July 2023

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

TIMOTHY M. BONDS

Keeping the World Close

How Taiwan Can Maintain Contact with Allies, Supporters, and Its Own People If Attacked

Over the past several decades, the People's Republic of China (PRC) has labored to isolate Taiwan internationally and bind Taiwan's future to China's. In his speech marking the 100th anniversary of the Chinese Communist Party (CCP), Xi Jinping, chairman of the CCP and the PRC's supreme leader, directly linked China's rejuvenation to reunification with Taiwan.[1] Subsequently, Xi said that China would "strive for peaceful reunification with the greatest sincerity and the utmost effort," but explicitly reserved all "measures necessary"—including the use of force—to wrest control of Taiwan.[2]

Although reunification could be a peaceful continuation of current efforts, the PRC poses a clear and growing military threat, as demonstrated by its increasing air and naval capabilities, heightened amphibious exercises, and military shows of force around Taiwan's periphery. U.S. Under Secretary of Defense for Policy Colin H. Kahl thinks China is likely to increase pressure on Taiwan but is not likely to invade over the next two years.[3] At the same time, Admiral Mike Gilday, Chief of Naval

RAND
CORPORATION

Operations, has warned that U.S. forces must be prepared for a Chinese invasion of Taiwan before 2024.[4]

The U.S. Department of Defense (DoD) has identified several approaches that the PRC could take to wrest control of Taiwan.[5] The PRC could

- establish a blockade of Taiwan and threaten to fire on any ships and aircraft attempting to land without China's permission
- invade the outlying Kinmen, Matsu, and Penghu islands and use them to tighten its military grip over the main island of Taiwan
- launch a full-scale air, sea, missile, special, and strategic forces assault on Taiwan with the goal of swiftly defeating Taiwan's military and the resistance of the Taiwanese people.

As part of these approaches, the PRC could utilize special operations teams and missile strikes to eliminate Taiwan's leadership while conducting sabotage, cyberattacks, and disinformation campaigns as part of a broad-gauge psychological warfare campaign to confuse and demoralize Taiwan's defenders.

Common to all these approaches is the People's Liberation Army (PLA) concept of "cognitive domain operations."[6] In short, the PLA seeks to control the information domain before and during a conflict, establish the dominant narrative, and put sufficient psychological pressure on its opponents to cause them to quit or surrender. China has likely watched Russia's invasion of Ukraine closely and noted President Volodymyr Zelenskyy's skillful use of media to communicate the urgency of Ukraine's plight and the depth of its determination to prevail.[7] Through its words and images, Ukraine has stiffened the resolve of its people and elicited sympathy and support from Western powers.

For example, immediately after the Russian invasion in 2022, Zelenskyy was reported to have refused a U.S. offer to evacuate, saying instead that "I need ammunition, not a ride."[8] Tweets by the Ukrainian Embassy in the United Kingdom and videos from Zelenskyy himself in the first few days of the war told the Ukrainian people and the world that Ukraine would fight and not surrender. President Zelenskyy spoke of the need to maintain close contact with his countrymen, saying that "to lose contact with . . . people is to lose control completely . . . the Russians told them that Ukraine doesn't exist anymore, and some people even began to believe it."[9]

If the PLA attacks Taiwan, it would likely be determined to make the Taiwanese leadership mute—unable to rally their own people or appeal to Western nations for support. In practical terms, this could include severing Taiwanese communications at home and with the outside world. The PLA could conduct operations to cut undersea cables, jam satellites and wireless communications, and destroy data centers and core networks. If successful, Taiwan's ability to command its military forces, communicate with its people, and coordinate with international allies could be entirely disrupted. Then, the only voices the Taiwanese people would hear would come from the PLA. The PLA could introduce its own, false narrative of the war; claim that the Taiwanese leadership and its allies had abandoned the nation; and inject fake versions of Taiwan's leadership, all without any Taiwanese rebuttal.

But, through Ukraine's experience, Taiwanese officials have seen the power of keeping in close contact with outside supporters and their own people. President Tsai Ing-wen has stated that Taiwan needs to have good leadership and, as the Ukrainian people have shown, the determination to defend itself.[10] This is likely part of the motivation for Audrey Tang, Taiwan's digital minister, to develop a backup for Taiwan's internet infrastructure in case of attack or natural disasters. Tang said, "[t]he experience of Russia's invasion of Ukraine . . . showed that the whole world can know what is happening in real time."[11] Therefore, Tang plans to build "digital resilience for all" in Taiwan.[12]

In the larger sense, building "digital resilience" should include reinforcing the access of officials and public figures to communications networks, securing essential databases, developing alternative communications pathways to international audiences, and improving the physical and cybersecurity of terrestrial infrastructure. I will explore each of these topics in this Perspective.

How Might China Attack Taiwanese Information Networks?

The PRC is reported to have gathered intelligence on nearly 300,000 points of interest (POIs) on Taiwan.[13] This includes 550 POIs containing the locations of such network infrastructure as cable landing stations, internet service provider facilities, and mobile telephone facilities. Another 2,397 POIs detail the location of local, provincial, and government offices. These facilities could be targeted in advance and could be destroyed by rocket artillery or captured by special operators emerging on the first day of the attack.

Abbreviations

4G	fourth generation of cellular communications
5G	fifth generation of cellular communications
AM	amplitude modulation
DoD	U.S. Department of Defense
FCC	Federal Communications Commission
FM	frequency modulation
GEO	geostationary orbit
GHz	gigahertz
GPS	Global Positioning System
LEO	low earth orbit
MEO	medium earth orbit
MHz	megahertz
MSP	managed service provider
MUOS	Mobile User Objective System
NASA	National Aeronautics and Space Administration
PLA	People's Liberation Army
PRC	People's Republic of China
SATCOM	satellite communications
T2C2	transportable tactical command communications
TDRS	Tracking and Data Relay Satellite
TV	television
UHF	ultra high frequency
VHF	very high frequency
VSAT	very small aperture terminal
WGS	Wideband Global SATCOM System

How Could Taiwan Make Its Home Networks More Resilient?

Recent advances in fifth generation (5G) mobile communications, networks, and cloud data systems could help Taiwan build more-resilient networks in advance of an attack. I review some potential approaches in each of the topical categories below.

Terrestrial Cellular Systems

Most Taiwanese residents will depend on their mobile cellular service for information and communications during a crisis or war. More than 84 percent of the Taiwanese people use their mobile devices to access the internet.[14] The main island is ringed by more than 80,000 cellular base stations, so users are well covered on roadways and in populated areas.[15] Eighty percent of the service used is fourth generation (4G), while 20 percent of the population uses 5G service provided by roughly 20,000 5G base stations.[16] The Taiwanese government is subsidizing an effort to deploy more than 56,000 5G bases by 2026.[17]

But terrestrial cellular systems are susceptible to physical destruction, and cellular macro-towers are prominently placed to achieve maximum coverage. Finding and destroying macro-towers would be an early task for PLA infantry and combat engineers.

It would be harder to find and destroy the micro- and pico-cells that are an increasing share of cellular base stations. But all cellular base stations have a fiber-optic backhaul connection to core telecommunications networks. And core network internet service providers, server farms, and the main and local offices of the major Taiwanese cellular providers would likely be priority targets for PLA special operations.

The 5G networks that Taiwan is growing might help reduce this vulnerability. The 5G standard enables self-contained edge networks with databases and computers colocated with base stations. This feature was established to reduce the time delay (or latency) within local networks, such as those in smart factories or automated traffic control networks. These same features enable edge networks to function even if their connection to the core network is disrupted by enemy action.

As an example, Ukraine engaged Amazon Web Services to deploy Snowball devices to help secure data on local networks. Snowballs are ruggedized compute and storage hardware that can be used as transfer devices or can be combined with miniature supercomputers to make up a local micro data center. These local clouds should be able to host both control plane functions and user plane functions and thereby operate as independent edge networks.

Such independent edge networks might be very useful in defending Taiwan. For example, they could connect forward artillery observers—or automated sensors—with rocket artillery batteries firing from hidden locations in the central mountains of Taiwan. Or they could enable workers in government offices, commercial warehouses, or factories to coordinate operations even after backhaul networks are disrupted. Local edge networks might also sustain the morale of Taiwanese civilians by connecting urban neighborhoods or clusters of mountain defenders.

At some point, most edge users will want to connect with other edge networks or the broader world. Artillery batteries will need to request supplies, government agencies will need to communicate with the Taiwanese people, commercial operations will need to move goods, and people will need to receive information from their leaders or the broader world (or maybe talk with family members located in a different edge network). If the terrestrial backhaul networks have been disrupted, these users will need another backbone link.

Ukraine has used satellites to link disconnected local networks. In one case, the Russian attack on Irpin, northwest of Kyiv, took all of its 24 cell towers offline, with most of them severely damaged.[18] Electrical power and fiber-optic connections for the cellular network were also severed. Two days after Ukrainian forces took the city of Irpin back, engineers installed mobile base stations to restore cellular services and hooked them to Starlink terminals to connect with the rest of Ukraine.

A similar alternative could be arranged in Taiwan by linking very small aperture terminals (VSATs) to 5G base stations in a variety of locations. As the terrestrial connections to core networks are severed, groups of 5G base stations could form edge networks and use VSATs to connect them to one another.

It is also important to note that Ukraine has used its mobile networks as an integral part of its effort to resist the Russian invasion. This includes degrading Russian military communications, gathering intelligence on Russian troop movements, and targeting Russian units and leaders.[19] These notable successes were the result of an information strategy to effectively employ the mobile network.

All the measures described here rely on electrical power to function. The PLA would almost certainly hit electrical generation early in a conflict. Taiwan will need to prepare backup power sources for its edge and core networks.

To make terrestrial cellular systems more resilient, Taiwan should take the following actions now:

- Increase deployment of 5G networks with the routers and computers needed to form edge networks.
- Equip groups of 5G base stations with VSAT terminals to connect them to one another and to core networks.
- Prepare to deploy mobile base stations equipped with satellite terminals to replace damaged base stations.
- Build an information strategy that employs the mobile network to gather intelligence, deceive enemy leaders, target invading forces, and keep connected with international partners and audiences.
- Deploy mobile generators to maintain electrical power at critical communication nodes.

> The PLA would almost certainly hit electrical generation early in a conflict. Taiwan will need to prepare backup power sources.

Messages, News, and Social Media Broadcasts over the Airwaves and the Internet

The fixed facilities supporting government messaging, news, and social media are likely to be among the first targets of invading forces. Taiwan has five major wireless TV networks and 186 wireless radio operators.[20] Over-the-airwaves broadcast operators do not require terrestrial cables to reach their listeners, but their antennas, the stations controlling them, and the studios producing news programs are all fixed and vulnerable to physical attack.

Similarly, news and social media transmitted over cable systems or the internet rely on a complex infrastructure of internet service providers, data centers, and server farms to enable their operations. The locations of Google, Facebook, and other media facilities are less publicized than those of traditional news outlets, but their approximate locations can be found online. Presumably, the PRC intelligence services have had time to build a more complete map.

> Government officials, media personalities, reporters, and internet influencers will be familiar sources of information and encouragement for the Taiwanese people in times of crisis and war.

Even more important than these fixed facilities are the people who represent the public face of Taiwan's government and free press. Government officials, media personalities, on-scene reporters, and internet influencers will be familiar sources of information and encouragement for the Taiwanese people in times of crisis and war. In the age of YouTube, Twitter, and Instagram, it should be possible for these individuals to report and broadcast from a nearly infinite variety of ad hoc locations. The Taiwanese government has most likely prepared contingency locations for its officials and their staff to continue operations during wartime. The government should also help the news media and private influencers prepare alternative places to produce and broadcast their reports and should assist their movement on warning of attack.

To maintain communications from familiar government spokespeople, media figures, and social media influencers, Taiwan should take the following actions now:

- Develop and maintain several alternative ways to communicate with the Taiwanese public and supporting audiences around the world.
- Establish multiple contingency locations from which Taiwan's civilian leadership and news media can communicate in wartime.
- Deploy mobile generators to maintain electrical power at critical communication sources.

Essential Data

Every nation depends on vast amounts of data for its day-to-day functions. These data include government records, banking transactions, the operating data of corporations, and the personal records of every individual. These data are vital to the daily activities of governments, banks, and industry in wartime as well as peacetime, so they must be safeguarded while also remaining available for regular use.

The importance of data to the modern nation might be analogous to the importance of gold a century ago. In World War II, the national banks of Poland, France, Belgium, and the United Kingdom shipped their gold reserves to Canada and the United States to secure them from capture by Nazi Germany.[21] In an analogous way, Ukraine moved its government, education, and banking services data offshore after Russia's invasion.

Russian cyberattacks in 2015 and 2016 prompted Europe and the United States to work closely to improve cyber defenses in Ukraine and across Western nations.[22] One such practice was to build good offline backups and use multiple cloud vendors, such as Amazon Web Services, Microsoft Azure, and Oracle. Three days after Russia invaded, Ukraine was preserving critical data in the cloud.[23]

It might be necessary for the government, industry, and people of Taiwan to preserve their essential databases in a similar way. At a minimum, crucial databases could be duplicated to prevent their loss due to enemy action. It might be possible to continue running these databases in Taiwan while regularly updating the offshore data repositories to keep them current. In some cases, it might be possible to host data operations completely offshore.

There would be some costs involved in moving data operations offshore. Government agencies might be able to negotiate prices they are willing to pay in advance of an attack, but businesses and individuals might be more cost-sensitive and, therefore, unwilling to preserve these data ahead of a conflict.

Some risks also exist. During World War II, the United Kingdom moved its gold to the National Bank of Canada, which is owned by and under the control of the Canadian government. There is no similar national data bank available to keep and operate Taiwan's data, so Taiwan would be entrusting its public and private data to private corporations. And Taiwan's government will want to be a bit careful about their messaging to the Taiwanese people about moving data offshore, so as not to create an unintended air of imminent abdication or collapse of the Taiwanese government.

In addition, for reasons I will discuss below, access to offshore data clouds will be restricted by the available communications capacity. For example, if submarine cables are severed, users in Taiwan are likely to have much lower-capacity satellite connections instead. Lower-capacity connections could suffice to make incremental changes to offshore databases (rather than transmitting them in their entirety), but appropriate protocols would need to be established ahead of time.

Ultimately, it might be better to accept the costs and difficulties involved in keeping and accessing essential data offshore rather than risk their destruction or theft as a result of a PRC attack.

To preserve key databases, Taiwan should take the following action now:

- Prepare offshore enclaves for key databases in Japan, the United States, or other overseas sanctuaries.

How Could Taiwan Strengthen Its International Communications?

Taiwan's submarine cables are inherently vulnerable to attack. Although the massive communications capacity of modern submarine cables cannot be readily replaced, recent developments in wireless communications can help. In the following sections, I briefly review submarine cables and then assess the role that airborne systems and satellite constellations could play in strengthening Taiwan's international communications.

Submarine Cables

Experts have described Taiwan's dependence on submarine cables as an "Achilles' heel."[24] At the time of this writing, Taiwan was connected to the outside world via 12 submarine cables, and the 13th and 14th cables are projected to be completed in 2024.[25] These cables handle the bulk of human and machine communications to and from Taiwan, and social media companies, such as Facebook and Google, directly own portions of several cables. The data capacity of the latest submarine fiber-optic cables is 200 terabits per second: a truly gargantuan capability that cannot be readily replicated using wireless technologies.[26]

All these cables are vulnerable to breakage by fishing vessels, ship anchors, or sabotage, as demonstrated by notable cable failures in the Red Sea and other locations.[27] Damaged cables can be repaired or replaced, though it might take several weeks even if the specialized ships and spare cable lengths are available. Furthermore, these operations are normally conducted in calm weather conditions and not under fire from adversaries; it is therefore likely that damaged cables would remain out of service until combat operations have ended.

Cable systems might be most vulnerable at the point at which they leave the water and connect to terrestrial fiber networks. Industry literature lists seven main cable landing stations at four distinct locations in Taiwan.[28] Some appear to be more precisely located than others, although all cable landing stations are likely to be on the collection list of Chinese intelligence. Once located, these cable landing stations are easy targets for rocket artillery or demolition teams.

It might be possible to construct duplicate cable landing stations at alternative locations. However, given that these stations must connect to a lengthy submarine cable, it is doubtful that these alternative locations could be effectively hidden; even if they were, the cables themselves would still be vulnerable and not easily replaced (as discussed earlier).

Although the massive communications capacity of modern submarine cables cannot be readily replaced, recent developments in wireless communications can help.

Therefore, Taiwan will need alternatives to maintain a connection with supporting nations and sympathetic people around the world, even though these alternatives will necessarily operate at a much reduced data rate. I will address the potential capabilities and vulnerabilities of airborne and satellite systems in the following sections.

To partially compensate for the loss of submarine cables in crisis or wartime, Taiwan should take the following actions now:

- Develop alternatives to submarine cables for the highest-priority government agencies and military units.
- Make provisions for businesses and individuals to access cable substitutes on an as-available basis; this should include protocols to prioritize their access and usage.

Airborne Systems

Several systems have been developed to put cellular base stations in the air, where they can see users at greater ranges unblocked by obstacles on the ground. These systems include unmanned aircraft systems and Google's free-flying Loon, a high-altitude balloon designed to provide a wireless network in remote areas.

Loon was discontinued by Google in 2021, but the equipment from the program might still exist in storage somewhere, and the people who developed it might be able to resurrect it. Loon consisted of a series of interconnected balloons operating at an altitude of 20 km. These balloons could be launched from the nations that would operate them or launched at a distance and then gradually drifted to their intended operating areas. The balloons relied on air currents, which circulate in differing directions depending on altitude, to push them to their destination.[29]

Google's Loon subsidiary had discussed deployments of 30 or more balloons to provide coverage for remote regions. Each balloon had a 4G base station with an uplink antenna to receive transmissions from user devices, a downlink to communicate with ground stations, and a crosslink to enable it to communicate with neighboring balloons. Standard user devices up to 25 km away could uplink to the balloon; greater ranges might be possible if users were to employ higher-powered devices with directional uplink beams. For the backhaul, crosslinks among the balloons have demonstrated the ability to travel 1,000 km.

It might be possible, then, for balloons operating between Taiwan and Okinawa to form a communications link with ground stations on Okinawa, the main Japanese Islands, and perhaps even South Korea. Once communications reach ground stations at these locations, they can be sent by submarine cables well away from Taiwan to any point on the globe. (Although these cables could potentially be severed by the PLA too, doing so would be a bigger task than damaging the cables coming only from Taiwan and would risk widening the war to all of Taiwan's neighbors.)

These balloons would face several potential threats. Balloons at stratospheric altitudes would be easily detected by signal intelligence systems within line of sight. This would make them targetable by jammers, fighter aircraft, and surface-to-air missiles.

The Chinese surveillance balloon that penetrated U.S. and Canadian airspace in early 2023 and was subsequently shot down provides an interesting case study.[30] DoD first stated that it detected the balloon after it entered U.S. airspace off the Aleutian Islands. This implies that the balloon was picked up by ground-based radars operating on U.S. soil (or, perhaps, airborne radars operating in U.S. airspace) and not space-based systems, which would have seen the balloon before it entered U.S. airspace. Balloons operating between Taiwan and Okinawa would be offset from Chinese ground radars by several hundred kilometers, which might make them harder to detect. Although China might be able to find these balloons with airborne radars, this would expose these aircraft to U.S. air and naval forces operating in the area. In any event, Chinese airborne radar aircraft would likely be busy with higher-priority operations over Taiwan itself.

The second interesting point from the Chinese surveillance balloon intercept is that it was shot down by an F-22 aircraft armed with an AIM-9 missile. The F-22 was at an altitude of 58,000 feet when it fired the AIM-9, and the balloon was at an altitude of between 60,000 and 65,000 feet when struck. The choice of a short-range AIM-9 with a heat-seeking sensor, rather than a longer-range AIM-120 with a radar seeker, might be significant. On one hand, the mission demonstrated a one-shot, one-kill success capability, indicating that Loon-like communications balloons would be vulnerable to advanced fighters operating with short-range missiles. On the other hand, if PLA fighters needed to close within a short distance to kill each balloon, they too would become vulnerable to attack by U.S. air and naval forces operating in the area. (One could imagine the balloons acting as decoys to lure PLA aircraft into a fight a long way from their bases.)

Alternatively, Taiwan might be able to acquire unmanned aerial vehicles, such as EQ-4B, to serve as airborne communications nodes. Three EQ-4B aircraft serving in this role have recently been retired by the U.S. Air Force in favor of a manned platform. These, or similar aircraft, might be useful for portions of Taiwan's connectivity needs.[31]

If operating from Taiwanese bases, these aircraft would be vulnerable to preemptive attacks by PLA aircraft or missiles. These aircraft could be based farther away—for example, in the Philippine Islands—but more aircraft would then be required to enable continuous coverage. The Philippine Islands and U.S. bases on Guam or Okinawa would also be vulnerable to preemptive missile strikes, and these aircraft would remain vulnerable in the same way as the balloons discussed earlier.

Because balloon and aircraft communication systems are vulnerable to Chinese fighter aircraft, the operational use of these systems would have to incorporate continuing equipment refresh to replace combat losses. Ultimately, the total data rate passed through these systems will be limited by the numbers of systems Taiwan would be able to keep aloft.

It is not clear that Taiwan should invest in airborne systems, but if Taiwan wanted something quick and with little development expense, it could take the following actions now:

- Negotiate with Google to bring Loon out of storage and conduct an extended test of the technology, including a dozen or so balloons (to form chains and provide spares) and two ground stations in Taiwan.
- Negotiate with Japan and the Philippine Islands for additional ground stations to be placed on their territory, preferably linked to submarine cables.
- Explore the feasibility of linking with Guam using a chain of balloons.

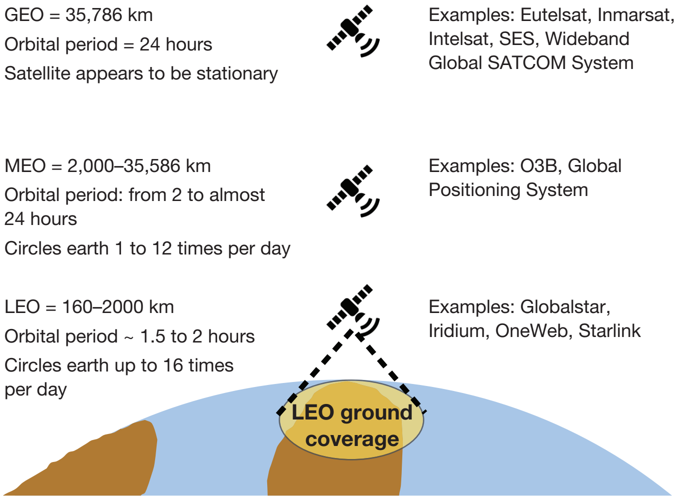
Satellites

For an island nation like Taiwan, satellites are the most feasible—albeit much less capable—substitute for submarine cables. Satellites cannot replace the enormous capacity of submarine cables, but they can connect high-priority fixed and mobile users, including government leaders, private citizens, and military units and the organizations and industries that support them. But this option is complicated, so I will discuss satellite communications (SATCOM) in a bit more depth.

There are several very different kinds of commercial and government SATCOM systems that cover Taiwan, each with its own advantages and drawbacks. These satellite-specific characteristics are especially important when assessing the ability of these systems to resist Chinese physical or electronic attacks. Also, because these systems carry orders of magnitude less data than submarine cables, Taiwan will need a carefully crafted strategy to cope with these capacity limits.

FIGURE 1

Satellite Orbits and Exemplar Systems



GEO = 35,786 km

Orbital period = 24 hours

Satellite appears to be stationary

Examples: Eutelsat, Inmarsat, Intelsat, SES, Wideband Global SATCOM System

MEO = 2,000–35,586 km

Orbital period: from 2 to almost 24 hours

Circles earth 1 to 12 times per day

Examples: O3B, Global Positioning System

LEO = 160–2000 km

Orbital period ~ 1.5 to 2 hours

Circles earth up to 16 times per day

Examples: Globalstar, Iridium, OneWeb, Starlink

SOURCES: Features information from Johnson, *Medium Earth Orbits*; European Space Agency, "Types of Orbits."

Types of Satellite Systems

Both government-owned and commercial communications satellites cover Taiwan and the air and sea lanes surrounding it. Communications satellites owned by the United States and other governments are mostly in geostationary orbit (GEO), while commercial communications constellations operate in low earth orbit (LEO), medium earth orbit (MEO), and GEO (Figure 1).

Satellites in GEO are placed at an altitude of 35,786 km above the earth's surface. At this altitude, they orbit the earth once every 23 hours and 56 minutes—precisely the same amount of time that it takes the earth to make one full rotation about its axis. For this reason, satellites in GEO appear to be stationary from any given spot on the earth's surface. This makes GEO a particularly popular orbit for communications satellites, especially for users (such as the average home and business) that want to use fixed dishes that do not have to track a satellite's movement across the sky. In addition, satellites in GEO are so high that they can view a large portion of the earth from a single orbital position (or slot). In fact, just three evenly spaced satellites in GEO could view the entire globe (except for the north and south polar regions), with some overlap.

Traditional SATCOM providers, such as Eutelsat, Inmarsat, Intelsat, and SES, have constellations in GEO.

Some military systems, such as the Wideband Global SATCOM System (WGS), are also located in GEO. One key disadvantage of GEO is that SATCOM users experience a time lag of about one-half second. Although this lag is imperceptible for receiving a TV broadcast, it can be distracting for a two-way telephone conversation.

Satellites in LEO operate in orbits between 160 km and 2,000 km.[32] Beginning with Iridium and Globalstar in 1998, several constellations of LEO communications satellites have emerged. The most famous of the recent entrants is Starlink, owned by SpaceX; it is being followed by OneWeb, with additional constellations planned to follow. If the full constellation promised by Starlink, OneWeb, Kuiper, and others are realized, thousands more LEO satellites will be available over the next ten years, greatly enhancing SATCOM availability and capacity.

The advantages of LEO include a short travel time between ground stations, which greatly reduces the time delay in voice and video communications, and that lower-power user terminals can be used, which reduces the size and power required for user devices.

The principal disadvantage of LEO is that satellites in LEO move rapidly relative to a user on the surface. This means that many satellites are required to provide continuity of coverage: Each satellite hands over calls or data connections to the next satellite arriving over the user. Furthermore, the low altitude of LEO satellites limits the size of the ground coverage of each satellite, necessitating a large number of orbital planes to cover the entire globe. While a satellite in GEO can see more than one-third of the earth's surface from one fixed orbital slot, satellites in LEO typically concentrate on spots with a radius (or major axis) of a few hundred kilometers. Finally, although the lower altitude of the satellites reduces the power requirements of user terminals, those terminals must be able to track a rapidly moving succession of satellites. This is relatively easy for Iridium and Globalstar terminals because they use a frequency (L-band) that can employ omnidirectional antennas, but it is a more significant challenge for such satellites as Starlink and Oneweb, which use the higher-frequency Ku-band: Their user terminals employ a sophisticated phased-array that can electronically track satellites without needing a mechanically steered antenna.

In between LEO and GEO is MEO, defined as everything between 2,000 km and just 200 km below GEO (35,586 km). Satellites in these orbits also move relative to earth but more slowly. Some of the more prominent inhabitants of this space are the Global Positioning System (GPS), which orbits at 20,200 km, and similar systems from Europe, Russia, and China. Each GPS satellite rotates around the earth twice each day. Various communications constellations have been conceived to inhabit this space, but the only modern example is the 20-satellite O3B system being launched by SES.

Satellite Service to and from Taiwan

Taiwan plans to set up a satellite network, with capabilities similar to those Starlink has provided to Ukraine, in case China tries to cut off its communications.[33] Taiwan's *Communication Network Digital Resilience Reinforcement with Response or Wartime Application Emerging Technology Plan* looks to LEO satellites to ensure that video conferencing, voice over internet protocol, and livestreaming can be maintained even if submarine cables and telephone networks are damaged. Taiwan envisions its satellite network to have 700 ground stations and at least 20 of its own satellites by 2030.[34]

However, even when completed, the satellite and network control stations of this system might have a severe vulnerability if the stations are located on Taiwan. Such stations have uplink antennas that can be readily detected and located with the kinds of signals intelligence systems that China possesses. Once located, these facilities can be destroyed by aircraft or rocket artillery. Therefore, if such facilities are built, it will be crucial for Taiwan to arrange alternative stations that can control the satellites and ground networks should the primary stations become damaged during a conflict. Established commercial LEO and GEO satellite systems have multiple control stations located away from Taiwan. These stations are less vulnerable to attack by Chinese conventional forces, and each provider could negotiate mutual-aid agreements with their competitors in case one or more control stations are damaged.

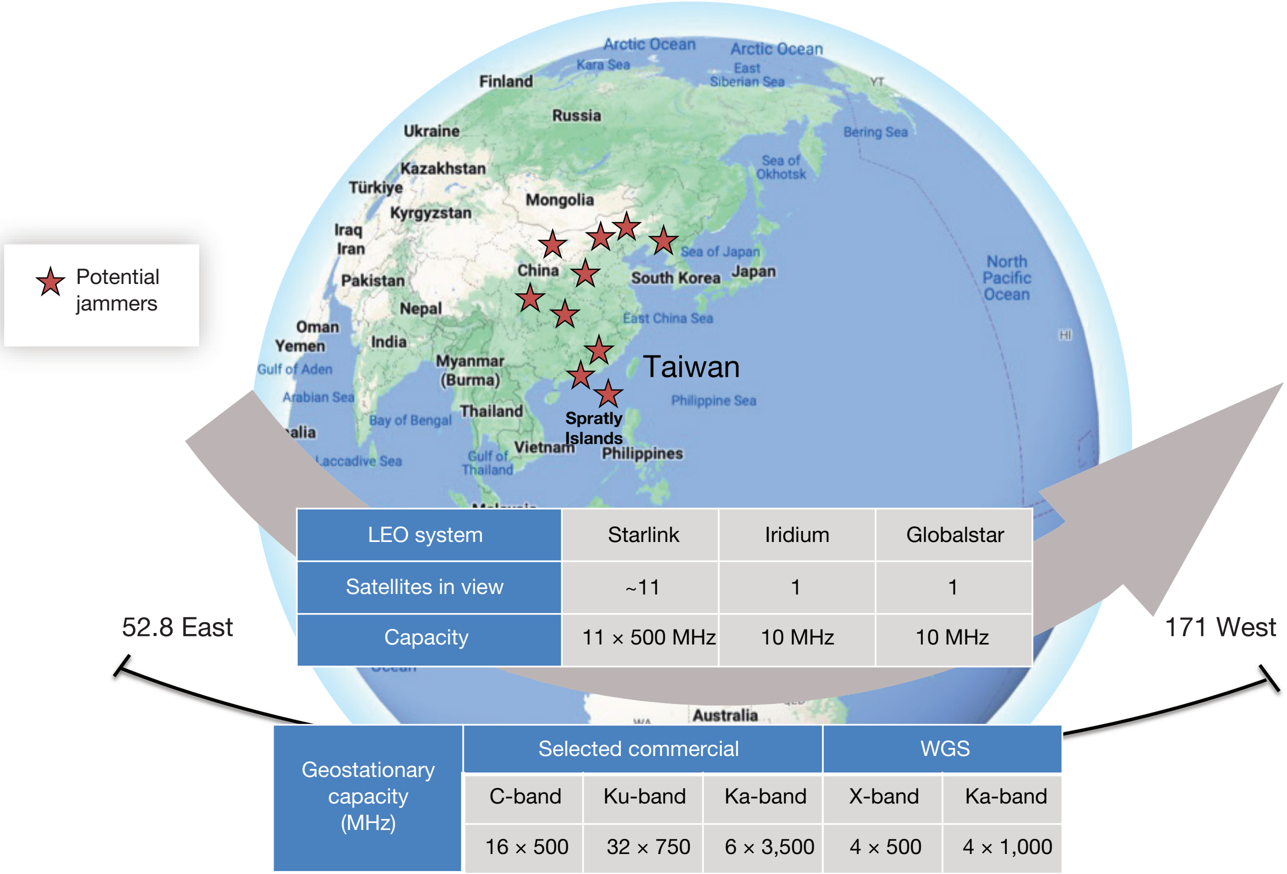
In the meantime, Taiwan could simply purchase services from one or more of the satellite systems depicted in Figure 2. (Note the potential Chinese jammers' locations, which I will discuss later.) The largest of the LEO systems is Starlink, which has approximately 3,600 satellites in orbit (of which perhaps 3,200 are operational) as of February 2023. Approximately 11 of these satellites should be within view of Taiwan at any given time to offer fixed and mobile uplink services on 500 MHz of Ku-band spectrum.[35] Interestingly, Starlink has been allocated 2,000 MHz of downlink bandwidth, meaning it offers a much larger data rate to users than the data rate it can uplink from users. Other LEO systems include OneWeb (approximately 600 satellites, but not yet offering service), Kuiper (due to begin launching in 2023), and the older Iridium and Globalstar constellations. Iridium and Globalstar have much smaller frequency allocations at about 10 MHz each, which limits these systems to providing mainly voice and text messaging services.

It will be crucial for Taiwan to arrange alternative satellite and network control stations should the primary stations become damaged during a conflict.

In addition, a total of 182 communications satellites lie in the portion of the GEO arc that is visible from Taiwan.[36] Of these, 63 are operated by commercial constellations based in countries most likely to be sympathetic with Taiwan if it is attacked by China. A quick review of these systems suggests that a significant portion of them cover Taiwan, including 16 satellites offering C-band, 32 offering Ku-band, and 6 offering Ka-band.[37] Although several nations (including the United States) have reallocated 300 MHz of C-band downlink bandwidth for terrestrial 5G use, it should still be possible to use the uplink bandwidth. Therefore, I estimate that each C-band satellite could provide 500 MHz of uplink capacity from users in Taiwan. The extended Ku-band contains 750 MHz of capacity, while the commercial Ka-band is allocated 3,500 MHz of

FIGURE 2

Satellites Within View of Taiwan



LEO system	Starlink	Iridium	Globalstar
Satellites in view	~11	1	1
Capacity	11 × 500 MHz	10 MHz	10 MHz

Geostationary capacity (MHz)	Selected commercial			WGS	
	C-band	Ku-band	Ka-band	X-band	Ka-band
	16 × 500	32 × 750	6 × 3,500	4 × 500	4 × 1,000

SOURCES: Features information from Eutelsat, “Satellites”; Aerospace Technology, “Globalstar Communication Satellite”; Federal Communications Commission (FCC) Office of Engineering and Technology Policy and Rules Division, “FCC Online Table of Frequency Allocations”; Inmarsat, “Satellites”; Intelsat, “Global Satellite Network"; Iridium Communications Services, “SMTS”; Optus, “The Optus Satellite Fleet”; SES, “Our Coverage”; SKY Perfect JSAT Group, “Satellite Fleet”; and Union of Concerned Scientists, “UCS Satellite Database.”

capacity. (A brief description of these frequency bands is provided in the appendix.)

The U.S. government and the governments of allied nations also operate 32 communications satellites, including four WGS satellites, that could provide coverage to users in Taiwan. Each WGS satellite can provide 500 MHz of X-band capacity and 1,000 MHz of military Ka-band capacity (which is at a higher frequency than commercial Ka-band).

A few caveats are important to mention here. If 100 percent of the capacity on all the LEO and GEO satellites shown in Figure 2 were available to Taiwan, then a combined total of 64.5 GHz of bandwidth would be available for uplinks from Taiwan. At a bit rate efficiency of 1 bit per second per Hertz of bandwidth, this would translate to 64.5 gigabytes per second (Gbps)—less than the capacity of one of the latest submarine cables. However, satellite systems typically plan to operate with 80 percent of their capacity filled by existing customers, so the available data rate for Taiwan could be as low as 13 Gbps before considering the effects of electronic interference (or jamming, which I will describe below).[38] In wartime, governments might be willing to preempt some users of SATCOM to make more bandwidth available for war-supporting functions, but Taiwan would still need to carefully control access to whatever amount of SATCOM it is able to secure.

Therefore, Taiwan needs to develop priorities and protocols for SATCOM usage. First priority should be given to government agencies and military units. These users should mainly transmit data and should send images, video, and even voice sparingly. Media sources providing coverage of the war will likely be somewhere in the next tier of priority. In their case, video will be important but might have to be placed in a queue for transmission when capacity becomes available. Noncritical businesses and individuals will likely have access on an as-available basis and should be prepared to rely on short data and text messages.[39]

Chinese Military Threats to Satellite Systems and Services

China clearly recognizes that Taiwan would become reliant on satellites in a war: China is developing capabilities to attack each of the satellite constellations described above and has made some public statements on its counterspace activities.

DoD has described the force structure that China is building to disrupt or destroy adversary SATCOM. General John W. Raymond, Chief of Space Operations of the U.S. Space Force, testified to Congress that China and Russia are building space weapons for "robust jamming of GPS and communications satellites" and "directed-energy systems that can blind, disrupt or damage our satellites."[40] China has demonstrated direct-ascent anti-satellite (ASAT) weapons that can destroy LEO satellites. It also has maneuverable satellites that could act as "space mines" by exploding near a GEO satellite and showering it with debris.[41] DoD judges that China might also be improving its ground-based lasers to cause structural damage to LEO satellites and might be developing a new ASAT weapon to strike GEO satellites.

So how might Taiwanese officials and civilians use SATCOM in the face of Chinese ASAT threats? The solution to ASAT threats might be as simple as increasing the number of satellites that Taiwan uses. China might launch enough ASATs or space mines to destroy the four WGS satellites over the Pacific and perhaps many commercial satellites as well. But destroying all 63 commercial and 32 government GEO satellites that Taiwan might use would be a significant undertaking. And if Taiwan bought time on Starlink and other emerging LEO systems, China would have to disable thousands of additional satellites to preempt all communications. Even if China's ground-based lasers prove capable of inflicting structural damage on LEO satellites, disrupting all SATCOM accessible by Taiwan would likely take quite some time.

Chinese military researchers have said that China needs the ability to disable or destroy Starlink satellites.[42] Charging the Van Allen radiation belts by an exo-atmospheric nuclear blast can cause satellites moving through them to fail, and the super-charged effects can last for several months.[43] However, the current Starlink satellites orbit at an altitude of 550 km—below the lowest of these belts. More recently, Chinese military scientists have simulated an upper-atmospheric burst that they believe might affect satellites in 500 km orbits in a similar way. If achievable in practice, an advantage of this new approach would be an effect that is localized—rather than affecting the entire globe—and limited in duration. Therefore, it might be possible to select a particular set of LEO satellites to attack without affecting others.[44] However, a localized hole in LEO coverage will quickly be filled by other satellites as the constellation moves over the surface of the earth. A longer-term disruption would require that satellites be disabled as they moved within sight of Taiwan.

Communications satellites are vulnerable to a form of electronic attack called *jamming*.

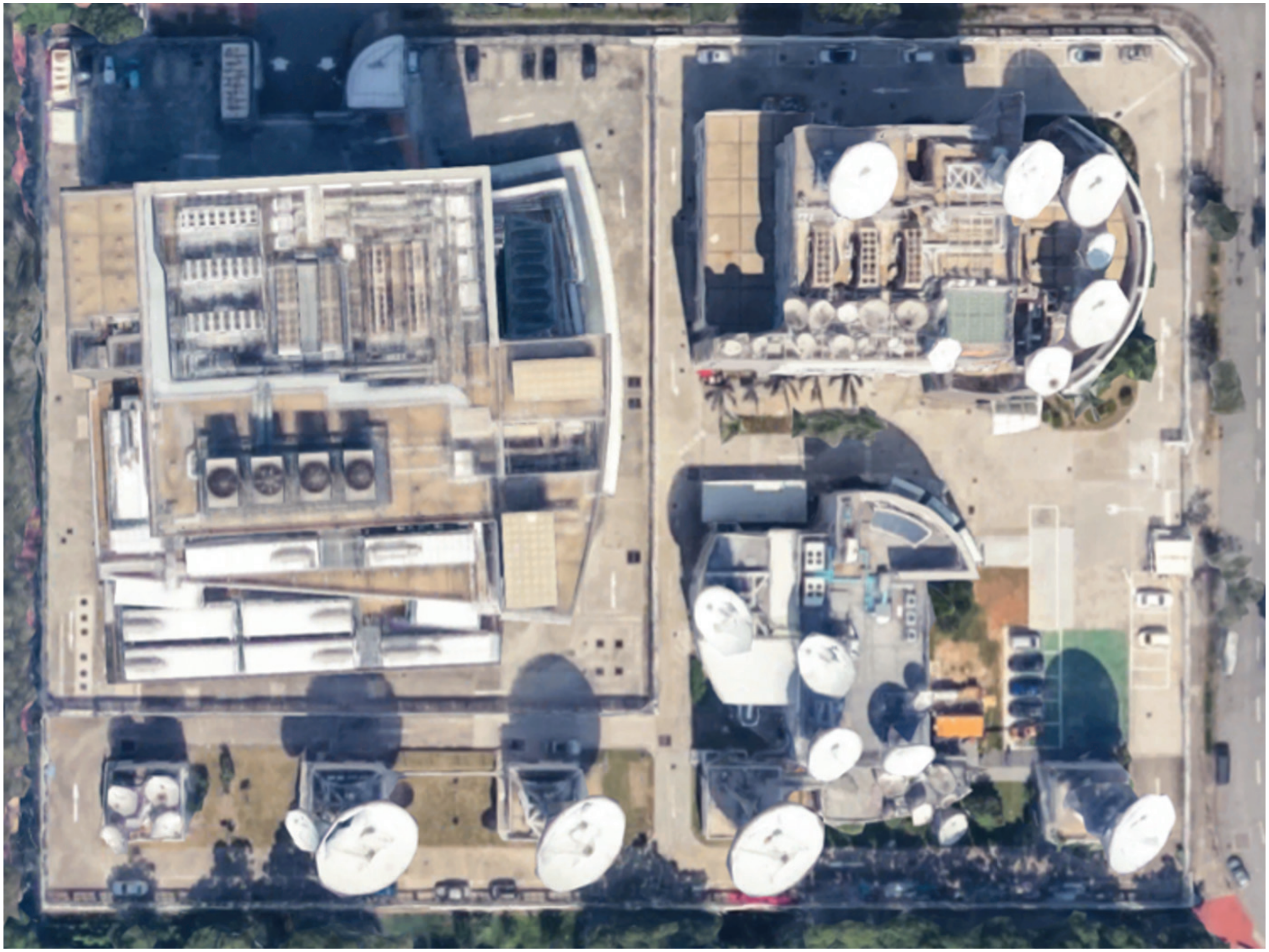
Chinese electronic attacks might pose a more immediate challenge. Communications satellites are vulnerable to a form of electronic attack called *jamming*. Typically, a jammer will try to interfere with the uplink signal sent to a satellite from a user terminal. Jamming attacks employ a high-powered terminal to transmit noise over the same satellite transponders used by terminals trying to communicate. Jammers often have an advantage: They can use a very large dish antenna, transmitting at very high power, without needing to maintain signal quality because they intend to transmit noise anyway.

Satellite dishes ranging in size from six to more than 30 m in diameter would be well-suited for use as jammers. China has dishes of this size at military bases, its satellite control centers, and the teleports that communicate with GEO satellites. More could be built with relative ease. One such teleport, controlling the APT Satellite Company's constellation from Hong Kong, is depicted in Figure 3. It features 35 large terminals. A neighboring complex in Hong Kong uses more than 40 large dishes to control the AsiaSat constellation.

The PLA has been observed increasing its jamming capabilities and appears to have developed specialized capabilities on artificial islands that it built on reefs in the South China Sea.[45] These capabilities include large satellite dishes that could be used to identify satellite uplinks from Taiwan or other nations—using interferometric techniques—and then jam them.[46]

FIGURE 3

APT Satellite Control Complex in Hong Kong



SOURCE: Reproduced from Google Maps.

Increasing the Robustness of Taiwan's Satellite Communications

If Taiwan waits until a war starts to increase its SATCOM capacity, China's offensive space capabilities will limit Taiwan's options. To be successful, Taiwan must develop and exercise satellite-based operational concepts that can mitigate China's threat systems.

To estimate the potential effects of jamming, I used a simple satellite link-budget analysis.[47] For the jammer, I assumed the PLA would use several high-powered commercial dishes, operating from military bases, commercial teleports, or other civilian sites (which could be ganged together remotely), to jam satellite uplinks. I assumed the Taiwanese users would have VSATs typically found on small businesses and mobile VSATs serving aircraft, ships, TV crews, and military users. The number of jammers needed to disrupt communications with selected LEO and GEO constellations is summarized in Table 1.

I estimate that five jammers would be required to disrupt user uplinks on a generic LEO Ku-band satellite. If 11 generic LEO satellites with no anti-jam capabilities are available to users in Taiwan at the same moment, it would require the PLA to allocate 55 jammers to jam all of them. Jamming LEO systems would require that the jamming systems track the satellites as they move across the sky. Such tracking antennas should be available at most satellite control centers.

In theory, Taiwan should also be able to lease services from satellites operated by Eutelsat, Inmarsat, Intelsat, SES, and similar entities based in Japan, South Korea, and Australia. If Taiwan leases individual transponders, for example at commercial Ku-band frequencies, the PLA could identify them using standard interferometric techniques and then disrupt any one of them with a single jammer. If Taiwan used several Ku-band transponders on a single satellite (like the ST-2 it co-owns with Singapore), the PLA should be able to jam its entire extended Ku-band uplink with eight high-power jammers if the PLA does not know exactly which transponders Taiwan is using. If the PLA had to jam the Ku-bands on the 32 commercial Ku-band satellite uplinks depicted in Figure 2, then it would have to add 256 terminals, as shown in Table 1.

So how could Taiwan hide its uplinks among these satellites without leasing all their capacity? The answer for Taiwan's military and government users might be to purchase services from managed service providers (or MSPs, as they are called in the industry). Leading global constellation owners, such as Intelsat and SES, and service bundlers, such as Viasat and Hughes, sell managed services for inflight internet connections to airplanes. Each of these companies has operations centers that allocate bandwidth from many different constellation providers to ensure that

TABLE 1

Large Terminals Needed to Jam Exemplar Satellite Constellations

	Large Terminals Needed to Jam		
User Terminals	LEO Ku-Band Constellation	32 GEO Satellites	4 WGS
LEO terminal	55	—	—
Against VSAT (e.g., 0.6 m)	—	Ku-band: +256	X- and Ka-band: +60
Medium terminal (e.g., 2.4 m)	—	C-band: +80	Put jammer in sidelobe: +280

aircraft can meet the video and data streaming demand of passengers. As the planes cross continents and oceans, communications are shifted from satellite to satellite to provide uninterrupted service. Viasat has applied its expertise serving commercial airlines to provide high-capacity communications to Air Force One, including when it makes short-notice flights to remote places.

The key will be to arrange contractual relationships now, well before a conflict begins. Taiwan would need to purchase terminals able to access MSP systems for its highest-priority government offices and military units. These users will need to be able to divide their outgoing (or uplink) communications into small chunks that can be quickly assigned to several satellites. If (or likely, when) the PLA jams one of these satellites, these small chunks could then be quickly reassigned to open slots on other available satellites. Taiwanese users would need to work closely with MSPs to develop and exercise the procedures they would use in wartime.

There is likely a limit to how many users can be shuttled among satellites to avoid jamming attacks. Although this process could work for high-priority government offices and military units, it might not suffice for lower-priority users in the general population. Luckily, jamming is likely to affect only the outgoing communications of these users. As long as the Taiwanese leadership succeeds in uplinking communications—such as broadcast messages for the population or orders to military units—to the satellite, the lower-priority users' downlinks should be unaffected.[48]

The U.S. government could help by providing some capacity from the four WGS satellites operating within view of Taiwan. If Taiwan purchases the appropriate terminals and DoD grants access, each satellite could provide up to 500 MHz of X-band and 1,000 MHz of Ka-band uplink spectrum. Absent any special capabilities the WGS might be able to employ, the PLA would need another 15 jammers to disrupt VSAT communications uplinks to each WGS (or a total of 60 more jammers to disrupt uplinks to all 4 WGS). The WGS could also move its spot beams so that users in Taiwan would be in the main uplink beam, but PLA jammers on the mainland or in the South China Sea would have to jam from outside the main beam (otherwise known as a *sidelobe jamming*). If Taiwan purchased some medium-sized X- and Ka-band terminals (with 2.4-m dishes), its users in the main beam could overcome these sidelobe jammers. The PLA would then have to either allow these medium-terminal communications to continue or add another 280 large jammers (70 more per satellite) to disrupt them.

The key will be for Taiwan to arrange contractual relationships with service providers now, well before a conflict begins.

Medium-sized terminals might bring other benefits as well, depending on which models are selected. Some terminals can access C-band in addition to X-, Ku-, and

Cyberattacks might also pose a threat to Taiwanese communications satellites.

Ka-band. (A typical such terminal is the heavy version of the U.S. transportable tactical command communications [T2C2] terminal, called T2C2-Heavy.) This would enable users in Taiwan to access the 16 commercial satellites identified in Figure 2 that offer C-band coverage. Typically, C-band provides 500 MHz of uplink bandwidth, which would require the PLA to allocate five more jammers for each satellite. If Taiwan contracted with MSPs for coverage from all 16 of these satellites, the PLA would require another 80 jammers.

Some important conditions must be met to use commercial systems and providers in this way. Taiwan would need to establish an agreement that explicitly covers services in wartime. This is risky for commercial providers: They would expose their systems to electronic (and perhaps physical) attack during wartime and risk losing important customers in peacetime.

As one example, Chinese authorities have already been reported asking Starlink not to provide coverage within China—by which they would include Taiwan.[49] And, recent media reports suggest that Starlink might be backing away from supporting warfighting uses.[50] There have also been some complaints that Starlink service to Ukrainian forces has been interrupted when the Ukrainian Army reclaimed territory vacated by Russian forces. While Starlink refuted these claims, others speculated that Starlink might have shaped its coverage to exclude Russian-occupied areas. Once Russian forces retreated, the advancing Ukrainian units would then have moved out of coverage.[51]

In theory, Taiwan could employ all the methods outlined above. If it did so, I estimate that the PLA would have to employ a force of more than 700 high-power jammers to disrupt all satellite uplinks from Taiwan. (Even more could be required if Taiwan reached agreements to use more of the commercial and government satellites in view.) A large, resource-rich nation like China could certainly marshal a jammer force of this size, either by building purpose-built systems or pressing existing teleports and corporate communications terminals into military service. For comparison, the United States hosts dozens of satellite teleports: Forty-four of these are part of the World Teleport Association, and some of them host 50 or more large dishes each.[52] But this would require a significant effort by the PLA, and Taiwanese government and military forces could further increase the numbers of jammers needed by focusing uplink energy into narrower channels, albeit with a lower data rate.

Cyberattacks might also pose a threat to Taiwanese communications satellites. A cyberattack against Viasat's KA-SAT network disrupted thousands of satellite modems across Europe at the beginning of Russia's invasion of Ukraine.[53] This attack affected a specific set of consumer modems but not Viasat's directly managed mobility or government users on KA-SAT or other worldwide networks.[54] And Starlink was apparently able to sidestep Russian cyberattacks with a simple change in its terminal software. But future cyberattacks could be larger in scope and scale.

For rank-and-file civilians, SATCOM use might be limited. At the time of this writing, the majority of the Taiwanese people do not appear to use satellite internet or TV services. Most Taiwanese people have cable TV, and only about 100,000 Taiwanese homes receive satellite TV.[55] These downlinks might continue working as long as PLA jammers are not in the direct-to-home satellite uplink beams. As mentioned previously, there are discussions underway to introduce satellite internet as a backup to cable systems. But two-way SATCOM might find their outgoing uplinks jammed by the PLA, as described above. And private citizens will not have the priority of government offices and military units for MSPs to shift them around to avoid jamming attacks.

To establish robust SATCOM for government and military users, Taiwan should take the following actions now:

- Establish usage agreements with at least one LEO constellation and purchase the necessary terminals to utilize them. Users would include Taiwanese civilian agencies and military forces and perhaps mobile cellular providers.
- Purchase VSAT terminals for government offices and military units able to access commercial and military GEO satellites at the Ku-, X-, and Ka-bands. Preferably, these terminals should be the same models purchased by the U.S. Army or U.S. Marine Corps for commonality. These could be the lighter versions of the T2C2-Heavy, such as the T2C2 Scout and Lite terminals.
- Purchase some medium-power terminals able to operate at higher power and utilize C-band frequencies. Once again, these should be models already in U.S. military inventories. The T2C2-Heavy terminals are an example.
- Negotiate agreements with DoD to use WGS X- and Ka-band services.
- Establish agreements with commercial MSPs for data services over each of the constellations covering Taiwan. The MSPs should demonstrate the ability to rapidly shift high-priority users among satellites as needed to provide capacity or overcome electronic interference.
- Develop concepts of operations to use commercial and military satellites for priority Taiwanese government, military, and civilian communications in the presence of heavy jamming attacks. Work closely with commercial providers to regularly exercise the ability to shift communications among satellites.
- Assign highest communications priority to key government offices and military units. Develop protocols to grant access to lower-priority public offices, businesses, and individuals on an as-needed and as-available basis.
- Deploy mobile generators to maintain electrical power for critical satellite terminals.

Final Thoughts

It is impossible to know with certainty whether—or when—China will take military action against Taiwan. If China does attack, it is very likely to attempt to control all communications on the island of Taiwan and prevent Taiwan's contact with the rest of the world.

Taiwan can do much to counter China's strategy. Taiwan's announced "digital resilience for all" plan is one important part of this; the steps outlined here are another. Data clouds and satellite and 5G communications could help Taiwan build a resilient network to continue governmental functions, command defenses, engage its people, and remain connected to supporters in the outside world.

Taiwan has an opportunity to preserve its voice if it takes the following actions now:

- **Accelerate 5G deployment and equip key segments to function as edge networks.** These edge networks would maintain connections among local civilians and military units even when terrestrial cables are severed. Equip edge networks with satellite terminals so they can maintain connections with each other.
- **Develop offshore enclaves for key databases.** In an attack, China would destroy or pillage crucial government, banking, and technical databases. As in the example of Ukraine, Taiwan could preserve these databases with the help of offshore data clouds. Taiwan should develop plans now to preserve these databases while ensuring their security and accessibility.
- **Prepare alternate locations for key spokespeople and media figures.** During crisis and war, the Taiwanese people will need reassurance from familiar officials and media influencers. Taiwan should prepare multiple alternate wartime locations for these people and their media teams and plans to move them when an attack is imminent.
- **Build satellite internet networks.** Although Taiwan has plans to build its own satellite system, those plans will take years to reach fruition. And, even if completed, satellite and network control stations in Taiwan would remain vulnerable to attack. Taiwan needs a satellite alternative now, before China mounts an invasion. LEO systems, such as Starlink or OneWeb, and managed services from international MEO and GEO constellations should be part of this alternative. Protocols to prioritize users will be needed to achieve the most benefit from the satellite capacity available.
- **Develop plans to equip wartime media locations, satellite terminals, and edge networks with power generators to replace damaged electrical infrastructure.** Fuel stockpiles (or solar panels, where appropriate) will also be needed.

APPENDIX

Frequency Bands and Selected Satellite and Terrestrial Uses

Table A.1 describes the frequency bands used for satellite and terrestrial communications, the range of frequencies in each band, the amount of bandwidth available, and some exemplar satellite allocations and terrestrial uses. The satellites and terrestrial examples listed represent just a few of the more well-known uses. Interested readers should consult the FCC Online Table of Frequency Allocations to gain a full appreciation for the complexity of bandwidth allocations and the crowd of users within each of the frequency ranges listed.

The first bands listed are very high frequency (VHF) (covering the frequencies from 30 to 300 MHz) and ultra high frequency (UHF) (300 MHz to 1,000 MHz). The U.S. Navy's Mobile User Objective System (MUOS) satellites use this band. These frequencies also host many terrestrial users, including traditional wireless (or free over-the-air) TV and amplitude modulation (AM) and frequency modulation (FM) radio broadcasts.

The L-band is the name given to frequencies ranging from 1 to 2 GHz, containing a total bandwidth of 1,000 MHz (or 1 GHz). GPS uses this band to downlink its timing signal. The Iridium satellite constellation also operates within this band and has been allocated 10 MHz of bandwidth for uplink and downlink communications.

The S-band is the name given to the frequencies from 2 to 4 GHz, containing 2,000 MHz of bandwidth. The Tracking and Data Relay Satellite (TDRS) system operated by NASA uses a portion of this band. Exemplar terrestrial uses of the L- and S-bands include radio navigation systems and 2G, 3G, 4G, and 5G mobile cellular systems.

The C-band is the name given to frequencies from 4 to 8 GHz, containing a total of 4,000 MHz of bandwidth. In the United States, communications satellites have traditionally been allocated 500 MHz of this bandwidth for uplinks from ground stations and another 500 MHz of bandwidth for downlinks from the satellites to the ground stations. (A somewhat bigger allocation had been given by some other nations for satellite uplinks and downlinks.) Subsequently, 300 MHz of the downlink bandwidth has been reallocated for use by 5G mobile systems (sometimes referred to as the *sub–6 GHz* band in the 5G community). This reduces the capacity of C-band SATCOM down to earth. However, it might still be possible to use the full uplink capacity of existing C-band satellites if the uplink transmissions are sufficiently directional or shielded to prevent interfering with adjacent 5G base stations.

The X-band is the name given to the frequency range from 8 to 12 GHz, containing 4,000 MHz of bandwidth. These frequencies are used by such U.S. military satellites as the WGS, but commercial satellites do not typically operate in this range. The WGS is allocated 500 MHz of X-band for uplink communications and another 500 MHz for downlink communications to users operating on the earth's surface or the airspace above it. Although the downlinks overlap with the high end of the C-band, they are still referred to as X-band communications by DoD. Terrestrial uses include land, airborne, and maritime radars.

TABLE A.1

Frequency Bands and Exemplar Communications Uses

Band[a]	Frequency Range[b]	Bandwidth	Exemplar Satellite Allocations	Exemplar Terrestrial Uses
VHF	30 to 300 MHz	270 MHz	—	TV, FM radio
UHF	300 to 1,000 MHz	700 MHz	MUOS[c]	TV, AM radio
L-band	1 to 2 GHz	1,000 MHz	GPS,[d] Iridium[e]	Radio navigation 2G, 3G, 4G, 5G mobile
S-band	2 to 4 GHz	2,000 MHz	TDRS[f]	
C-band	4 to 8 GHz	4,000 MHz	GEO SATCOM: 500 MHz[g]	5G mobile
X-band	8 to 12 GHz	4,000 MHz	WGS: 500 MHz[h]	Radars
Ku-band	12 to 18 GHz	6,000 MHz	GEO SATCOM: 750 MHz[i] Starlink: 500/2,000 MHz	Microwave towers, radars, navigation, and radio astronomy
Ka-band	18 to 40 GHz	32 GHz	Commercial SATCOM: 3,500 MHz[j] WGS: 1,000 MHz	5G mobile

SOURCES: Features information from the sources mentioned below.

[a] See NASA, “Communications.”

[b] See FCC Office of Engineering and Technology Policy and Rules Division, “FCC Online Table of Frequency Allocations.”

[c] See Oetting and Jen, “The Mobile User Objective System.”

[d] See National Institute of Standards and Technology, “Time and Frequency from A to Z, G.”

[e] See Iridium Communications Services, “SMTS.”

[f] See NASA, “Tracking and Data Relay Satellite (TDRS) Second Generation Capabilities.”

[g] C-band satellites long held bandwidth allocations of 500 MHz for uplink and 500 MHz for downlinks. Recently, the United States and other nations have reallocated 300 MHz of the downlink bandwidth for 5G cellular systems. However, most C-band satellites still have 500 MHz of uplink capacity built into them, and it might be possible for Taiwan to use that uplink capacity in wartime. For a discussion of C-band allocations, see Lagunas et al., “5G Cellular and Fixed Satellite Service Spectrum Coexistence in C-Band”; and Chem Europe, “C Band.”

[h] See Spaceflight101, “WGS—Wideband Global Satcom.”

[i] See Magallanes, “Looking for Capacity Options in Extended Ku-Band Segment.”

[j] See Christensen, “ITU Regulations for Ka-Band Satellite Networks.”

The Ku-band is the name given to frequencies in the 12 to 18 GHz range, containing 6,000 MHz of bandwidth. In the United States, commercial communications satellites in GEO have been allocated 500 MHz of bandwidth for uplinks to satellites and another 500 MHz for downlinks to earth terminals. However, other nations have allocated an extended Ku-band with 750 MHz of uplink and downlink bandwidth. I use the extended Ku-band in this analysis because satellites operating over the western Pacific Ocean might have access to it. The Starlink constellation operating in LEO has been allocated 500 MHz of bandwidth for uplinks and 2,000 MHz (2 GHz) of bandwidth for downlinks to user terminals. Historical terrestrial uses include microwave towers, radars, navigation, and radio astronomy.

The Ka-band is the name given to frequencies from 18 to 40 GHz, containing 32 GHz of bandwidth. Commercial communications satellites have been allocated 3,500 MHz of bandwidth for uplinks to satellites and downlinks to user terminals. The WGS system has been allocated 1,000 MHz of bandwidth. Terrestrial users of this frequency range include 5G mobile services.

Notes

[1] Sacks, "What Xi Jinping's Major Speech Means for Taiwan."

[2] Ruwitch, "These Are 4 Key Points from Xi's Speech at the Chinese Communist Party Congress."

[3] Grady, "China Will Increase Pressure on Taiwan in Next Two Years Rather Than Invade, Says Pentagon Official."

[4] Sevastopulo, "US Navy Chief Warns China Could Invade Taiwan Before 2024."

[5] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2022*, pp. 126–128.

[6] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2022*, p. 140.

[7] Simonite and Volpicelli, "Ukraine's Digital Ministry Is a Formidable War Machine."

[8] Braithwaite, "Zelensky Refuses US Offer to Evacuate, Saying 'I Need Ammunition, Not a Ride'."

[9] Cain, "Volodymyr Zelensky on War, Technology, and the Future of Ukraine."

[10] Rhodes, "Taiwan Prepares to Be Invaded."

[11] Yee, "Taiwan Plans for Ukraine-Style Back-Up Satellite Internet Network Amid Risk of War."

[12] Dangwal, "Taiwan's Own 'Starlink' Satellite Network Under Development; Aims to Build 700 Ground Stations Across the Country."

[13] McDaniel and Zhong, *Submarine Cables and Container Shipments*.

[14] Wu et al., *Taiwan Internet Report*.

[15] Ferry, "Building Cellular Connectivity."

[16] Statista, "Share of Respondents Using 5G in Taiwan in 2020 and 2022."

[17] Shan, "NCC Allots NT$16bn for Base Station Subsidies."

[18] Simonite, "How Starlink Scrambled to Keep Ukraine Online." See also Booth, "Ukraine Needs 1.6 Billion Euros to Rebuild Telecoms Sector, Says Official."

[19] McDaid, "The Mobile Network Battlefield in Ukraine—Part 1."

[20] Thomala, "Number of Radio and TV Operators in Taiwan 2010–2021, by Segment."

[21] For example, see Low, "Operation Fish," and McDowall, *Due Diligence*.

[22] Menn, "Impact of Ukraine-Russia War."

[23] Amazon, "Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future."

[24] "Breaking: Subsea Cables Connecting Taiwan to U.S. at Risk."

[25] TeleGeography, "Submarine Cable Map: Taiwan."

[26] Janson, "Advances in Subsea Fiber Cable Technology."

[27] Burgess, "The Most Vulnerable Place on the Internet."

[28] Submarine Cable Networks, "Cable Landing Stations in Taiwan."

[29] Davies, "How Loon's Balloons Find Their Way to Deliver the Internet."

[30] Garamone, "F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast."

[31] Allport, "USAF Retires BACN EQ-4B Global Hawks."

[32] The LEO and MEO altitudes used here correspond with definitions provided by NASA and the European Space Agency. See European Space Agency, "Types of Orbits," and Johnson, *Medium Earth Orbits*.

[33] Everington, "Taiwan Building Backup Satellite Internet Network Amid Risk of Chinese Attack."

[34] Dangwal, "Taiwan's Own 'Starlink' Satellite Network Under Development; Aims to Build 700 Ground Stations Across the Country."

[35] The number of Starlink satellites providing service to a given area depends on many physical and design parameters. In this analysis, I am assessing the Starlink shell located at 550 km altitude, with a design elevation angle of 40 degrees for users. This yields a coverage radius of 580 km per satellite, which, on average, puts 11 satellites within view of some part of Taiwan. (A lower elevation angle would put more satellites in view; I use a higher angle to account for ground obstacles around users.) How Starlink orients and schedules the uplink beams of its satellites, and whether a given satellite prioritizes traffic from Taiwan over traffic from China, Japan, or the Philippine Islands, is a different matter. It might be that some of these satellites are busy with traffic from

another nation within its view. See Cakaj, "The Parameters Comparison of the 'Starlink' LEO Satellites Constellation for Different Orbital Shells"; Starlink Satellite Map, homepage; Hughes, "SpaceX Launches 56 More Starlink Satellites in Heaviest Payload Yet"; Jonathan's Space Pages, "Starlink Statistics."

[36] Union of Concerned Scientists, "UCS Satellite Database."

[37] Among the commercial GEO networks I assessed were satellites operated by Intelsat, SES, Eutelsat, Inmarsat, SKY Perfect JSAT Group, and Optus. See Intelsat, "Global Satellite Network"; SES, "Our Coverage"; Eutelsat, "Satellites"; Inmarsat, "Satellites"; SKY Perfect JSAT Group, "Satellite Fleet"; and Optus, "The Optus Satellite Fleet."

[38] Based on U.S. Government Accountability Office, *Telecommunications* and private conversations with SATCOM providers.

[39] It might be useful to frame these restrictions as moving most users from a "real-time TikTok upload" capability to a "text message sometime today" model.

[40] Keller, "Chinese Ability to Use Laser Weapons and Electronic Jamming to Defeat U.S. GPS Satellites a Growing Concern."

[41] Defense Intelligence Agency, *Challenges to Security in Space*.

[42] Chen, "Chinese Military Must Be Able to Destroy Elon Musk's Starlink Satellites if They Threaten National Security: Scientists."

[43] The detonation of nuclear weapons between the altitudes of 600 km and 10,000 km can charge the Van Allen radiation belts. A 1962 detonation by the United States demonstrated that satellites passing through a charged belt can accumulate a sufficient charge over a short period of time to be disabled. See Advanced Systems and Concepts Office, Defense Threat Reduction Agency, "High Altitude Nuclear Detonations (HAND) Against Low Earth Orbit Satellites ('HALEOS')"; King, "Going Nuclear Over the Pacific"; and Sale, "U.S. Physics Blunder Almost Ended Space Programs."

[44] Chen, " Chinese Physicists Simulate a Nuclear Blast Against Satellites."

[45] Aviation Week Network, "Satellite Imagery Exposes China's Space-Jammer Buildup."

[46] Dahm, *Electronic Warfare and Signals Intelligence*.

[47] This section draws on analyses performed by RAND Corporation colleague Scott Grossman. It assumes a 10-m jammer terminal transmitting a 93 decibel watt (dBW) signal at uplink frequencies across 100 MHz of instantaneous bandwidth against a 0.65-m user terminal transmitting a signal occupying 10 MHz of bandwidth at 53.3 dBW. Variations consider 2.4 m and larger user terminals at C-, X-, Ku-, and Ka-bands. The simplified analysis presented here is intended to indicate the scale of jamming that would be required. Generic LEO and GEO satellites without anti-jam capabilities were assumed. Some actual satellites will have processing capabilities to resist jamming, and some jammers might operate with more or less than 100 MHz of instantaneous bandwidth.

[48] Satellite uplinks are most vulnerable when the jammer is in the same uplink footprint as the user. Both then have the same access to the satellite antenna. Downlink jamming is much more difficult: The jammer has to inject its signal into a user dish. Although aircraft-mounted dishes can be vulnerable to line-of-sight downlink jamming, it is much harder if the terminal is on the ground.

[49] Cheng, "Musk Says Beijing Doesn't Want Him to Sell Starlink in China."

[50] Tucker, "Decrying Starlink's 'Weaponization,' SpaceX Cuts Support for Ukrainian Military."

[51] SOFREP, "Starlink 'Catastrophic Outages' While Ukraine's Pushing Against Russia, a Service US Is Secretly Funding."

[52] See World Teleport Association, "Teleport Operators."

[53] Satter, "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset—Ukrainian Official."

[54] Swinhoe, "Viasat: Our Network Was Hit By a 'Multifaceted And Deliberate' Cyberattack."

[55] See S&P Global Market Intelligence, "Asia Pacific Pay TV Growth Slows as Cable and DTH Lose Subs."

References

Advanced Systems and Concepts Office, Defense Threat Reduction Agency, “High Altitude Nuclear Detonations (HAND) Against Low Earth Orbit Satellites (‘HALEOS’),” briefing, April 2001.

Aerospace Technology, “Globalstar Communication Satellite,” webpage, undated. As of April 28, 2023:
https://www.aerospace-technology.com/projects/globalstar

Allport, Dave, “USAF Retires BACN EQ-4B Global Hawks,” *Key.Aero*, August 8, 2021.

Amazon, “Safeguarding Ukraine’s Data to Preserve Its Present and Build Its Future,” June 9, 2022.

Aviation Week Network, “Satellite Imagery Exposes China’s Space-Jammer Buildup,” November 1, 2022.

Booth, Nick, “Ukraine Needs 1.6 Billion Euros to Rebuild Telecoms Sector, Says Official,” Mobile Europe, January 18, 2023.

Braithwaite, Sharon, “Zelensky Refuses US Offer to Evacuate, Saying ‘I Need Ammunition, Not a Ride,’” CNN, February 26, 2022.

“Breaking: Subsea Cables Connecting Taiwan to U.S. at Risk,” Bloomberg News, October 27, 2022.

Burgess, Matt, “The Most Vulnerable Place on the Internet,” *Wired*, November 2, 2022.

Cain, Geoffrey, “Volodymyr Zelensky on War, Technology, and the Future of Ukraine,” *Wired*, June 2, 2022.

Cakaj, Shkelzen, “The Parameters Comparison of the ‘Starlink’ LEO Satellites Constellation for Different Orbital Shells,” *Frontiers in Communications and Networks*, May 7, 2021.

Chem Europe, “C Band,” webpage, undated. As of March 1, 2023:
https://www.chemeurope.com/en/encyclopedia/C_band.html

Chen, Stephen, “Chinese Military Must Be Able to Destroy Elon Musk’s Starlink Satellites if They Threaten National Security: Scientists,” *South China Morning Post*, May 25, 2022.

Chen, Stephen, “Chinese Physicists Simulate a Nuclear Blast Against Satellites,” *South China Morning Post*, October 20, 2022.

Cheng, Evelyn, “Musk Says Beijing Doesn’t Want Him to Sell Starlink in China,” CNBC, October 10, 2022.

Christensen, Jorn, “ITU Regulations for Ka-Band Satellite Networks,” AsiaSat, September 2012.

Dahm, J. Michael, *Electronic Warfare and Signals Intelligence*, John Hopkins Applied Physics Laboratory, August 2020.

Dangwal, Ashish, “Taiwan’s Own ‘Starlink’ Satellite Network Under Development; Aims to Build 700 Ground Stations Across the Country,” *EurAsian Times*, January 4, 2023.

Davies, Alex, “How Loon’s Balloons Find Their Way to Deliver the Internet,” *Wired*, July 23, 2019.

Defense Intelligence Agency, *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion*, 2022.

European Space Agency, “Types of Orbits,” webpage, March 30 2020. As of February 28, 2023:
https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits

Eutelsat, “Satellites,” webpage, undated. As of January 29, 2023:
https://www.eutelsat.com/en/satellites.html

Everington, Keoni, “Taiwan Building Backup Satellite Internet Network Amid Risk of Chinese Attack,” *Taiwan News*, September 14, 2022.

FCC—*See* Federal Communications Commission.

Federal Communications Commission Office of Engineering and Technology Policy and Rules Division, “FCC Online Table of Frequency Allocations,” July 1, 2022.

Ferry, Timothy, “Building Cellular Connectivity,” AmCham Taiwan, December 14, 2017.

Garamone, Jim, “F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast,” *DoD News*, February 4, 2023.

Grady, John, “China Will Increase Pressure on Taiwan in Next Two Years Rather Than Invade, Says Pentagon Official,” *USNI News*, November 7, 2022.

Hughes, Clyde, “SpaceX Launches 56 More Starlink Satellites in Heaviest Payload Yet,” United Press International, January 26, 2023.

Inmarsat, “Satellites,” webpage, undated. As of January 29, 2023 at:
https://www.inmarsat.com/en/about/technology/satellites.html

Intelsat, “Global Satellite Network,” webpage, undated. As of January 29, 2023:
https://www.intelsat.com/global-network/satellite-network/

Iridium Communications Services, “SMTS,” webpage, undated. As of March 1, 2023:
http://www.smtspl.com/iridium.html

Janson, Chris, “Advances in Subsea Fiber Cable Technology,” Lightwave, November 16, 2022.

Johnson, Nicholas L., *Medium Earth Orbits: Is There A Need For A Third Protected Region?* National Aeronautics and Space Administration, 2010.

Jonathan’s Space Pages, “Starlink Statistics,” webpage, last updated March 1, 2023. As of March 1, 2023:
https://planet4589.org/space/con/star/stats.html

Keller, John, “Chinese Ability to Use Laser Weapons and Electronic Jamming to Defeat U.S. GPS Satellites a Growing Concern,” *Military and Aerospace Electronics*, June 8, 2021.

King, Gilbert, “Going Nuclear Over the Pacific,” *Smithsonian*, August 15, 2012.

Lagunas, Eva, Christos G. Tsinos, Shree Krishna Sharma, and Symeon Chatzinotas, “5G Cellular and Fixed Satellite Service Spectrum Coexistence in C-Band,” *IEEE Access*, Vol. 8, April 1, 2020.

Low, Robert, “Operation Fish,” *The Museum* blog, Bank of Canada Museum, May 8, 2018.

Magallanes, Raul, “Looking for Capacity Options in Extended Ku-Band Segment,” *Via Satellite*, April 1, 2011.

McDaid, Cathal, “The Mobile Network Battlefield in Ukraine—Part 1,” *ENEA AdaptiveMobile Security* blog, March 29 2022.

McDaniel, Christine, and Weifeng Zhong, *Submarine Cables and Container Shipments: Two Immediate Risks to the US Economy if China Invades Taiwan*, Mercatus Center, George Mason University, August 29, 2022.

McDowall, Duncan, *Due Diligence: A Report on the Bank of Canada’s Handling of Foreign Gold During World War II*, Bank of Canada, November 1997.

Menn, Joseph, “Impact of Ukraine-Russia War: Cybersecurity Has Improved for All,” *Washington Post*, February 25, 2023.

NASA—*See* National Aeronautics and Space Administration.

National Aeronautics and Space Administration, “Tracking and Data Relay Satellite (TDRS) Second Generation Capabilities,” webpage, October 4, 2017. As of March 2, 2023:
https://www.nasa.gov/directorates/heo/scan/services/networks/tdrs_second_gen

National Aeronautics and Space Administration, “Communications,” in *State-of-the-Art Small Spacecraft Technology*, January 2023.

National Institute of Standards and Technology, “Time and Frequency from A to Z, G,” webpage, updated March 1, 2023. As of March 2, 2023:
https://www.nist.gov/pml/time-and-frequency-division/popular-links/time-frequency-z/time-and-frequency-z-g

Oetting, John D., and Tao Jen, “The Mobile User Objective System,” *Johns Hopkins APL Technical Digest*, Vol. 30, No. 2, 2011.

Office of the Secretary of Defense, *Military and Security Developments Involving the People’s Republic of China 2022: Annual Report to Congress*, U.S. Department of Defense, November 2022.

Optus, “The Optus Satellite Fleet,” webpage, undated. As of January 29, 2023:
https://www.optus.com.au/about/network/satellite/fleet

Rhodes, Ben, “Taiwan Prepares to Be Invaded,” *The Atlantic*, November 7, 2022.

Ruwitch, John, “These Are 4 Key Points from Xi’s Speech at the Chinese Communist Party Congress,” NPR, October 16, 2022.

S&P Global Market Intelligence, “Asia Pacific Pay TV Growth Slows as Cable and DTH Lose Subs,” September 25, 2019.

Sacks, David, “What Xi Jinping’s Major Speech Means for Taiwan,” *Asia Unbound* blog, Council on Foreign Relations, July 6, 2021.

Sale, Richard, “U.S. Physics Blunder Almost Ended Space Programs,” United Press International, December 8, 2000.

Satter, Raphael, “Satellite Outage Caused ‘Huge Loss in Communications’ at War’s Outset—Ukrainian Official,” Reuters, March 15, 2022.

SES, “Our Coverage,” webpage, undated. As of January 29, 2023:
https://www.ses.com/our-coverage

Sevastopulo, Demetri, “US Navy Chief Warns China Could Invade Taiwan Before 2024,” *Financial Times*, October 20, 2022.

Shan, Shelley, “NCC Allots NT$16bn for Base Station Subsidies,” *Taipei Times*, March 4, 2021.

Simonite, Tom, “How Starlink Scrambled to Keep Ukraine Online,” *Wired*, May 11, 2022.

Simonite, Tom, and Gian M. Volpicelli, “Ukraine’s Digital Ministry Is a Formidable War Machine,” *Wired*, March 17, 2022.

SKY Perfect JSAT Group, “Satellite Fleet,” webpage, undated. As of January 29, 2023:
https://www.skyperfectjsat.space/jsat/en/service/satellite_fleet

SOFREP, “Starlink ‘Catastrophic Outages’ While Ukraine’s Pushing Against Russia, a Service US Is Secretly Funding,” October 10, 2022.

Spaceflight101, “WGS—Wideband Global Satcom,” webpage, undated. As of March 1, 2023: https://spaceflight101.com/spacecraft/wgs-wideband-global-satcom

Starlink Satellite Map, homepage, undated. As of January 9, 2023: https://satellitemap.space

Statista, “Share of Respondents Using 5G in Taiwan in 2020 and 2022,” webpage, undated. As of January 9, 2023: https://www.statista.com/statistics/1346458/taiwan-usage-rate-of-5g

Submarine Cable Networks, “Cable Landing Stations in Taiwan,” webpage, undated. As of January 27, 2023: https://www.submarinenetworks.com/en/stations/asia/taiwan

Swinhoe, Dan, “Viasat: Our Network Was Hit By a ‘Multifaceted and Deliberate’ Cyberattack,” Data Center Dynamics, March 31, 2022.

TeleGeography, “Submarine Cable Map: Taiwan,” webpage, last updated April 19, 2023. As of April 21, 2023: https://www.submarinecablemap.com/country/taiwan

Thomala, Lai Lin, “Number of Radio and TV Operators in Taiwan 2010–2021, by Segment,” webpage, Statista, September 26, 2022. As of January 27, 2023: https://www.statista.com/statistics/1200932/taiwan-number-of-radio-and-tv-service-providers-by-segment

Tucker, Patrick, “Decrying Starlink’s ‘Weaponization,’ SpaceX Cuts Support for Ukrainian Military,” *Defense One*, February 9, 2023.

Union of Concerned Scientists, “UCS Satellite Database,” webpage, updated May 1, 2022. As of January 27, 2023: https://www.ucsusa.org/resources/satellite-database

U.S. Government Accountability Office, *Telecommunications: Competition, Capacity, and Costs in the Fixed Satellite Services Industry*, GAO-11-777, September 2011.

World Teleport Association, “Teleport Operators,” webpage, undated. As of March 3, 2023: https://www.worldteleport.org/page/Teleports

Wu, Chyi-In, Chen-Chao Tao, Shu-Fen Tseng, Tai-Yee Wu, Ching-Chun Chen, and Chen-Ya Chen, *Taiwan Internet Report*, Taiwan Network Information Center, 2022.

Yee, Yip Wai, “Taiwan Plans for Ukraine-Style Back-Up Satellite Internet Network Amid Risk of War,” *Straits Times*, September 22, 2022.

About the Author

Timothy M. Bonds is a senior fellow at the RAND Corporation. His areas of research emphasis include the economic, technical, and social impacts of the 5G era; forces and capabilities needed to meet national security objectives and commitments; command-and-control capabilities; personnel mission-day metrics; and military employment of commercial space systems and services. He has an M.S. in aero/astro engineering and an M.B.A.

Acknowledgments

I would like to thank Barry Pavel, Michael Spirtas, and Chris Mouton of the RAND National Security Research Division for funding this Perspective.
I also wish to acknowledge RAND Corporation colleagues Jim Bonomo, Scott Savitz, and Jim Powers for their thorough and helpful reviews and the many suggestions they made to improve this Perspective. Finally, my thanks to Saci Haslam, Yun Kang, and others at RAND for their help in producing this Perspective.

About This Perspective

Taiwan's ability to command its military forces, communicate with its citizens, and coordinate with international allies is dependent on terrestrial, submarine, and satellite networks. In this Perspective, the author discusses the vulnerabilities of these information networks and proposes actions that Taiwan should take to mitigate lost capabilities if attacked by China. The analyses presented in this Perspective can inform Taiwan's approach and serve as a useful complement to Taiwan's "digital resilience for all" initiative.

This Perspective was completed in March 2023 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This Perspective was conducted within the Acquisition and Technology Policy Program of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise. This Perspective was made possible by NDRI exploratory research funding that was provided through the FFRDC contract and approved by NDRI's primary sponsor.

For more information on the RAND Acquisition and Technology Policy Program, see www.rand.org/nsrd/atp or contact the director (contact information is provided on the webpage).

For more information on this publication, visit www.rand.org/t/PEA2557-1.