"Beijing's Air, Space, and Maritime Surveillance from Cuba: A Growing Threat to the Homeland"

Written Testimony of Leland Lazarus
Associate Director, National Security Program – Jack D. Gordon Institute for Public Policy, Florida International University,

Non-Resident Fellow, Global China Hub, Atlantic Council

House Subcommittee on Transportation and Maritime Security
U.S. House of Representatives – May 6, 2025

Introduction

Chairman Gimenez, Ranking Member McIver, and distinguished members of the Subcommittee, thank you for the opportunity to testify before you today.

My name is Leland Lazarus, and I serve as the Associate Director of the National Security Program at Florida International University (FIU)'s Jack D. Gordon Institute for Public Policy, and Non-Resident Fellow at the Atlantic Council's Global China Hub. Throughout my career as a Fulbright Scholar studying the Chinese diaspora in Panama, a State Department Foreign Service Officer in China and the Caribbean, and the Special Assistant to two Commanders of U.S. Southern Command, I have seen firsthand China's growing strategic engagement in Latin America and the Caribbean (LAC), especially in the area of national security.

As we gather here for today's hearing, Xi Jinping is preparing to host various regional leaders– including Cuba–in Beijing next week for the China-Community of Latin American and Caribbean States (CELAC) Summit on May 13th. They will most likely announce the next three-year Joint Action Plan including more Chinese investments in electric vehicles, solar panels, and renewable energy. But the Summit is also an example of the robust strategic presence China has steadily built in our own neighborhood over the past two decades. Cuba, in particular, is

emerging as a centerpiece of China's efforts to challenge the United States near its shores, echoing Cold War dynamics but with 21st-century tools.

China's presence in Cuba is a microcosm of how the PRC approaches the entire LAC region. In Cuba, we see every dimension of Chinese strategy on display: commercial port investments by sanctioned Chinese state-owned enterprises; dual-use telecommunications infrastructure provided by firms like Huawei and Nuctech; signals intelligence (SIGINT) sites likely supporting Chinese military and space goals; and academic and military exchanges that further embed the Chinese Communist Party's influence within Cuban institutions. Chinese journals describe Cuba and other key LAC countries as "strategic support points" (战略支点) serving commercial and security purposes. Chinese sources frame the PRC's engagement in Cuba as a legitimate counterweight to U.S. activities in Asia. The logic is clear: if the U.S. insists on maintaining freedom of navigation operations near Chinese waters, Beijing reserves the right to operate near Florida. That form of "strategic reciprocity" is evident in everything from China's cyber footprint on the island to reported upgrades at Chinese SIGINT facilities.

This testimony draws on open-source information, Chinese-language sources, and cutting-edge research—especially from our FIU Chinese Activities in Latin America Dashboard, a tool we have built to aggregate and visualize all of China's regional activities and projects. I will also offer a set of concrete, actionable recommendations for U.S. policymakers to mitigate these risks, strengthen our regional posture, and support transparency and resilience across the Americas.

The U.S. cannot afford to treat the Western Hemisphere as an afterthought in our global competition with China. If Beijing is willing to establish listening posts, upgrade ports, and export authoritarian technologies to a country just 90 miles from Florida, then we must treat this challenge with the urgency and strategic clarity it deserves.

Ports as "Strategic Support Points"

China's global ambition is to seek "national rejuvenation" by 2049, which includes transforming the People's Liberation Army into a world-class military with global reach.[i] Since the late 2000s, China's expanding global maritime strategy has increasingly incorporated Latin America and the Caribbean (LAC) as part of its "far seas" vision. In Chinese strategic discourse, analysts use the term "战略支点" (zhànlüè zhīdiǎn) – sometimes also "战略支撑点" (zhànlüè zhīchēngdiǎn) – meaning strategic support point or strategic fulcrum, to describe key overseas locations that can support China's military and economic operations.[ii] PLA naval strategist Captain Zhang Wei wrote in a 2018 China Military Science article that PLA presence on both the Atlantic and Pacific coasts of the Americas would "improve the PLA's far-oceans strategic disposition" (完善我军远洋战略布势") by providing more options for deployments and supply in a contingency.[iii]

Unlike traditional foreign "bases," these strategic strongpoints would provide logistical support and economic benefits without constituting offensive military garrisons.[iv]

Just as Chinese private and state-owned enterprises have invested in port facilities from Panama to Peru, they have also helped expand Cuba's port terminals. China Communication Construction Company–a state-owned enterprise sanctioned for directly supporting China's military-industrial complex[v]–expanded Santiago de Cuba's port, Cuba's second-largest.[vi] This mirrors Chinese port projects in the Bahamas, Panama, and across the Caribbean, aiming to secure logistical hubs and footholds astride vital sea lanes. Control or influence over ports gives China dual-use benefits – commercial leverage and potential naval access. Cuba's location at the gateway of the Gulf of Mexico means that Chinese involvement in its ports could position Beijing to monitor or, in a crisis, disrupt shipping routes that lead to U.S. ports like Miami, New Orleans, and Houston.

Snapshot of Chinese port projects in the FIU Chinese Activities in LAC Dashboard[vii]

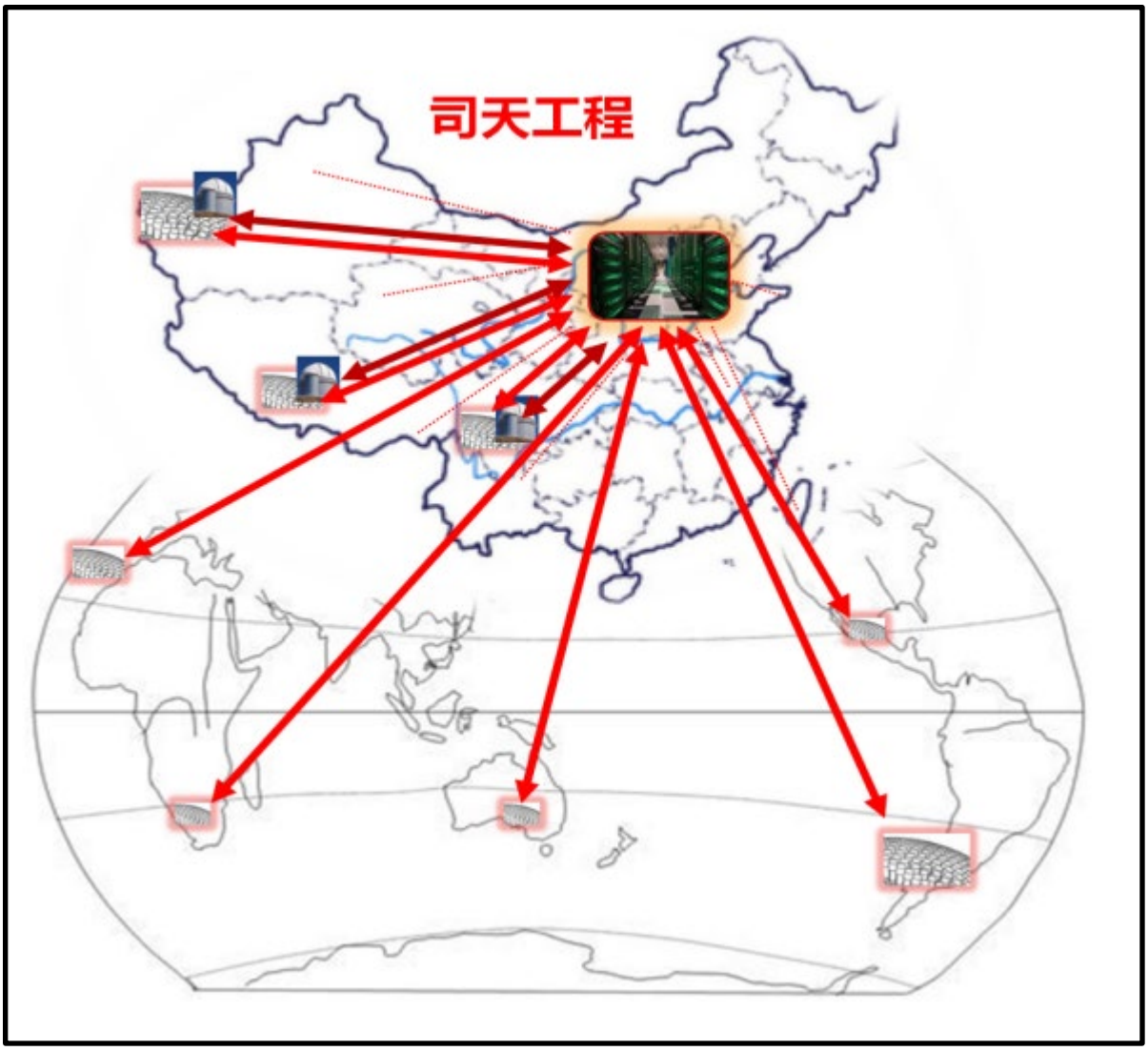
Moreover, regular visits by Chinese commercial shipping lines to Cuban ports increase Chinese visibility into maritime traffic. Havana's deepening dependency on Chinese trade (China is now Cuba's #1 or #2 trading partner) ensures Chinese firms have a major role in port operations and customs. This raises security concerns that Chinese entities could collect data on U.S.-bound cargo or even facilitate intelligence collection under commercial cover.

Strategic support points could also encompass airports. Chinese company Nuctech–which creates scanners at ports and airports–is expanding its business throughout the region, particularly in Cuba. At Havana's José Martí International Airport and the Port of Havana, modern Nuctech

radiographic scanners inspect cargo containers and luggage.[viii] Cuba was reportedly the first Caribbean nation to use some of Nuctech's newest scanning technology. While such equipment can help interdict drugs or contraband, it also can be a source of intelligence. Western security agencies have warned that Nuctech scanners could covertly transmit information about customs inspections back to Beijing.[ix] In an era where tracking supply chains is strategic, knowing what goods pass through Cuba is valuable. The EU recently raided Nuctech's offices for security concerns;[x] having their hardware in Cuba could similarly threaten U.S. interests if, for example, it were used to surveil diplomatic cargo of the U.S. Interests Section (the de facto U.S. embassy in Havana).

China's Sitian Space Program and Signals Intelligence Outpost

Space has similarly emerged as a strategic domain in China-LAC relations. In recent years, China has built space infrastructure in the region – most notably a satellite tracking station in Argentina's Neuquén province. According to Newsweek, China's space facilities in Latin America are part of the Sitian (司天) Project, a plan by the National Astronomical Observatory of China (NAOC) to create a global space monitoring system that will help "meet national strategic needs."[xi] The needs listed were "space fragment monitoring and cataloging; medium and high orbit satellite monitoring; and detection and early warning of near-Earth objects to prevent civilization disasters."[xii] A global map of the Sitian sites includes Mexico and Southern America (ostensibly Argentina and/or Chile).



A map from a 2022 NOAC presentation about the Sitian space program. Arrows point to Mexico and southern America (ostensibly Argentina and/or Chile).

The space domain is also critical for signals intelligence (SIGINT), and Cuba is a prime location for China to target the United States. Southern U.S. states host key military installations – including U.S. Southern Command in Miami, various Navy and Air Force bases, and NASA's Kennedy Space Center. Having listening posts in Cuba puts these within China's earshot. Indeed, Voice of America's Chinese service reported that PLA intelligence values Cuba because it "places the U.S. East Coast under coverage, including Florida's military and civilian space launches and several large Army and Navy bases."[xiii] Satellite imagery analysis from the Center for Strategic and International Studies indicates that China has built or upgraded at least four SIGINT sites in Cuba aimed at intercepting sensitive communications.[xiv] Some Chinese scholars suggest that this is simply retaliation for what they see as U.S. meddling in the Indo-Pacific. In a 2024 Global Times article responding to the CSIS report, Fudan University professor Shen Yi

said: “If the US does not want to see China strengthen its intelligence operations near the US, then Washington should not do the same thing near China, or the US will have to gradually adapt to a new reality of other countries' countermeasures against it.”[xv]

Enabling Digital Authoritarianism

In the past decade, Chinese strategic commentary has increasingly highlighted emerging security domains – notably cyberspace – in the context of Latin America. Beijing sees these high-tech arenas as critical to the future security architecture. Chinese officials have sought Cuban and other Latin American support at the U.N. for principles like cyber sovereignty and a global treaty on cybercrime. They frequently warn against the use of cyber tools to “undermine another nation’s stability”[xvi] – a thinly veiled reference to U.S. intelligence operations and support for opposition groups via social media. This reflects China’s concern over “color revolution” risks in developing countries, and Latin American governments similarly wary of online destabilization– like Cuba–have shown interest in China’s approach.

Across Latin America, Huawei and ZTE have become the dominant suppliers of telecom gear, from 3G/4G cellular networks to fiber-optic cables. Cuba is no exception. The Cuban government’s telecom monopoly ETECSA relies almost entirely on Chinese technology. Huawei, ZTE, and TP-Link are the primary providers of Cuba’s internet and mobile infrastructure. As early as 2000, Cuba contracted Huawei to lay fiber-optic cables nationwide. Chinese tech now underpins everything from the Wi-Fi hotspots in Cuban parks to the routers in Cuban homes. A 2017 network analysis found traces of Chinese code in the login portals for Cuba’s public Wi-Fi, revealing how deeply embedded Chinese software is in Cuban systems. Moreover, the Cuban regime utilizes Huawei’s eSight network management software to filter and block internet content, essentially importing China’s Great Firewall tactics to the island. This Chinese-built digital ecosystem in Cuba grants Beijing extraordinary access and influence. It not only secures China a long-term telecommunications client, but also provides the PLA and Chinese intelligence potential backdoors into communications transiting Cuban networks. Notably, U.S. officials suspect that Chinese telecom technicians have assisted Cuban authorities in setting up systems for signals intelligence – monitoring both Cuban citizens and communications in the surrounding region. In short, Cuba’s telecom sector exemplifies China’s “Digital Silk Road” strategy: export critical tech infrastructure and gain a strategic listening post in return.

Hand in hand with telecom dominance, China exports surveillance tools and know-how to sympathetic regimes in LAC. In Cuba, the Chinese have helped build what can be termed a digital police state in miniature. The same Cuban internet that Chinese companies helped stand up can be shut down on demand – and indeed was, during Cuba’s historic July 11, 2021 protests. When thousands of Cubans took to the streets in rare anti-regime demonstrations, the government cut off internet and mobile service across the island. How could an already

connectivity-poor country so effectively "pull the plug"? The key was Chinese technology and expertise. As I wrote at the time, Beijing's telecom companies played a "fundamental role" in enabling the Cuban regime to control and choke its communications network.[xvii] Then-Senator Marco Rubio noted that Cuba's blackout was achieved using "technology from China" specifically for controlling internet access.[xviii] Research by the Open Observatory of Network Interference and others later confirmed this: Cuba's networking equipment is Chinese, its traffic filtering tools are Chinese, and its entire internet architecture is configured in a way reminiscent of China's own censorship regime.[xix]

Recommendations for U.S. Policymakers

Confronting the challenge of Beijing's investments in dual-use ports, space and SIGINT capabilities and digital authoritarian tools in Cuba will require a multifaceted strategy. The goal is to protect U.S. homeland security, help Cubans gain a freer and more secure digital future, and rally regional support – all without pushing Cuba entirely into China's strategic embrace. Below are clear, actionable recommendations.

1) **Enhance Technical Countermeasures in Florida and Gulf States:** The Department of Homeland Security (DHS) and Department of Defense should deploy advanced counter-SIGINT and counter-surveillance technologies in the Southeast U.S. This could include encryption upgrades for all communications emanating from South Florida military installations (to thwart Chinese interception from Cuba) and spectrum monitoring to detect any unusual signals interference originating from Cuba. The U.S. Air Force and Space Force, for instance, could adjust flight telemetry and communication protocols for launches at Cape Canaveral – using directional antennas or frequency-hopping techniques to minimize interceptable leakage toward Cuba. Similarly, U.S. Navy exercises in the Gulf might use secured datalinks and practice emissions control when near Cuban waters. Essentially, we must "spy-proof" our sensitive activities in the Southeast. This also means hardening Guantanamo Bay base's communications and monitoring any electronic probing from nearby Cuban territory.
2) **Deploy Aerial and Undersea Surveillance:** To better understand what China is doing in Cuba, the U.S. intelligence community should increase surveillance of the relevant sites. This could involve deploying high-altitude drones or aircraft to periodically overfly (from international airspace) areas like Bejucal and El Salao to collect signals and imagery – tracking changes in antenna arrays or unusual transmissions. Undersea, the U.S. Navy should monitor waters between Cuba and Florida for any Chinese deployment of sonar or oceanographic devices that could threaten U.S. submarines. We might also quietly work with allies who have satellite imagery capabilities to keep Cuban sites under watch.
3) **Expand Internet Access Initiatives for the Cuban People:** As recommended by experts, the U.S. can provide the Cuban public with greater connectivity independent of

state-controlled networks. This might involve supporting satellite internet services (like Starlink) for Cuba through third-party arrangements, or enabling mesh network devices to be smuggled in that create peer-to-peer communications even when Havana shuts down the web. Congress recently authorized funding for promoting internet freedom in closed societies; a portion should target Cuba specifically. By reducing the Cuban population's reliance on ETECSA (and thus Huawei-run systems), we diminish China's grip and give Cubans a taste of uncensored information.

4) **Promote Alternatives to Chinese Telecom in Latin America and Caribbean:** The U.S. should coordinate with allies (Japan, Europe, etc.) to offer competitively priced alternatives to Huawei/ZTE for countries upgrading telecom networks. While we can't change the Cuban regime's choices easily, we can ensure its Caribbean neighbors have options. This reduces regional Chinese telecom dominance and indirectly pressures Cuba if it becomes the sole Huawei-dependent network (Cuba might worry about isolation or vulnerabilities). The U.S. International Development Finance Corporation (DFC) could finance projects to roll out Nokia or Ericsson equipment in nearby nations, showing that non-Chinese 5G is viable in developing markets. Over time, if Cuba ever opens its market, those alternatives would be more attractive.
5) **Improve Regional Cyber Defense Collaboration:** Work with Western Hemisphere partners to create an early warning system for cyber threats emanating from Cuba or involving Chinese tech. For instance, if unusual traffic patterns suggest a Cuban network is being used as a launchpad for cyber intrusions (perhaps by Chinese hackers), having sensors in regional internet service providers could catch it. The U.S. Cyber Command and DHS could quietly assist willing nations (even possibly friendly telecoms in Latin America that connect to Cuba) to install monitoring that flags suspicious activity, without violating any sovereignty. Essentially, if China tries to use Cuba as a base for cyber operations against us or allies, we want to know and block it. Enhanced information sharing through the Organization of American States (OAS) cyber committee could include warnings about hardware like Nuctech or Hikvision which might harbor vulnerabilities.
6) **Scrutinize Undersea Cables and Infrastructure:** There is an initiative to build new undersea cables in the Caribbean.[xx] The U.S. should support secure cable projects and oppose any that have Chinese contractors laying the cable near U.S. waters. If China proposes linking Cuba to other cables (for redundancy beyond ALBA-1), we should rally partners to prevent Chinese firms from getting those contracts. Also, consider agreements with the Bahamas to allow U.S. inspection of cable segments near Cuba for tampering. While technical, this kind of infrastructure security is paramount since cables carry bulk communications that China may seek to tap from Cuba.
7) **Coordinate with Allies (Canada, EU, Japan) on Cuba Strategy:** The United States should consult closely with Canada and European partners who have diplomatic relations with Cuba. Many of these countries are also wary of China's global surveillance

activities. A coordinated message from multiple nations to Cuba – expressing concern about the Chinese spy installations – would be harder for Havana to ignore than just U.S. protests. For instance, Canada and select EU states could quietly let Cuba know that Chinese military bases on the island would adversely affect their relations and investment prospects. Such behind-the-scenes diplomatic leveraging might give Cuba pause about becoming too dependent on Beijing.

8) **Leverage Latin American Partners to Engage Cuba:** Countries like Argentina, Brazil, and Mexico have closer ties with Cuba and might serve as intermediaries. The U.S. can share its concerns about the Chinese bases with these partners and encourage them to raise it in their bilateral talks with Cuba. For instance, Mexico (which values strategic autonomy) might tell Cuba that a Chinese signals base so close to the U.S. could increase tensions in the region – not desirable for anyone. If Cuba hears this not just from Washington, but from fellow Latin Americans, it might carry weight.
9) **Leverage U.S. Academic Institutions to Illuminate China's Strategy in Latin America and the Caribbean:** Policymakers should invest in and partner with U.S. academic institutions to produce publicly accessible, data-driven research that exposes the breadth of China's strategic activities in Latin America and the Caribbean (LAC). Universities and think tanks—especially those with regional and language expertise—are uniquely positioned to monitor and analyze China's evolving presence in the Western Hemisphere. Their research can help fill critical intelligence gaps, shape interagency awareness, and support strategic communications to allies and the general public. One strong model is the Florida International University (FIU) Chinese Activities in Latin America Dashboard, an interactive geospatial platform that aggregates and visualizes all known Chinese investments, infrastructure projects, diplomatic exchanges, and military engagements in the LAC region.[xxi] The dashboard provides near-real-time data and mapping of critical assets, including potential dual-use deepwater ports, Chinese-built telecom nodes, Confucius Institutes, and space-enabling infrastructure such as satellite ground stations and tracking facilities. It will soon leverage AI to add risk indicators—such as port locations near chokepoints or known Chinese state-owned enterprise involvement—that help flag projects with possible national security implications.

Conclusion

Cuba is not just an outpost of Chinese influence—it is a warning. China is strategically embedding itself in the Western Hemisphere not just through trade and investment by also through ports, space, and espionage. Havana offers Beijing a "strategic support point" from which it can enhance its maritime power projection and space/SIGINT capabilities to challenge the United States—strategically and economically.

This is part of a deliberate, long-term campaign by the Chinese Communist Party to erode U.S. influence globally. The same playbook being used in Cuba—state-backed investments, dual-use infrastructure, diplomatic denial, and strategic ambiguity—is unfolding across Latin America and the Caribbean.

The United States must respond with resolve and creativity. That means investing in regional partnerships, leveraging academic research to expose malign influence, and signaling clearly that America will defend its interests in this hemisphere. Strategic neglect of our region–our shared neighborhood–is no longer an option.

References

[i] U.S. Department of Defense. Military and Security Developments Involving the People's Republic of China 2024. December 18, 2024. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

[ii] Kennedy, Conor. Strategic Strong Points and Chinese Naval Strategy. The Jamestown Foundation. China Brief Volume: 19, Issue: 6, March 22, 2019. https://jamestown.org/program/strategic-strong-points-and-chinese-naval-strategy/#:~:text=,20%2C%202017%2C%20Zhongnan%20University%20of (accessed April 25, 2025)

[iii] Zhang Wei (张炜) of the Naval Command College, "拓展海外存在与完善我军远洋战略布势" ("Expanding Overseas Presence to Perfect Our Military's Far-Seas Strategic Disposition") in China Military Science (《中国军事科学》) 2018, Issue 2, pp. 120–128 (accessed April 30, 2025).

[iv] Kennedy, Conor. Strategic Strong Points and Chinese Naval Strategy. The Jamestown Foundation. China Brief Volume: 19, Issue: 6, March 22, 2019. https://jamestown.org/program/strategic-strong-points-and-chinese-naval-strategy/#:~:text=,20%2C%202017%2C%20Zhongnan%20University%20of (accessed April 25, 2025)

[v] Office of Foreign Asset Control. Sanctions List Search–China Communication Construction Company. https://sanctionssearch.ofac.treas.gov/Details.aspx?id=30930 (accessed May 3, 2025)

[vi] Cuba Business Report Staff. Chinese-funded Terminal at Port of Santiago Opens. https://cubabusinessreport.com/chinese-funded-terminal-at-port-of-santiago-opens/ (accessed May 3, 2025)

[vii] FIU Gordon Institute. Chinese Activities in Latin America Dashboard. Security Research Hub, https://srh-fiu.maps.arcgis.com/apps/dashboards/9e25652d76774664a09e2424900e18c2 (accessed May 3, 2025)

[viii] Camacho Casado, Ledys, Nueva tecnología para la inspección de contenedores, Opciones Web, https://www.opciones.cu/turismo/-0001-11-30/nueva-tecnologia-para-la-inspeccion-de-contenedores (accessed May 3, 2025)

[ix] "U.S. Department of Transportation Maritime Administration. Worldwide-Foreign Adversarial Technological, Physical, and Cyber Influence. https://www.maritime.dot.gov/msci/2023-009-worldwide-foreign-adversarial-technological-physical-and-cyber-influence (accessed May 3, 2025)

[x] Chinese security firm Nuctech loses appeal against EU inspection. Reuters. March 27, 2025. https://www.reuters.com/technology/chinese-security-firm-nuctech-loses-appeal-against-eu-inspection-2025-03-27/ (accessed May 3, 2025)

[xi] Tatlow, Didi Kirsten. China Space Project Investigated by Newsweek Illegal, Chile Says. Newsweek. April 21, 2025. https://www.newsweek.com/china-chile-us-space-observatory-astronomy-security-2061691 (accessed April 28, 2025)

[xii] A July 19, 2022 presentation slide from the National Astronomic Observatory of China presentation. A Newsweek journalist acquired it and shared it with the author. http://101.201.56.194/events/20/files/20220718.%E5%8F%B8%E5%A4%A9%E5%B7%A5%E7%A8%8B.VO.pdf (accessed April 27, 2025)

[xiii] 中国正在全球电子间谍竞赛中努力追赶. Voice of America Mandarin Language Service. June 15, 2023. https://www.voachinese.com/a/china-s-efforts-to-catch-up-in-global-electronic-spying-race-20230614/7137720.html (accessed May 3, 2025)

[xiv] Funaiole, Matthew P., Aidan Powers-Riggs, Brian Hart, Henry Ziemer, Joseph S. Bermudez Jr., Ryan C. Berg, and Christopher Hernandez-Roy. China's Intelligence Footprint in Cuba: New Evidence and Implications for U.S. Security. CSIS. December 6, 2024. https://www.csis.org/analysis/chinas-intelligence-footprint-cuba-new-evidence-and-implications-us-security (accessed May 3, 2025)

[xv] Wang, Qi. Hyping Chinese 'spy bases' in Cuba slander; shows US' hysteria: expert. Global Times. July 3, 2024. https://www.globaltimes.cn/page/202407/1315376.shtml (accessed May 3, 2025)

[xvi] Ministry of Foreign Affairs of the People's Republic of China. China's policy documents on Latin America and the Caribbean. November 24, 2016. https://www.mfa.gov.cn/web/ziliao_674904/zcwj_674915/201611/t20161124_7949957.shtml (accessed April 26, 2025)

[xvii] Lazarus, Leland and Evan Ellis. How China Helps the Cuban Regime Stay Afloat and Shut Down Protests. The Diplomat. August 3, 2021. https://thediplomat.com/2021/08/how-china-helps-the-cuban-regime-stay-afloat-and-shut-down-protests/

[xviii] Marco Rubio X Post, August 3, 2021. https://x.com/marcorubio/status/1422596544004509700

[xix] Xynou, Maria, Arturo Filastò, Simone Basso. Measuring Internet Censorship in Cuba's ParkNets. Open Observatory of Network Interference. August 28, 2017. https://ooni.org/post/cuba-internet-censorship-2017/

[xx] Data Insight: The upcoming submarine cables for Latin America and the Caribbean. BNAmericas. November 22, 2024. https://www.bnamericas.com/en/features/data-insight-the-upcoming-submarine-cables-for-latin-america-and-the-caribbean (accessed May 4, 2025).

[xxi] FIU Gordon Institute. Chinese Activities in Latin America Dashboard. Security Research Hub, https://srh-fiu.maps.arcgis.com/apps/dashboards/9e25652d76774664a09e2424900e18c2 (accessed May 3, 2025)