability to use natural gas as a lever in international discourse)—while simultaneously driving a wedge between long-standing, like-minded Atlantic allies. Although national security concerns are paramount, Chinese surveillance intrusion also presents a grave threat to Western values regarding the individual rights to privacy and information control and access. This, in turn, relates back to the targeting and holding at risk of citizens and private business—attacking the very fabric of Western society.

The above examples illustrate the immense potential of social A2/AD. Free-speech democracies are particularly vulnerable to these types of actions, as they take advantage of civil liberties held sacred by the United States and other open, free societies. In the European example, the Russians used social A2/AD to defeat a key military strength of the United States—its operational reach. That the Russians may or may not lack capability or capacity to fight the U.S. military in a multi-month campaign is irrelevant if the United States and its NATO allies are unable to get forces to the battlefield. Even if the United States and NATO were to find a path around the German impediment described above, Vladimir Putin would have already succeeded in gaining one of his most sought-after strategic objectives: gutting NATO through German rejection of an obvious article 5 event. If Russia or China successfully influence the *populations* of the champions of the existing global system, the impacts would be grievous for the existing world order and its leader, the United States. Defending democratic societies against authoritarian threats who would deceive, obfuscate, coerce, and subvert them must be the United States' and its allies' highest priority. Significantly, these concerns are just as real at home in the United States.

The special counsel investigation into alleged collusion with Russia presents an interesting example of the potential of social A2/AD. Acknowledging significant popular and media animosity toward President Donald J. Trump, it is easy to envision that the trickle of collusion-associated information was part of a scheme to drive further division within an already fractured U.S. society.[21] The point is not that the investigation itself is a Russian act, but that it provides an opportunity to exacerbate sociopolitical friction by providing information

designed to push the investigation along, widening existing fractures within American society. Although it is impossible to prove a negative, it takes little imagination to see that Russia may have hedged its bets during the 2016 presidential election. Consider the ire of the Republican Party with the findings of the Federal Bureau of Investigation (FBI) probe into the Hillary Rodham Clinton email scandal, among other issues. These issues provide the ideal opportunity for disinformation coming from opaque sources to fan a flame of anti-Clinton sentiment designed to hamstring government action and increase existing societal friction. In either of these examples, emotion overtakes fact, propagated by a 24-hour news cycle and a social media environment dominated by the dramatic at the expense of truth. In *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, authors Peter Pomerantsev and Michael Weiss explain, "The Kremlin exploits the idea of freedom of information to inject disinformation into society. The effect is not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods."[22] Even if both the above scenarios are off base, it is a common refrain that the current U.S. social environment is highly divided and antagonistic; U.S. society is ripe and open for exploitation. Sadly, much of this damage is done at the behest of China and Russia unwittingly; blinded by animosity, Americans are frequently the chief propagators of this intra-American social fratricide, serving Russian and Chinese interests as cyber and information goons. This concept is captured well by Douglass Rushkoff as he reintroduces the Leninist term of *useful idiots* for modern-day Russia:

> [L]ess important for their indictment of Trump and the agents he hired than for how they expose the way we all continue to buy into this manufactured animosity. So, no, the liberal elite did not infuse the landscape with today's more belligerent forms of identity politics. Neither did the far right invent the most contagious conspiracy theories about Hillary Clinton or George Soros. They are the result of four decades and hundreds of millions of dollars of targeted disinformation by Russia. Even more damaging than the stories themselves is how they make us feel about the "other side," who we believe has stooped to this level of shameful lying and rhetoric.[23]

The opioid epidemic, a front-page story within the United States, provides an even more sinister example of the breadth and cross discipline character of social A2/AD. As this crisis has grown in intensity, a new dynamic has emerged: China is a leading producer of both opioids and opioid precursor chemicals in what many call the "Reverse Opium War."[24] Further, much of the processing and transportation of these illegal drugs is done by Mexican cartels. Although

widespread popular recognition of the opioid epidemic is relatively recent, the Mexican government has recognized the concern for more than a decade. A former Mexican ambassador to Beijing describes the issue:

> When Jorge Guajardo arrived in Beijing as Mexican ambassador in 2007, he came with a directive about what was his country's most urgent issue with the Chinese government. Mexico needed China to curb its manufacturing and sale of a dangerous class of chemicals—precursors to making fentanyl and other synthetic drugs—that flowed nearly unchecked into North America. . . . Drug cartels in Mexico used the China-made chemicals to fuel their growing arsenal of heroinlike synthetics sold into the United States to feed the country's hunger for opioids. For six years, his tenure as ambassador, Guajardo tried to get China's government to stop production of the chemicals powering the deadly epidemic. . . . "Every single time, the Chinese would shrug and say, 'We don't know what you're talking about'," he recalled. "They never wanted to pay attention to it."[25]

Fitting the profile of attribution evasion, the nexus between Chinese government, opioid production, and Mexican cartels provides a perfect example of actions that cross multiple domains, making attribution, let alone response, very challenging. The opioid epidemic is so severe that it has led to a decline in American life expectancy and labor participation rates, compounding adverse societal impacts.[26] Beyond these implications, something far more wicked could be in play: American opioid deaths may not simply be the unintended consequences of legitimate pharmaceutical production but part of a larger design to compromise the social fabric of the United States.

American addiction to Chinese products is not limited to opioids and their derivatives. "Made in China" is a ubiquitous label in the United States; Americans are accustomed to cheap, throwaway Chinese products, as well as high-tech products such as smartphones, televisions, and other appliances.[27] American consumption of Chinese goods has not only led to a massive trade deficit, but there is another much more concerning dependency that has been created: the U.S. military's industrial supply chain has many Chinese producers at its base.[28] As reported in *Financial Times*, "China represents a significant and growing risk to the supply of materials and technologies deemed strategic and critical to US national security."[29]

Despite the fractious U.S.-Chinese trade battles in 2019, American companies continue their addiction to the massive and growing Chinese consumer market, as illustrated by Walmart's declared intent to invest $1.2 billion in its

Chinese distribution centers.[30] The lure of Chinese market share comes with challenges and stipulations, most notably in requirements for Chinese-majority joint venture (JV) and the transfer of intellectual property (IP):

> First, the Chinese government uses foreign ownership restrictions, such as formal and informal JV requirements, and other foreign investment restrictions to require or pressure technology transfer from U.S. companies to Chinese entities. These requirements prohibit foreign investors from operating in certain industries unless they partner with a Chinese company, and in some cases, unless the Chinese partner is the controlling shareholder. Second, the Chinese government uses its administrative licensing and approvals processes to force technology transfer in exchange for the numerous administrative approvals needed to establish and operate a business in China.[31]

Here again, we witness the wisdom of Sun Tzu: "Thus, those skilled at making the enemy move do so by creating a situation to which he must conform; they entice him with something he is certain to take, and with lures of ostensible profit, they await him in strength."[32] Although Sun Tzu is considered a military philosopher, the above comment could be applied in a variety of domains—including economic. Economic warfare has many adaptations, such as coercion (as mentioned previously with Gazprom), market enticement, and the theft of intellectual property.

Concerns regarding the transfer of intellectual property are not limited to Chinese government transfer from foreign companies that want to do business in China. Eric Rosenbaum of CNBC reported, "One in five North American-based corporations on the CNBC Global CFO Council says Chinese companies have stolen their intellectual property within the last year."[33] Disturbingly, the theft of American intellectual property seems to follow a theme similar to that of China's opioid production. A Washington-based U.S. trade lawyer with 30 years of experience in the field told *Asia Times*, "We can raise tariffs, have high-level meetings, sign memoranda of eternal understanding and eternal friendship, but [China] will not change." He continued, "Their policies favoring *theft of intellectual property on an industrial scale* have contributed to the greatest wealth transfer since the Iranian-Arab creation of the OPEC cartel raised the price of energy in the West."[34]

Emergent Dynamics of Social A2/AD

It is time to seriously assess the changing character of conflict and consider the steps necessary to ensure the American and Western democratic societies succeed in this type of nonkinetic war. Interestingly, the SARS-CoV-2 (COVID-19)

pandemic presents compelling lessons and opportunities to address the threats posed by social A2/AD.

Supply chain challenges were quickly evident as Americans (and presumably others) rushed to buy surgical and N95 masks. This rush to stockpile quickly expanded to toilet paper, cleaning supplies, and bread and other foodstuffs, among other things. This rush for masks (and other medical supplies) impacted the medical and first responder communities—the people who need them most. With approximately 80 percent of medical masks made in China, and the Chinese government consuming and buying all the masks made in China, the United States struggled to manufacture these masks domestically.[35] The U.S. government invoked the Defense Production Act of 1950, a Cold War-era mobilization mechanism, to increase production of existing production capacity while speeding the conversion of other domestic manufacturing facilities.[36] As Americans adapt to the COVID-19 outbreak, there is growing realization that the United States is held hostage by Chinese manufacturing. This extends beyond masks and into other life-critical items, such as pharmaceuticals and the previously mentioned concerns with the U.S. military supply chains.[37] Simply stated, China can—and is—holding lifesaving equipment back from the United States during this outbreak. China's motivation can be debated but not the actions.

COVID-19 is also proving that accurate and up-to-date information at national and global levels is vital. Certainly, the rush to hoard masks and toilet paper derived from a lack of information and understanding that fostered perceptions that led to panic buying and purchasing habits. Despite this, the most compelling information discussion is the narrative being used by China, Russia, and others that the United States is the cause of the virus: "In the case of China, Russia and several other countries, however, misinformation is deliberately being spread by state media to deflect criticisms of their government actions, or lack thereof, and to push the blame onto someone else."[38] Of additional note is the suppression of information, especially concerning China's published time line of the virus outbreak.[39] Chinese foreign ministry official Zhao Lijian took to twitter saying, "CDC was caught on the spot. When did patient zero begin in US? How many people are infected? What are the names of the hospitals? It might be US army who brought the epidemic to Wuhan. Be transparent! Make public your data! US owe us an explanation!"[40] This information battle has included Chinese protests about references to the virus as the Wuhan Virus, with declarations of racism, not just from Chinese officials, but from American outlets as well.[41] The information campaign took on a different dynamic in Italy, where China allocated modest amounts of medical supplies and staff to assist in Italy's COVID-19 response. As Alessandra Bocchi of the *Wall Street Journal* points out,

> these acts are not as altruistic as they might appear. The major-

> ity of ventilators shipping to Italy are from the Chinese company Mindray, which sells its products at a lower price than its global competitors. China has a surplus of medical equipment now that the outbreak appears to have reached its peak there. Demand is rising elsewhere as the virus spreads, so Chinese companies are ramping up production to gain global market share.[42]

When taken together, the socioeconomic and information dynamics created by COVID-19 look like a Chinese social A2/AD strategy in a box. The true opportunity for the United States and our allies is the unmasking of China's nonmilitary levers of power. From supply chain prowess (and corresponding dependency of the United States and others) to its information strategy, the world has seen that China will act rapaciously in its attempt to control both materials and information, using them as weapons to gain power, influence, and market share. The COVID-19 outbreak has—unintentionally—given the world a view of how China might use various mechanisms to coerce others for their advantage—or worse.

Counterstrokes

Besides the COVID-19 example, some recognition of the threat by social A2/AD-like concerns have been made in recent years. Many cyberattacks have been attributed to Russia and China (among others); Russian election tampering is recognized, attributed, and countermeasures have been taken; Chinese unfair business practices and intellectual property theft is common discussion in national security and corporate circles and is a core element of ongoing U.S.-China trade discussions; and the Committee on Foreign Investment in the United States has dramatically increased its China-related agenda items and has been reinforced by the Foreign Investment Risk Review Modernization Act of 2018.

Although significant, these steps need to be expanded in scope and depth, with specific attention paid to nefarious actions designed to compromise the U.S. and Western domestic environments. Recognition that Chinese and Russian information and economic entities are fundamentally agents of their respective governments is paramount. Gazprom, ZTE, and Huawei (among scores of others) meet allegations of government control with a well-rehearsed chorus of denials arguing that they are not agents of the state.[43] Despite these protests, there is little question that—even if not the current "arrangement"—Putin and Xi Jinping have the ability and will to weaponize Russian and Chinese information and economic outputs to support national agendas.[44] On the heels of recognizing the threat presented by social A2/AD, there must be a com-

prehensive, competitive strategy designed to defend against and counter malicious incursions. This approach is characterized by Thomas Mahnken through five features:

> First, it presupposes a concrete, sophisticated opponent. . . . Second, the competitive strategies approach assumes interaction between competitors. . . . Third, the competitive strategies approach acknowledges that the choices competitors have open to them are constrained. . . . Fourth, the competitive strategies approach acknowledges that interaction may play out over the course of years or decades. . . . Finally, the competitive strategies approach assumes sufficient understanding of the competitor to be able to formulate and implement a long-term competitive strategy, a task that requires not only an understanding of what a competitor is doing, but also why he or she is doing it. Effective competitive strategies are predicated on an understanding of a competitor's decision-making process and doctrine.[45]

The prescription that Mahnken details requires a level of study, detail, coordination, resource allocation, and commitment that describe a great challenge for the United States and our allies. As one witnesses the dysfunction of political discourse throughout the Western world, it is difficult to envision a strategy of substance being developed, let alone one that is properly resourced and effectively executed across decades. This challenge comes at a time where continuing resolutions are more frequent than actual budgets, just as debt, deficit, and nondiscretionary spending continue to grow, leaving an ever-shrinking portion of federal outlays to manage the business of government operation and national security.

Social A2/AD attacks are a national security concern. Unlike past threats to national security, the response to social A2/AD incursions is generally not a military one. As it is fundamentally an attack on society, the response must start as a social one. First and foremost, U.S. leadership (from a national level down to to municipal and community levels) needs to realize that they are often the unwitting pawns by furthering divisive rhetoric, functionally serving as this century's "useful idiots." Indeed, none other than former sectary of defense and U.S. Marine Corps general James N. Mattis considers American tribalism as the chief threat to the nation.[46] Economic entities must also recognize that the search for profit can lead to negative implications, as has been illustrated repeatedly. There must be fundamental recognition that a strong *Western* free market economy is to their benefit; short-term thinking for immediate return from growing Chinese markets only digs a deeper hole.[47] These are uncomfort-

able discussions to have with domestic and allied corporations, publics, and present immediate costs. There is risk but risk that is visible. The longer that the "invisible" risk engendered by social A2/AD is denied, the harder it will be to recover—the so-called slow boil of the frog. There are, however, opportunities. Why not combat Huawei's 5G development in Europe through a multinational corporate effort bringing Ericsson, Nokia, and Cisco together to form a high-quality, cost-effective counter to Huawei's advances? Further, as some have suggested that 5G is a national security issue, there should be a discussion of a public-private partnership that removes *some* of the cost and risk from private companies.[48] It is recognized that there are many legal challenges (domestic and international) with such proposals, but creative solutions are necessary as we lurch forward into the twenty-first century's unknowns. A safe information domain is critical to national and individual security and liberty. Considering existing information domain risks, it is easy to envision a much higher cost if authoritarian-directed corporations dominate the international 5G network.

Conclusion

Social A2/AD presents a critical threat to the United States. It is often said that the only way to beat America is from within. The threat presented through the sociopolitcal and socioeconomic means, described as social A2/AD, illustrates the concern. Inherently opaque, social A2/AD is easy to dismiss and difficult to ascribe to any particular source. It must be viewed through a comprehensive lens, not as discrete actions. Social A2/AD recognizes nonmilitary activities designed to deny an adversary the ability or will to act or respond. Social A2/AD creates and exploits social fissures to the point where the target society is so fractured that response is prevented due to internal dynamics that impede, distract, or preoccupy the instruments of governance. The building of these social fissures is multifaceted (economic, informational, illicit) and dynamic, in many ways facilitated by social media, which is an ideal medium for propaganda and disinformation with masses of willing, ignorant, and unwitting propagators. All these pathways are designed to exploit societal vulnerabilities just as they are concealed by counter narratives and legal obfuscation, exploiting and challenging the high standard of legal clarity that is necessary for decisive response. Indeed, ever-threatened Taiwan recognizes the threat presented by social A2/AD: "The main worry of military planners here isn't so much a full-scale amphibious invasion. Rather, they fear the mainland sowing chaos and disrupting the economy as a way of trying to bring Taiwan to heel."[49]

The aggregate effect of the multitude of social A2/AD attacks could be disastrous for the United States and our allies. The combined effect, over time, of unattributed or unrecognized actions—some with the perception of benefit—is irresistible. It is critical that the United States, along with our allies

and partners, realize that China and Russia already act as though they are in great power *conflict* with the United States, using nonmilitary means as their weapons. Many may not wish to believe this the case, but the comprehensive view of Russian and Chinese activities illustrates strong adversarial strategies against the United States. To misappropriate Joseph Heller from *Catch-22*, "Just because [you are not] paranoid doesn't mean they aren't after you."[50]

Endnotes

1. For discussion of Chinese A2/AD, please see Matthew Jamison, "Countering China's Counter-Intervention Strategy," Strategy Bridge, 11 August 2020; and Ngo Minh Tri, "China's A2/AD Challenge in the South China Sea: Securing the Air From the Ground," *Diplomat*, 19 May 2017.
2. Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Knopf, 2007), 269–307.
3. Pease see *Insurgencies and Countering Insurgencies*, Field Manual 3-24 (Washington, DC: Department of the Army, 2014).
4. *National Security Strategy of the United States of America* (Washington, DC: White House, 2017).
5. "The Fulda Gap represented the shortest route (through the cities of either Fulda or Giessen) from the border between East Germany and West Germany to the Rhine River. Throughout the Cold War, North Atlantic Treaty Organization (NATO) and Warsaw Pact military forces remained heavily concentrated in the area. Constant patrols, surveillance, and alerts were carried out along the border, where opposing observation points stood less than 100 yards apart, until the reunification of Germany in 1990." For an explanation of the Fulda Gap during the Cold War, please see "Fulda Gap," Britannica, 19 December 2018.
6. The term *social A2/AD*, although not a one-for-one analog to antiaccess/area-denial, was selected due to its functional utility in inhibiting, or preventing altogether, a nation's ability to respond to an adversarial act. If a country is unable or unwilling to respond, A2/AD has been achieved.
7. Doug Livermore, "China's 'Three Warfares' in Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, 25 March 2018; Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, 30 January 2018; and "US Needs China More Than China Needs the US," IndustryWeek, 6 April 2018.
8. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford, UK: Oxford University Press, 1963), 77.
9. Sun Tzu, *The Art of War*, 84.
10. William M. Mott IV and Jae Chang Kim, *The Philosophy of Chinese Military Culture: Shih vs. Li* (New York: Palgrave MacMillan, 2006), 11.
11. Michael Howard and Peter Paret, eds. and trans., *Carl Von Clausewitz: On War* (Princeton, NJ: Princeton University Press,1984), 485–86, 495–96.
12. Howard and Paret, *Carl Von Clausewitz*, 595–96.
13. Jessica Brandt and Torrey Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing," Brookings, 19 May 2020.
14. Katie Simmons, Bruce Stokes, and Jacob Poushter, "NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid," Pew Research Center, 10 June 2015.
15. Gabriel Collins, *Russia's Use of the "Energy Weapon" in Europe*, Baker Institute for Public Policy Issue Brief (Houston, TX: Rice University, 2017).
16. Kristin Huang, "Why China Buying Up Ports Is Worrying Europe," *South China Morning Post*, 23 September 2018; Eric Reguly, "China's Piraeus Power Play: In Greece, a Port Project Offers Beijing Leverage over Europe," *Globe and Mail*, 7 July

2019; and Joanna Kakissis, "Chinese Firms Now Hold Stakes in Over a Dozen European Ports," NPR, 9 October 2018.

17. Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," *New York Times*, 25 June 2018.
18. See Owen Churchill, "China Hasn't Changed Belt and Road's 'Predatory Overseas Investment Model', US Official Says," *South China Morning Post*, 13 September 2018; Cheang Ming, "China's Mammoth Belt and Road Initiative Could Increase Debt Risk for 8 Countries," CNBC, 5 March 2018; and Jeff Smith, *China's Belt and Road Initiative: Strategic Implications and International Opposition* (Washington, DC: Heritage Foundation, 2018).
19. "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations, accessed 30 March 21; and Nyshka Chandran, "Surveillance Fears Cloud China's 'Digital Silk Road'," CNBC, 12 July 2018.
20. Josephine Ma, "US and China Escalate Huawei Feud in Europe with Warnings to Germany and Poland," *South China Morning Post*, 12 March 2019; and Steve McCaskill, "UK May Reconsider Huawei Ban," TechRadar, 13 August 2019.
21. Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2 vols. (Washington, DC: Department of Justice, 2019).
22. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money* (New York: Institute of Modern Russian, 2014), 6.
23. Douglas Rushkoff, "How We All Became Russia's 'Useful Idiots'," Medium.com, 5 December 2018.
24. Greg R. Lawson, "The Fentanyl Crisis Is a Reverse Opium War," *National Interest*, 26 December 2017; and Vicky Yates Brown Glisson, "America Is in an Opium War for the 21st Century," Real Clear Policy, 22 March 2019.
25. Kathleen E. McLaughlin, "China Killed Prince: Fentanyl Is the PRC's Deadliest Export—and New Promises Probably Won't Stop It," *Foreign Policy*, 7 December 2018.
26. Rob Stein, "Life Expectancy Drops Again as Opioid Deaths Surge in U.S.," NPR, 21 December 2017; and Brennan Hoban, "The Far-Reaching Effects of the US Opioid Crisis," Brookings, 25 October 2017.
27. See also Heather Somerville, "China's Penetration of Silicon Valley Creates Risks for Startups," Reuters, 28 June 2018.
28. Gina Heeb, "Trump's Favorite Scorecard for the US-China Trade War Took a Hit in July," Business Insider, 4 September 2019.
29. Katrina Manson, "Trump Attacks Chinese Control of Military Supply Chains," *Financial Times*, 5 October 2018. Note: comment from *Executive Order 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018) as quoted by Manson.
30. Laura He, "Walmart Is Investing $1.2 Billion in China," CNN, 4 July 2019.
31. *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Washington, DC: Office of the United States Trade Representative, 2018).
32. Sun Tzu, *The Art of War*, 93.
33. Eric Rosenbaum, "1 in 5 Companies Say China Stole Their IP Within the Last Year: CNBC CFO Survey," CNBC, 1 March 2019.
34. Grant Newsham, "U.S. Helpless against China's IP Theft," *Asia Times*, 2 April 2019. Emphasis added by author.
35. Pamela Boykoff and Clare Sebastian, "With No Shipments from China, Medical Mask Suppliers Have to Choose Whom to Supply," CNN, updated 6 March 2020.
36. "DOD Announces $74.9 Million in Defense Production Act Title III COVID-19 Actions," Department of Defense, 4 December 2020.
37. Yanzhong Huang, "U.S. Dependence on Pharmaceutical Products from China," Council on Foreign Relations, 14 August 2019.

38. Joseph Micallef, "Blaming America: China Weaponizes Misinformation About COVID-19," Military.com, 23 March 2020.
39. Please note that while the Axios.com time line begins in December, Chinese accusations point at U.S. soldiers introducing the virus to China in October 2019, indicating awareness well before December. Bethany Allen-Ebrahimian, "Timeline: The Early Days of China's Coronavirus Outbreak and Cover-up," Axios, 18 March 2020.
40. Zhao Lijian, as quoted in Ben Westcott and Steven Jiang, "Chinese Diplomat Promotes Conspiracy Theory that US Military Brought Coronavirus to Wuhan," CNN, updated 13 March 2020.
41. See Joseph Wulfsohn, "CNN Blasted for Now Declaring 'Wuhan Virus' as 'Racist' After Weeks of Network's 'China's Coronavirus' Coverage," Fox News, 12 March 2020; and Marie Myung-Ok Lee, " 'Wuhan Coronavirus' and the Racist Art of Naming a Virus," Salon, 7 February 2020.
42. Alessandra Bocchi, "China's Coronavirus Diplomacy," *Wall Street Journal*, 20 March 2020; and Theresa Fallon, "China, Italy, and Coronavirus: Geopolitics and Propaganda," *Diplomat*, 20 March 2020.
43. Lindsay Maizland and Andrew Chatsky, "Huawei: China's Controversial Tech Giant," Council on Foreign Relations, updated 6 August 2020; Lingling Wei, "China's Xi Ramps Up Control of Private Sector. 'We Have No Choice but to Follow the Party'," *Wall Street Journal*, 10 December 2020; and Macey A. Bos, "Gazprom: Russia's Nationalized Political Weapon and the Implications for the European Union" (master's thesis, Georgetown University, 2012).
44. Tom Mitchell and Xinning Liu, "Chinese Communist Party Asserts Greater Control over Private Enterprise," *Financial Times*, 28 September 2020; Wei, "China's Xi Ramps Up Control of Private Sector"; and Bos, "Gazprom."
45. Thomas G. Mahnken, ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice* (Stanford, CA: Stanford University Press, 2012), 7–8.
46. Jim Mattis, "Jim Mattis: Duty, Democracy, and the Threat of Tribalism," *Wall Street Journal*, updated 28 August 2019.
47. "US Needs China More Than China Needs the US"; and "China and the NBA Are Coming to Blows over a Pro-Hong Kong Tweet. Here's Why," Business Insider, 22 October 2019.
48. Please see *The National Security Challenges of Fifth Generation (5G) Wireless Communication: Winning the Race to 5G, Securely* (Arlington, VA: Intelligence and National Security Alliance Cyber Counsel, 2019).
49. Nicholas Kristof, "This Is How War with China Could Begin," *New York Times*, 4 September 2019.
50. Joseph Heller, *Catch-22* (New York: Samuel French, 1971). The original quote was "Just because you're paranoid doesn't mean they aren't after you."