PERSPECTIVE

Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China

Ainikki Riikonen

Abstract

Technologies for creating and distributing knowledge have impacted international politics and conflict for centuries, and today the infrastructure for communicating knowledge has expanded. These technologies, along with attempts to exploit their vulnerabilities, will shape twenty-first-century great power competition between the US and China. Likewise, great power competition will shape the way China develops and uses these technologies across the whole spectrum of competition to make decisions, disrupt the operational environment, and destroy adversary capabilities.

*****

The 2019 US National Defense Strategy (NDS) cites Russia and the People's Republic of China (PRC) as "revisionist powers" that "want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions."[1] It describes these countries as competitors seeking to use "other areas of competition short of open warfare to achieve their [authoritarian] ends" and to "optimize their targeting of our battle networks and operational concepts."[2] The NDS assesses that competition will occur along the entire spectrum of statecraft from peace to open conflict and that Russia and the PRC will align their foreign policies with their models of governance. If this assessment is correct, and if technology plays a significant role in international politics, then technology will affect the whole spectrum of great power competition and conflict. Information architecture—the structures of technology that collect and relay information worldwide—is innately connected to power projection. The PRC has been innovating in this area, and its expanded information capabilities—and risks to US capabilities—will shape competition in the twenty-first century. Likewise, this competition will influence how the PRC develops and uses communications technologies before, during, and after the threshold of a potential conflict.

The PRC has, in its short 70 years of history, matured from a fledgling postrevolutionary state to an impressive near-peer competitor with a global vision for foreign policy. Xi Jinping has touted a "community of common destiny" as the PRC's foreign policy vision.[3] This concept predates Xi, as do many other Chinese Communist Party (CCP) concepts. While leadership personalities change, the PRC has demonstrated a great deal of continuity in its approach to foreign policy, including an emphasis on strategic information support, information operations, and shaping adversaries' actions below the threshold of open conflict. Even as the PRC grows in its ambitions and capabilities, these concepts can inform an understanding of its activities and the ways it seeks to accomplish its objectives.

The CCP's drive to mitigate existential threats to its leadership underlies PRC foreign and domestic policy and informs PRC efforts to build an international environment open to CCP influence.[4] The CCP envisions an international environment where it can be a guiding force in a "community of common destiny." On its surface, the community of common destiny is about cultivating mutual interests and shared responsibilities between the PRC and other states.[5] In practice, it seeks to generate a "global network of partnerships centered on China" to render the international environment "compatible with China's governance model and emergence as a global leader."[6] For these objectives, the PRC will weaponize connectivity and employ technologies that maximize the CCP's agency over the availability and flow of information. Agency over information architecture is a potent tool for states in understanding and shaping the international environment and in winning both political and military confrontations. The technologies for producing, sharing, and policing knowledge are global and are an area of interest for the CCP before the outset of conflict. Technologies relating to connectivity are equally important for military operations, including global command, control, and communications (C3). This tech-enabled connectivity is part of the backbone of US military superiority, and its vulnerabilities are therefore an area of priority for the PRC. At the heart of the PRC's competition to grow power and expand its influence is access to information, manipulation of the information space, and denial of critical US communications capabilities in the event of a conflict. Current, emerging, and future technologies will be vectors for building and combating state power.

The ability to access and influence information as well as to neutralize an opponent's use of information informs the way technologies will be used in twenty-first-century great power competition and potential conflict. These technologies fit into three broad categories. First are technologies of decision advantage, the tools for understanding the environment and analyzing information to support state decision-making. Second are technologies of disruption, those that can influence the information space to shape the environment and extend state power. Third are technologies of destruction, designed for fighting and winning by paralyzing the enemy. This article overviews relevant PRC doctrine for each technology category to provide context for technology objectives. Next, it offers examples of established technology use cases to ground the discussion of known practices. Finally, it highlights emerging technologies and speculates about future trends.

Technologies of Decision Advantage

Information superiority can create advantages for states by preventing strategic surprise or by folding opponents into the inside of a "decision loop," rendering them prone to outmaneuver. The CCP regards strategic information support as "a key enabler, providing both the avenues and intelligence necessary for well-timed political and operational decisions and action."[7] It has combined technology with institutional innovations to set the foundation for information support in the form of a nascent global surveillance architecture. Building blocks in this foundation are embedded within a myriad of PRC foreign policy projects, business practices, and legal regimes.

The PRC is already a formidable cyber actor, able to exploit software vulnerabilities to find information relevant to its political objectives. It is also becoming adept at inserting itself into supply chains and states' networks. In part, it uses development projects and business practices to do so. New technologies like fifth-generation wireless networks (5G) and artificial intelligence (AI)-enabled facial recognition will only increase the PRC's access to information over time, as long as the PRC maintains and grows access to international networks. Expansion of technological capabilities and consequent deployment of those technologies will further the PRC's ability not just to hunt and exfiltrate specific data but to vacuum it up en masse from a wider variety of sources.

Fusion Deployment and Development Projects

The PRC systematically "fuses" categories to render state-backed projects as dual use; development projects could create doorways for state surveillance.[8] Companies might not want to work for the state and, of course, government connections with companies are not evenly distributed or monolithic. But the blurring of public and private entities and several new PRC laws create challenges for understanding whether companies are independent from the state. These laws and practices create backdoors for the PRC to access information through companies working abroad.

One type of fusion comes in the form of opaque private company ownership. The recent Huawei controversy has raised questions about the intentions of Chinese companies operating abroad, how these companies fit into the PRC's foreign policy, and whether Chinese companies can be independent from the state. Huawei—an ostensibly private company known for its phones, undersea cables, and 5G projects—has prompted a litany of analysis addressing these questions. A scholarly investigation of Huawei's ownership concludes that the company is one percent owned by CEO Ren Zhengfei and 99 percent owned by a "trade union committee."[9] The researchers infer that Huawei "may be deemed effectively state-owned."[10] Ashley Feng in *Foreign Policy* adds that assessing which companies work for the CCP is also challenging because of internal party committees and the PRC's recent intelligence and cybersecurity laws.[11] Legal regimes give the government the ability to request assistance from private companies without recourse for companies to push back. Article 7 of the PRC's National Intelligence Law, for example, states, "Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work."[12]

Government ownership, party committees, and legal requirements create risks for companies' independence. These practices and regulations are a feature, not a bug, and create pathways for the PRC to request access to companies' work and data. This year, tech giants Alibaba and Tencent elected to withhold data from a government-backed financial credit score system, but time will tell how long their refusal might last.[13] Lack of transparency makes Chinese vendors of information technologies difficult to vet. These factors pose significant risks for countries that adopt Chinese-built information infrastructure.

Information infrastructure projects increasingly feature in foreign policy projects as well, especially development-related projects like the Belt and Road Initiative (BRI). Through the Belt and Road, and components of it like the Digital Silk Road, the PRC offers development projects with competitive pricing or financing backed by the Chinese state. The BRI has been criticized in recent years for transitioning from "pocketbook diplomacy" to "debt-trap diplomacy" where states unable to pay for projects give up some sovereign element like ports or territory for lease. The PRC has used the debt-trap approach not only for physical infrastructural projects but also for digital infrastructure, as in the case of Nigeria's telecommunications satellites. The state-owned enterprise (SOE) China Great Wall Industry Corporation built a pair of telecommunications satellites for the Nigerian government but, instead of charging $550 million for them, acquired a stake in Nigerian Communications Satellite (NIGCOMSAT) Limited.[14] NIGCOMSAT Ltd. is owned by Nigeria's Federal Ministry of Communications Technology and manages Nigeria's satellite communications. PRC information-based development projects pose risks to host nation governments' control of telecommunications assets.

The technologies built by companies like Huawei and the China Great Wall Industry Corporation are not necessarily built for spying, but PRC institutional practices create risks for the confidentiality of user data traveling along this information infrastructure. The way the PRC combines technology with institutional innovations and foreign policy projects could manifest in the building blocks of a global surveillance architecture.

Established Initiatives

Historical instances demonstrate how aggressive, diverse, and systematic the PRC approach is to accessing information—especially information connected with political objectives—through technical means. Some instances follow well-established methods; for example, FireEye identified APT40 (advanced persistent threat) as a PRC-sponsored cyber operation using a seemingly typical attack life cycle.[15] APT40 targeted actors involved in either South China Sea disputes or possessing advanced maritime technology. FireEye assessed that "APT40's emphasis on maritime disputes and naval technology ultimately support China's ambition to establish a blue-water navy."[16] While APT40 is only one of many APTs attributed to the PRC, the case illustrates the PRC's worldwide reach and firm grasp of well-established cyber methods for obtaining privileged information important to state objectives during peacetime and conflict.

The PRC's breaches of information infrastructure exploit vulnerabilities in networks as well as supply chains. The PRC is adept at penetrating software and hardware supply chains and supply of management personnel (wetware). Hardware supply chain vulnerabilities can exist almost anywhere in the chain of custody of equipment. In the case of the new

African Union headquarters, Huawei installed network hardware components in the building, which the PRC consequently hacked.[17] Whether Huawei played an active role is unclear, but the case does little to instill confidence in the company. Digital supply chain attacks work through common trusted software and updates—software patches may themselves be an attack vector. In 2017, cybersecurity researchers discovered that CCleaner, a common computer security tool, had been manipulated—possibly by a PRC-backed actor—so that updates would install backdoors into users' devices.[18] The CCleaner attack infected thousands of devices for the purpose of gaining entry into only a few dozen belonging to technology companies. In terms of wetware, a recent *Wall Street Journal* investigation uncovered a case of Huawei employees tasked with managing telecommunications networks spying on dissidents on behalf of African host nation governments.[19] While this Huawei case does not implicate the Chinese government, if Huawei is not able to deny state requests for access, it demonstrates that host nations are not necessarily the only ones that can spy on their citizens. These situations show the risks posed by PRC entities' involvement anywhere in putting together or maintaining systems, whether software, hardware, or wetware.

Emerging Examples

More recently, the PRC is leveraging its infrastructure-building approach to potentially expand its network penetration capabilities, including amassing new kinds of data. Technologies that increase risks for surveillance include 5G and AI-enabled technologies like facial recognition. These technologies are likely to be deployed as part of development projects such as digital infrastructure upgrades and Smart City initiatives.

Fifth-generation mobile networks add a layer of complication to the telecommunications surveillance problem. As 3G enabled smartphones to send e-mails and 4G enabled media streaming, 5G will enable new applications by transmitting even greater amounts of data to travel at high speed and volume. The applications of 5G are wide-ranging, from the industrial Internet of Things (IoT) to autonomous vehicles. The 5G connections could transmit sensor data from these user devices to cloud-based computing or even cloud AI systems, which in turn could operate devices or perform analysis for use during military operations. Huawei's push to install 5G networks around the world has created a firestorm for policy makers concerned about foreign espionage, and rightly so.[20] The volume of data that will be transmitted via this foundational technology would be a goldmine for any state actor. The data would include not only person-to-person communications but also information produced as part of industrial processes. High-fidelity industrial data could also be a valuable source of economic intelligence.

Smart City initiatives employ a suite of interconnected sensors and objects that pose a surveillance risk as well, especially the security component of Smart Cities often called "safe city." Surveillance cameras connected with facial and other recognition systems mean that individuals can be automatically tracked anywhere, anytime. Ongoing initiatives include Ecuador's ECU911 project and Venezuela's Integrated Monitoring and Assistance System (SIMA), both built by SOE China National Electronics Import and Export Corporation (CEIEC).[21] These projects include the installation of thousands of surveillance cameras combined with networking equipment, data centers, and emergency response command centers. The Venezuela case is cause for elevated concern given the country's *carnet de la patria* or fatherland card initiative, built by ZTE, that will connect citizens' IDs with government services including voter registrations.[22] If politically sensitive data from the fatherland card initiative is ever connected with SIMA, Venezuela's poor governance will be compounded by increased state capacity for control. SIMA and the fatherland card projects are built and managed by Chinese companies; the Venezuelan government may not be the only entity with access to citizens' centralized data. PRC law requires that companies—like ZTE, CEIEC, and Huawei—building Smart City initiatives cooperate with the state when requested.

Future Trends

The PRC has expanded its access to information, and infrastructure projects and new technologies will only continue to expand that access. Smart City initiatives and 5G deployment, by installing sensors and building the means of transporting sensor and other data, could create a firehose of information available upon state request. This massive amount of data may have limited value for a state due to finite resources for processing and analysis, but artificial intelligence could diminish this limitation. Machine learning, a method of AI, is adept at identifying patterns in big data and will likely refine the PRC's ability to sift through and interpret it. AI can make sense of the mass or hunt for specific information within it. The PRC is already testing AI applications for surveillance domestically in Xinjiang, which some observers have called a "surveillance lab."[23] Those efforts are likely to expand over time in geography, scope, and depth.

Facial, voiceprint, gait, and other types of biometric recognition made possible by AI can pick a person out in a crowd and will make hiding from the PRC difficult. The state has subjected the Uyghur ethnic minority population to biometric data collection and has used it to enforce control. The state uses facial recognition at checkpoints to limit where individuals may and may not travel; some wanted persons are even detained on sight.[24] Voiceprint recognition, developed by companies like iFlytek, can identify participants in eavesdropped phone calls.[25] The PRC is already beginning to aggregate surveillance information on platforms like the Integrated Joint Operations Platform (IJOP) in Xinjiang and the Golden Shield and Sharp Eyes projects elsewhere in the country.[26] Aggregating data in the IJOP is labor intensive at present, but data collection and processing may become more automated in the future.[27] Advances in speech recognition, natural language processing, and keyword detection could also allow the government to track the content of individual conversations or monitor public opinion at scale. In terms of where all this data might go, in addition to tracking and trend analysis, the People's Liberation Army (PLA) and PRC Ministry of Foreign Affairs have expressed interest in AI tools for decision-making.[28] They will need data to support these initiatives. If the PRC has access to foreign surveillance cameras, telecommunications networks, and sensing equipment, it may be able to use AI to process and analyze vast quantities of data to gain decision advantage over other states.

Implications for Great Power Conflict

Competition for better decision-making tools already drives technology investments in the PRC and the US. The US intelligence community's (IC) Augmenting Intelligence Using Machines (AIM) Initiative envisions an IC that can "provide decision advantage at machine speed" by using AI to "clos[e] the gap between decisions and data collection."[29] Part of the Defense Advanced Research Projects Agency's (DARPA) AI Next Campaign looks to develop machines that can work with humans to "facilitate better decisions in complex, time-critical, battlefield environments."[30] The PRC is investing in capabilities to assist decision-making on and off the battlefield as well. A researcher from the Chinese Academy of Sciences disclosed that the Ministry of Foreign Affairs is working with a system for vetting foreign investment projects.[31] The system, still under development, supposedly accesses PRC government databases to perform geopolitical environment simulations. With regard to open conflict, one researcher from the PRC's Army Command College anticipates an eventual "singularity" where machine-speed decision-making overtakes the human mind's ability to keep pace with the speed of operations on the battlefield.[32] With increased worldwide connectivity and the deployment of myriad sensors, states are acquiring access to exponentially more data. AI can leverage that data to generate decision advantage in great power competition and conflict.

The challenges these emerging technologies pose for the PRC's foray into decision advantage—sensors, 5G, and AI-enabled processing—come not from the technologies themselves but the PRC policies that generate surveillance risks. The PRC's mode of fusion deployment through ambiguous private-public relationships poses severe hazards for states, especially as the PRC integrates digital and information infrastructure into its development projects. By the time states go looking for a smoking gun, it may be too late. The United States ought to work with allies and partners to build risk-based frameworks to assess and mitigate surveillance risks from PRC-built technologies, especially where massive data flows are involved.

Technologies of Disruption

Information superiority creates advantages for operating in an environment, but the environment itself can be disrupted and shaped. This shaping can be used to influence "an adversary's decision-making through actions below the threshold of outright war" and for "setting the terms of conflict in peacetime."[33] The CCP regards information operations as part of "discourse power" or "the power to control perceptions and shape narratives that advance Chinese interests and undermine those of an opponent."[34] It frames its voice in the world, and its building of that voice, as "discourse power."[35] Discourse constitutes knowledge and shapes governance, and it can be manipulated in part by determining who is permitted to speak and about what. It is about cultivating a dominant narrative, in part by promoting certain perspectives and censoring others. This narrative can be general, such as to foster perceptions of the CCP, or specific, such as election interference to drive specific political outcomes. This discourse power forms a part of military strategy as well, according to PLA documents from as early as 2003.[36] Peter Mattis states that "the whole point of pushing that kind of propaganda out is to preclude or preempt decisions that would go against the People's Republic of China."[37] Information superiority and information support thus play a significant role in great power competition below the threshold of conflict.

The CCP's goal for using discourse power is to create an external environment amenable to the "Chinese Dream of national rejuvenation." Well-known initiatives include the United Front, which the CCP regards as its third "magic weapon," in addition to open conflict and party building.[38] The United Front works by coopting or neutralizing people and organizations that could undermine CCP rule or authority. Discourse power lies in the CCP's ability to determine who may or may not speak as well as what is said. Methods can be psychological, public opinion–based, or legal in nature.[39] The PRC is well practiced in shaping or manipulating the information environment. It employs some technical tools now and is likely to expand its abilities as other technologies advance.

Established Initiatives

The PRC boasts one of the most advanced censorship capabilities in the world. The "Great Firewall" is designed to block web content considered politically sensitive, such as the Tiananmen Square massacre and, more recently, the Hong Kong protests. Censorship is not limited to the "public" areas of the internet like websites but is prolific on social media platforms and messaging apps like Weibo and WeChat. Increasingly, WeChat users have reported that automated censorship catches private messages and even images.[40] The PRC is well established in its efforts to censor sensitive contributions in the public and private information space.

Discourse power also involves strengthening a point of view through promotion or mass. Here, the CCP employs the *wumao dang* or "50 Cent Party" to spread positive sentiments about the CCP. The 50 Cent Party so far seems composed of real human people that react to anti-CCP online content by flooding the comments with pro-PRC sentiment. Research from Harvard University indicates that the 50 Cent Party approach varies from the Russian "troll farm" method. First, the 50 Cent Party does not rely on bots but a large volume of people.[41] Second, its content coopts or deflects conversations to push for pro-CCP unity in lieu of driving political division or sowing outrage. But as the PRC forays its online initiatives to more international audiences, it may take a more targeted approach to drive specific political objectives.

The PRC has started to target its online information operations to drive political outcomes and to respond to international and off-mainland crises. In the lead-up to Taiwan's 2018 elections, the PRC released fabricated news designed to undermine Taiwanese citizens' faith in their government. One story widely circulated on social media claims that Taiwanese travelers stranded at Osaka's Kansai International Airport during a typhoon were offered transport by PRC officials if they self-identified as Chinese.[42] The story stoked outrage in Taiwan. It may have culminated in the suicide of a Taiwanese diplomat in Japan and influenced certain election outcomes. But social media operations on platforms not controlled by the PRC, particularly Western platforms, still seem to be maturing. Twitter, Facebook, and YouTube exposed "coordinated inauthentic behavior" on their platforms in response to the Hong Kong protests.[43] Analysis suggests that the PRC hastily acquired these social media accounts but had not matured them as part of a sophisticated long-term operation. Whether the haste was caused by a lack of foresight into the protests or was due to the PRC's relatively new entry into this open social media space is unclear.[44]

The PRC has been influencing the online information space by driving volume—dialing certain perspectives up or down through promotion or censorship—and by seeding disinformation to drive political objectives. Its approach, while not yet on par with Russia's efforts, is likely to become more sophisticated with time.

Emerging Examples

The PRC is beginning to use structural and infrastructural approaches to shape the information space. Structural approaches condition actors to adopt certain narratives or self-censor by incentivizing and deterring certain behaviors. Infrastructural approaches work by deploying the information infrastructure necessary to disseminate information.

Structural approaches are powerful because they link discourse with incentives, and they work by using accounting systems to fuse them together. One example is the corporate "social credit" system, a digital accounting method that assigns positive values to certain behaviors and negative values to others.[45] Companies that accumulate positive values by aligning with CCP narrative maintain access to the PRC market. Those that do not risk their access. The PRC has had success so far with manually issued warnings, for example around companies' regard for the One China policy. A number of airlines and fashion companies ran afoul of the CCP by listing Taiwan as a country on their websites or by showing China on a map without including Taiwan.[46] The corporate social credit system goes a step further than manual threats; it will require companies to submit their data for inspection, allowing the PRC to have deeper access into their activities and more efficient screenings for state policy and narrative compliance.[47] The system creates a more stringent way to use the "lure of the Chinese market—to stifle discussion."[48] This tool will be especially powerful given the high visibility of large companies and their ability to monitor the conduct of their employees as a second-order effect. Cathay Pacific's response to the recent Hong Kong protests—it has fired employees—demonstrates the power of a warning from the PRC.[49] By making companies' behavior easier to surveil, the corporate social credit system will gradually improve the efficiency of structure-based incentives for policing dissent.

The PRC has used information infrastructure development projects to increase its ability to disseminate information. As with the installation of technologies that could be used for surveillance, the PRC leverages a fused approach to build the means to purvey its message. This approach blends development projects with state initiatives and organizations. The 10,000 Villages project is a development initiative for upgrading analog television to digital in African states.[50] StarTimes, a private company, received millions of dollars in funding from the Export-Import Bank of China for these upgrades. As of 2019, StarTimes completed upgrades in 30 African states and boasts some 10 million subscribers. PRC state media gained advantage through this initiative because StarTimes offers cheaper pricing for television packages, including PRC state-run channels, than other outlets.[51] By using development projects to establish the technological means of transmission, the PRC enables its state media to expand its overseas reach at the expense of other media outlets. As Chinese state media lacks editorial independence and is required to toe the party's line, development projects that elevate state media serve to increase the CCP's overseas discourse power.

Future Trends

The next generation of PRC information operations will likely include microtargeting and synthetic media, also known as deepfakes. These technologies can tailor messaging to individuals and increase the believability of disinformation. While already in use to a limited degree, such technologies are likely to become more pervasive. Chinese social media platforms already use microtargeting to a degree, as do Western-based platforms. Mictrotargeting is the use of algorithms to optimize content recommendations for a specific audience.[52] This technology can be used for commercial purposes in the case of product or content recommendations on social media. It can also be used for social manipulation as in the case of the Cambridge Analytica scandal around the 2016 US presidential elections, in which Russia proved especially adept at manipulating algorithmic processes of content distribution to promote social divisions. PRC social media platforms benefit the state because of the PRC's agency to control their content through the promotion of state media and censorship. The role of algorithms to automate content distribution is increasing, however, according to Leiden University's Florian Schneider. He terms this capability "digital nationalism," "a process in which algorithms reproduce and enforce the kind of biases that lead people to view the nation as a major element of their personal identity and as the primary locus of political action." Schneider adds that digital nationalism is "special in that these existing biases are further strengthened and made to seem natural by virtue of the pervasive personalisation processes, preference filters, and group bubbles that have come to define communication on the commercial internet."[53]

This digital nationalism in the PRC is mostly a domestic phenomenon, but the PRC's app ecosystem is growing and gaining more international users. TikTok, owned by the Beijing-based company ByteDance, has enjoyed a meteoric rise. In 2018, it was the fourth most downloaded nongame app in the world—trailing Facebook but beating Instagram—and has been installed by 1.3 billion users worldwide.[54] TikTok is not subject to the same content restrictions as Douyin, its sibling app for mainland Chinese users. In the wake of the Hong Kong protests, observers have begun to point out what appears to be a conspicuous lack of protest content or any other content considered sensitive by the CCP. The *Washington Post* reports that ByteDance calls TikTok "a place for entertainment, not politics, and said its audience gravitates there for positive and joyful content as a possible explanation of why so few videos relate to sensitive topics as the protests in Hong Kong."[55] Yet the platform does boast plenty of American political content.[56] ByteDance has been opaque about how it moderates its platform, but recently leaked documents indicate how content sensitive to the CCP might be banned under broader rules.[57] TikTok's approach to politically sensitive content might indicate how other Chinese-owned apps could operate in international settings. Like Western social media platforms including Facebook and Twitter, TikTok uses recommendation algorithms, but its content rules are more likely to be state-regulated than those of its non-PRC counterparts. ByteDance cultivates "stars" on Douyin; if it begins to choose stars on TikTok as well, the messages they purvey will be something to watch in future.[58] If more users come to PRC-run platforms, these platforms recommend content to users, and the state dictates what type of content platforms can carry, then the state can begin to extend microtargeting beyond its borders.

AI could supercharge disinformation through synthetic media. Synthetic media, also known as deepfakes, consists of realistic audio or visual media created by a type of AI system called a generative adversarial network (GAN). Reports about deepfakes used for malign purposes are beginning to emerge. In June 2019, AP News reported on a potential espionage recruitment operation involving synthetic media. [59] A LinkedIn profile named "Katie Jones" connected with senior US government officials and think tank experts, but the account was for a person who does not exist—the account sported a GAN-generated profile picture to fool connections. This operation was not attributed to the PRC, but the country is known for recruiting over LinkedIn. Just as AI can create images of imaginary people, it can also mimic real humans—whether to deceive the general public or specific individuals. In 2018, opponents of Gabon's president Ali Bongo attempted a coup after the release of a video speculated to be a deepfake of the president.[60] In early 2019, criminals defrauded a United Kingdom–based company of $243,000 by using AI-manipulated audio to pose as leadership of its parent company over the phone.[61] These tools are becoming more widely available, and researchers are racing to create detection systems. If a state has agency over a social media platform or television station, however, it may choose what content to show or filter. Deepfakes will likely be more effective on platforms where they are intentionally deployed at scale as propaganda or disinformation.

Implications for Great Power Conflict

The CCP has been building its presence in the information space by increasing its ability to control the flow and content of information. This effort has been rooted in its approach to technology. Established initiatives include exerting governance via censorship over domestic online platforms, building positive narratives on the CCP via mass posting of propaganda, and distributing disinformation in neighboring states to stoke outrage. Emerging initiatives increase the CCP's agency to distribute information by building and controlling the physical technological infrastructure needed to do so.[62] These initiatives also increase the CCP's discourse power by binding the CCP's economic weight to incentives for narrative compliance. In the future, as CCP-regulated platforms start to collect more company and user data, they could also employ microtargeting to automatically optimize delivery of content in ways that feel natural to consumers. Synthetic media will further complicate matters; the state could use it to create audio and visual media that support the version of reality it wants people to believe.

Technologies of Destruction

Just as states can build technologies to access information or manipulate information, they can destroy adversaries' information channels and ability to communicate. The US military's global information architecture enables the United States to perform operations almost anywhere on the globe. Elements that connect this architecture include fiber, cable, microwaves, shortwaves, and satellite nodes.[63] In addition to organizational and personnel communications, networks are critical for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and for the positioning, navigation, and timing (PNT) capabilities that enable the US military's signature precision strike systems.[64] A history of the 1990 Gulf War written by China's Academy of Military Science states that "the Gulf War has led to a world-wide military transformation characterized by the shift from mechanized warfare to information warfare."[65]

In the event of a conflict, the PRC is not likely to take on the United States in a "fair fight" but will employ an offset strategy.[66] If the PRC cannot win without fighting, then it will look to win by "decapitation and paralysis rather than outright destruction."[67] This approach underpins the PLA theory of victory, which is to disrupt or destroy the enemy's operational system through "systems destruction warfare."[68] Once paralyzed, the enemy "loses the will and ability to resist."[69] The PLA has identified information architecture—especially C3—as the US military's center of gravity. In the event of a conflict, the PLA will attack key points and nodes in US information architecture with kinetic or nonkinetic means.

US reliance on these systems—especially space assets—is only growing. In the 2003 invasion of Iraq, 68 percent of munitions used satellites, a significant increase from 10 percent during the 1990 Gulf War.[70] The US way of war demonstrated in Desert Storm informed the PRC's military strategy, and the PRC has accordingly formed its institutions to counter US information systems. These efforts include "informatized" warfare and long-range strike capability to hold C3 assets at risk.[71] The PLA established the PLA Rocket Force (PLARF) as a fully-fledged armed service to fulfill this strike capability.[72] A recent PLA reorganization included the new Strategic Support Force (SSF) that folds the PLA cyber, space, and electronic warfare efforts into one organization.[73] Cyber, space, and electronic warfare are ultimately all about information flows—the key target for paralysis in a fight.

Current Risks

If the PRC is already building information support and information operations as key parts of shaping battlefield conditions, then it is likely taking other measures as well to tilt the field in its favor. Supply chain risks have been a source of consternation for the US Department of Defense because the manufacture of technology, especially components of information technologies, is typically global.[74] Supply chain risks occur when actors along a technology's chain of custody cannot be verified as trustworthy. Supply chain attacks can happen to software supply chains, as with the CCleaner attack, or in hardware supply chains as during semiconductor manufacturing. The Department of Defense has made efforts to secure its supply chains through initiatives like the Trusted Foundry program.[75] As an example of hardware supply chain issues, a United Kingdom–based company that manufactures circuit boards for the F-35 Joint Strike fighter was discovered to have been acquired by Fastprint, a company based in Shenzhen.[76] The British company Exception PCB manufactures the bare-board component of the circuit board and was assessed not to pose an immediate risk, but the case illustrates the challenges of accounting for all the actors that touch complex platforms. Supply chains are becoming more globalized over time and will pose an ongoing challenge for the integrity of US platforms.

These efforts to secure supply chains are imperfect not only because of the global nature of supply chains, but because of the US military's integration with partners and allies. Despite a growing reliance on space systems, NATO does not own satellites. Instead, NATO requests access to "products and services" and uses a mix of military, civilian, and commercial space assets made available through memoranda of understanding among the allies. According to a Chatham House report on satellite, cyber, and supply chain vulnerabilities, NATO's reliance on commercial companies for military purposes creates vulnerabilities whether physical, personnel, or procedural.[77] The PRC has incentives to act now on these vulnerabilities where it can because cyberattacks need network access to deliver payloads; state actors require persistence to keep attack options open.[78] The SSF was designed for "peacetime-wartime integration" to facilitate the transition from cyber reconnaissance and attack.[79] Even in peacetime, the SSF is probably exercising persistence and conducting reconnaissance on critical information infrastructure, especially in the parts where that infrastructure seems most vulnerable. Satellites pose risks because of supply chain concerns and because civilian interaction with them increases the attack surface.

Data on the Battlefield

Fighting under "informatized" conditions means dismantling adversary information systems and also possessing superior capabilities. For the PLA, "a truly joint force must be able to control the information environment through information-networked forces."[80] This theory of operations involves understanding the environment, making decisions, and acting swiftly. Components include sensors, network equipment, analysis tools, and weapons that can perform at high speed. This suite of sensors and connected objects could manifest as an "Internet of Battlefield Things" (IoBT). The IoBT could potentially connect to cloud services by way of 5G networks; the PRC is already piloting 5G-connected devices for border control in Jilin province on the North Korea border.[81] The PLA is investing in a number of platforms to support battlefield communications and decision-making. The integrated command platform is designed to facilitate communication to multiple moving units to quickly adapt to the battlespace.[82] The platform is supported by digital databases and command automation tools in what the PLA terms "intelligentized" command and decision-making.[83] From there, the PLA has invested in hypersonic missiles and directed energy weapons to minimize the time between target identification and attack.[84] Sensors, networks, decision-making tools, and fast weapons support the PLA's ambition to observe, orient, decide, and act more quickly than its adversaries.

Future Hazards

The opening salvo of conflict will likely target information flows for operations, C4ISR and firepower elements, and operational systems and networks.[85] The SSF will employ cyber, electronic warfare, and counterspace capabilities to destroy, disrupt, or delay the functioning of US information systems. Cyberattacks could exploit logic bombs placed during peacetime operations or other pre-positioned payloads. The PRC would not be the first to engage in this practice. During the Iran nuclear negotiations, the US planted malware into Iranian military networks as an insurance measure in case the talks failed.[86] The operation, Nitro Zeus, stopped short of activating the payload that would have disabled those networks. Future network vulnerabilities might also impact US allies or partners, especially if they accept Huawei as a vendor for 5G. Cybersecurity company Finite State found poor practices from Huawei within its firmware.[87] Whether these vulnerabilities are "bug doors" or backdoors, they would leave states' economies open to coercion if new industrial IoT is dependent on Huawei 5G networks. Network disruption via cyber means could impact the information backbones of both military and economic systems.

Where cyberattacks use the language and logic of computers to disrupt networks, electronic warfare is about controlling the physical electromagnetic spectrum to achieve desired effects. Effects can include degradation of adversaries' connections or outright destruction of systems. Jamming works, for example, by overpowering the signals a platform is looking to receive. Directed energy, such as high-powered microwaves, uses a concentration of electromagnetic waves to dazzle or physically damage systems. Both techniques have successfully disabled unmanned aerial vehicles by disrupting their connections or physically damaging them.[88] As the technology advances, it will be able to strike other platforms at light speed. To target satellites in particular, the PLA is developing a number of measures that use directed energy and other means. The US Defense Intelligence Agency anticipates that the PRC will have lasers capable of countering low Earth orbit satellites by 2020 and geostationary orbit satellites by the mid-2020s.[89] In addition to directed energy weapons, some threats to satellites are kinetic, such as antisatellite missiles and orbital threats (satellites) designed to damage or interfere with other satellites.[90]

Implications for Great Power Conflict

An assessment of the PRC's technological investments and strategy—and the way they target US vulnerabilities—can inform American approaches to technology and war fighting. DARPA launched its Mosaic warfare concept to disaggregate sensors, decision-making nodes, and effects platforms to boost resiliency.[91] It also seeks to eliminate concentrated points of failure from communications networks. Scholars in the defense community have argued that the US may need an entirely new "way of war" altogether to adapt to new competitive and technological landscapes.[92]

The US and PRC understand that their forces will operate in environments where communications are degraded or denied, even as both countries invest in shielding, cognitive electronic warfare offense and defense, and other resiliency measures. Degraded networks could prompt increasing reliance on autonomous systems that can operate on the edge. These systems will create new implications for conflict escalation dynamics, operational concepts, ethics, and strains of technological competition.

Conclusion

From Smart Cities, to deepfakes, to systems destruction warfare, the technologies that connect, manipulate, or disconnect nation-states will lie at the heart of great power competition. The development and deployment of technology are not linear but are shaped by norms, governance, and the choices of the actors that interact with and through that technology. The PRC's projects and initiatives do not delineate cleanly between public and private or between development and defense. This fusion poses a unique challenge to US national security and foreign policy as it will require creative interagency solutions. In developing strategy and communicating with US allies, partners, and like-minded states, agencies will need to use a risk assessment approach. The US will need to find ways to empower states to adopt the technologies that connect people, make cities more efficient, and increase security without taking on undue risk should the competition escalate or lead to war. The innovation behind the PRC's growing access to information comes not from the 5G or other technology platforms but from the PRC's institutional practices and foreign policy. The PRC is shaping the information space by increasing the reach of platforms it can extend its governance over. It is grooming the battlespace by organizing its military around what it has identified as an American vulnerability and has shaped its technology innovation around those principles. The PRC's approach to twenty-first-century great power competition and conflict stretches across the whole spectrum from accessing information, to shaping the information space, to denying adversaries' information systems in a conflict. Competition thus involves technologies of decision advantage, disruption, and destruction, along with the institutional practices that embed them.

Ainikki Riikonen

Ms. Riikonen is a research assistant for the Technology and National Security Program at the Center for a New American Security (CNAS). Previously, she worked at the Near East South Asia Center for Strategic Studies supporting security cooperation seminars. She holds a degree in international relations from the University of St Andrews and is a master's degree candidate at Georgetown University's Security Studies Program.

Notes

[1] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), 2, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[2] *Department of Defense,* 3.

[3] Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies," *Texas National Security Review* 2, no. 1 (November 2018), https://tnsr.org/.

[4] The CCP maintains a monopoly on power in the PRC and is deeply embedded across PRC state and nonstate institutions. The government is subordinate to but not necessarily always synonymous with the CCP.

[5] Jacob Mardell, "The 'Community of Common Destiny' in Xi Jinping's New Era," *The Diplomat,* 25 October 2017, https://thediplomat.com/.

[6] Tobin, "Xi's Vision for Transforming Global Governance."

[7] John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives no. 13 (Washington, DC: National Defense Uni-

versity Press, October 2018), 45, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

8. Tobin, "Xi's Vision for Transforming Global Governance."

9. Christopher Balding and Donald C. Clarke, "Who Owns Huawei?," SSRN, 17 April 2019, 2, http://dx.doi.org/10.2139/ssrn.3372669.

10. Balding and Clarke, 2.

11. Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy,* 7 February 2019, https://foreignpolicy.com/.

12. Samantha Hoffman and Elsa Kania, "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws," *The Strategist*, 13 September 2018, https://www.aspistrategist.org.au/.

13. Yuan Yang and Nian Liu, "Alibaba and Tencent Refuse to Hand Loans Data to Beijing," *Financial Times*, 18 September 2019, https://www.ft.com/content/.

14. Felix Onuah, Chijoke Ohuocha, and Adrian Croft, "Nigeria Agrees $550 Million Satellite Deal with China," Reuters, 3 January 2018, https://www.reuters.com/.

15. Fred Plan et al., "APT40: Examining a China-Nexus Espionage Actor," *Threat Research* (blog), *FireEye Blogs*, 4 March 2019, https://www.fireeye.com/.

16. Plan et al.

17. John Aglionby, Emily Feng, and Yuan Yang, "African Union Accuses China of Hacking Headquarters," *Financial Times*, 29 January 2018, https://www.ft.com/content/.

18. Andy Greenberg, "The CCleaner Malware Fiasco Targeted at Least 18 Specific Tech Firms," *WIRED*, 20 September 2017, https://www.wired.com/.

19. Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *The Wall Street Journal*, 15 August 2019, https://www.wsj.com/articles/.

20. Elsa Kania, "The Much Ado about Huawei Continues," *Lawfare*, 19 December 2018, https://www.lawfareblog.com/.

21. Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," *Foreign Policy*, 9 August 2018, https://foreignpolicy.com/; and Ryan Mallett-Outtrim, "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets," *Venezuelanalysis.com*, 27 November 2013, https://venezuelanalysis.com/.

22. Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," Reuters, 14 November 2018, https://www.reuters.com/.

23. Dake Kang, "Backlash at Chinese University Shows Limits to Surveillance," Associated Press, 20 November 2018, https://www.apnews.com/; and Zak Doffman, "Beyond 5G: Huawei's Links to Xinjiang and China's Surveillance State," *Forbes*, 25 April 2019, https://www.forbes.com/sites/zakdoffman/2019/04/25/huawei-xinjiang-and-chinas-high-tech-surveillance-state-joining-the-dots/#eb87d2acd52e.

24. Darren Byler, "China's Hi-Tech War on Its Muslim Minority," *The Guardian*, 11 April 2019, https://www.theguardian.com/.

25. Isobel Cockerell, "Inside China's Massive Surveillance Operation," *WIRED*, 9 May 2019, https://www.wired.com/.

26. Edward Schwarck, "Behind the Golden Shield: China Reforms Public Security Intelligence," *China Brief* 17, no. 16 (December 2017), https://jamestown.org/; and Oiwan Lam, "With 'Sharp Eyes,' Smartphones and TV Sets Are Watching Chinese Citizens," *Hong Kong Free Press*, 8 April 2018, https://www.hongkongfp.com/.

27. "China's Algorithms of Repression," *Human Rights Watch*, 1 May 2019, https://www.hrw.org/.

28. Elsa B. Kania, Adjunct Senior Fellow, "Chinese Military Innovation in Artificial Intelligence," Testimony before the U.S.-China Economic and Security Review Commission, Hearing on Trade, Technology, and Military-Civil Fusion, 7 June 2019, 3–4, https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence.pdf; and Stephen Chen, "Artificial Intelligence, Immune to Fear or Favour, Is Helping to Make China's Foreign Policy," *South China Morning Post*, 30 July 2018, https://www.scmp.com/.

29. Office of the Director of National Intelligence (ODNI), *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (McClean, VA: ODNI, January 2019), 1–2, https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

30. Defense Advanced Research Projects Agency, "AI Next Campaign," accessed October 2019, https://www.darpa.mil/work-with-us/ai-next-campaign.

31. Chen, "Artificial Intelligence."

32. Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Washington, DC: Center for a New American Security, November 2017), https://www.cnas.org/.

33. Costello and McReynolds, *China's Strategic Support Force*, 45.

34. Costello and McReynolds, 28.

35. Elsa Kania, "The Right to Speak: Discourse and Chinese Power," *Center for Advanced China Research*, 27 November 2018, https://www.ccpwatch.org/.

36. Louisa Lim and Julia Bergin, "Inside China's Audacious Global Propaganda Campaign," *The Guardian,* 7 December 2018, https://www.theguardian.com/.

37. Lim and Bergin.

38. Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities under Xi Jinping" (paper presented at the conference on "The Corrosion of Democracy under China's Global Influence" for Taiwan Foundation for Democracy, Arlington, Virginia, September 16–17, 2017), https://www.wilsoncenter.org/sites/default/files/magic_weapons.pdf, 7.

39. Kania, "The Right to Speak."

40. Jeffrey Knockel and Ruohan Xiong, "(Can't) Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats," *The Citizen Lab*, 15 July 2019, https://citizenlab.ca/.

41. Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (2017): 484–501.

42. Keoni Everington, "Beijing-Based PTT Users Spread Fake Osaka Airport Bus Story," *Taiwan News*, 17 September 2018, https://www.taiwannews.com.tw/.

43. Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from China," Facebook Newsroom, 19 August 2019, https://newsroom.fb.com/news/2019/08/removing-cib-china.

44. Jake Wallis, "China's Information Warfare Darkens the Doorstep of Twitter and Facebook," *The Strategist,* 21 August 2019, https://www.aspistrategist.org.au/.

45. Samantha Hoffman, "Social Credit," *Australian Strategic Policy Institute*, 28 June 2018, https://www.aspi.org.au/.

46. Brenda Goh and John Ruwitch, "China Cracks Down on Foreign Companies Calling Taiwan, Other Regions Countries," *Reuters*, 12 January 2018, https://www.reuters.com/.

47. European Union Chamber of Commerce in China, *The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors* (Beijing: European Union Chamber of Commerce in China, 2019), 13, https://www.sinolytics.de/wp-content/uploads/2019/08/Sinolytics_The-Digital-Hand-How-Chinas-Corporate-Social-Credit-System-Conditons-Market-Actors.pdf.

48. Louisa Lim, "China Is Exporting Its Tiananmen Censorship, and We Are All Victims," *Foreign Policy*, 4 June 2015, https://foreignpolicy.com/.

49. Ezra Cheung and Tiffany May, " 'Big Brother' in the Sky: Cathay Pacific Workers Feel China's Pressure," *The New York Times*, 11 September 2019, https://www.nytimes.com/.

50. Jenni Marsh, "How China Is Slowly Expanding Its Power in Africa, One TV Set at a Time," *CNN Business News*, 24 July 2019, https://www.cnn.com/.

51. Lim and Bergin, "Inside China's Audacious Global Propaganda Campaign."

52. Richard Fontaine and Kara Frederick, "The Autocrat's New Tool Kit," *The Wall Street Journal*, 15 March 2019, https://www.wsj.com/.

53. Émilie Frenkiel, "China's Digital Nationalism and the Hong Kong Protests: An Interview with Florian Schneider," *Books and Ideas*, 5 September 2019, https://booksandideas.net/.

54. "The Incredible Rise of TikTok – [TikTok Growth Visualization]," *Influencer Marketing Hub*, 30 April 2019, https://influencermarketinghub.com/.

55. Drew Harwell and Tony Romm, "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience," *The Washington Post*, 15 September 2019, https://www.washingtonpost.com/.

56. Caroline Haskins, "TikTok Can't Save Us from Algorithmic Content Hell," *Vice,* 31 January 2019, https://www.vice.com/.

57. Alex Hern, "Revealed: How TikTok Censors Videos That Do Not Please Beijing," *The Guardian*, 25 September 2019, https://www.theguardian.com/.

58. John Herrman, "How TikTok Is Rewriting the World," *The New York Times*, 10 March 2019, https://www.nytimes.com/; and Hans Tung and Zara Zhang, "8 Lessons from the Rise of Douyin (Tik Tok)," *technode, 15* June 2018, https://technode.com/.

59. Raphael Satter, "Experts: Spy Used AI-Generated Face to Connect with Targets," *Associated Press*, 13 June 2019, https://www.apnews.com/.

60. Drew Harwell, "Top AI Researchers Race to Detect 'Deepfake' Videos: 'We Are Outgunned,'" 12 June 2019, https://beta.washingtonpost.com/.

61. Catherine Stupp, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," *The Wall Street Journal*, 30 August 2019, https://www.wsj.com/.

62. Echo Huang, "China Is Building Its New Silk Road in Space, Too," *Quartz*, 18 June 2018, https://qz.com/.

63. Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), 101, https://www.rand.org/.

64. Paul Scharre, "The US Military Should Not Be Doubling Down on Space," *Defense One*, 1 August 2018, https://www.defenseone.com/; and Beyza Unal, *Cybersecurity of NATO's Space-based Strategic Assets* (London: Chatham House, Royal Institute of

International Affairs, July 2019), https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf.

65. Lt Gen David A. Deptula, USAF, Retired, and Heather R. Penney, with Maj Gen Lawrence A. Stutzriem, USAF, Retired, and Mark A. Gunzinger, *Restoring America's Military Competitiveness: Mosaic Warfare* (Arlington, VA: The Mitchell Institute for Aerospace Studies, Air Force Association, September 2019), 14, http://docs.wixstatic.com/ugd/a2dd91_29e021b297f2492ca7f379d31466ad0c.pdf.

66. Christopher M. Dougherty, *Why America Needs a New Way of War* (Washington, DC: Center for a New American Security, June 2019), 1, https://www.cnas.org/.

67. Costello and McReynolds, *China's Strategic Support Force*, 45.

68. "China's Competitive Strategy: An Interview with Robert O. Work," *Strategic Studies Quarterly* 13, no. 1 (2019): 2–11, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-1/Work.pdf; and Robert O. Work and Greg Grant, *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics* (Washington, DC: Center for a New American Security, June 2019), 7, https://www.cnas.org/.

69. Engstrom, *Systems Confrontation and System Destruction Warfare,* 15.

70. Unal, *Cybersecurity of NATO's Space-based Strategic Assets*, 9.

71. Deptula and Penney, *Restoring America's Military Competitiveness*, 15.

72. Work and Grant, *Beating the Americans at Their Own Game*, 11.

73. Work and Grant, 8; and Derek Grossman, *Envisioning a "World-Class" PLA: Implications for the United States and the Indo-Pacifi*c (Santa Monica, CA: RAND Corporation, 2019), 11, https://www.rand.org/.

74. Tim Hwang, "Computational Power and the Social Impact of Artificial Intelligence," *SSRN Electronic Journal*, 23 March 2018, http://dx.doi.org/.

75. Government Accountability Office, *Trusted Defense Microelectronics: Future Access and Capabilities Are Uncertain*, GAO-16-185T (Washington, DC: GAO, 28 October 2015), 2, https://www.gao.gov/assets/680/673401.pdf.

76. Zak Doffman, "U.S. and U.K. F-35 Jets Include 'Core' Circuit Boards from Chinese-Owned Company," *Forbes,* 15 June 2019, https://www.forbes.com/sites/zakdoffman/2019/06/15/chinese-owned-company-supplies-electronics-on-u-s-and-u-k-f-35-fighter-jets/#5193df5a25c0.

77. Unal, *Cybersecurity of NATO's Space-based Strategic Assets*, 8.

78. Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press, 2016), 41–42.

79. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (Spring 2018): 109, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf?ver=2018-07-31-093713-580.

80. Grossman, *Envisioning a "World-Class" PLA*, 3.

81. Minnie Chan, "China to Use 5G Technology to Tackle Flow of Refugees, Smuggled Goods over North Korean Border," *South China Morning Post*, 8 April 2019, https://www.scmp.com/.

82. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Arlington, VA: Department of Defense, 2 May 2019), 63–64, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

83. Kania, *Battlefield Singularity*.

84. Work and Grant, *Beating the Americans at Their Own Game*, 11–12; and Lora Saalman, "China's Calculus on Hypersonic Glide," Stockholm International Peace Research Institute, 15 August 2017, https://www.sipri.org/.

85. Engstrom, *Systems Confrontation and System Destruction Warfare*, x.

86. Buchanan, *The Cybersecurity Dilemma,* 32.

87. Finite State, *Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.*, FS-SCA1 (Columbus, OH: Finite State, June 2019), 2, https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf.

88. Brian Barrett, "The Marines' New Drone-Killer Aces Its First Real World Test," *WIRED, 22* July 2019, https://www.wired.com/; and Michael Peck, "Did a Turkish Combat Laser Shoot Down a Chinese Drone," *The National Interest*, 1 September 2019, https://nationalinterest.org/.

89. Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC: Defense Intelligence Agency, 2019), 20, https://www.dia.mil/Military-Power-Publications/.

90. Defense Intelligence Agency, 20.

91. Deptula and Penney, *Restoring America's Military Competitiveness*, 3.

92. Dougherty, *Why America Needs a New Way of War*.