



# EIB World Trade Headlines

Evolutions In Business • [www.eib.com](http://www.eib.com) • (978) 256-0438  
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

February 15, 2020 - Volume 12, Issue 4



## DECCS LIVE as of February 18, 2020!

You will be able to access your ITAR Registration and  
ITAR Licenses online.

Click below to Enroll or to learn more.

[https://www.pmdtcc.state.gov/ddtc\\_public](https://www.pmdtcc.state.gov/ddtc_public)

### NEWSLETTER NOTES

- \* DECCS will ...
- \* STAY INFORMED
- \* U.S. charges four members ...
- \* USTR Revises \$7.5 Billion A...
- \* Airbus Agrees to Pay over \$3.9 ...
- \* Consumers confused by distinction between biobased and biodegradable plastics
- \* U.S. weighs blocking GE ...
- \* Beijing's backdoors into infrastructure and technology have a name...and a far-reaching purpose
- \* Mojo Vision Sees Augmented Reality's Future Through Contact Lenses

## STAY INFORMED

ASK if you need updated Training:

EAR, ITAR, Free Trade Agreements  
Critical Technologies, Deemed Exports,  
CFIUS...

Incoterms 2020

**DEAD Incoterms**  
*Don't Use These!*



*During Audits,  
I still find DDU being used!*



EVOLUTIONS IN BUSINESS

## U.S. charges four members of Chinese military in connection with 2017 hack at Equifax that compromised data of about 145 million

In a nine-count indictment filed in federal court in Atlanta, federal prosecutors alleged that four members of the People's Liberation Army hacked into Equifax's systems, stealing personal data. In a statement announcing the case, Attorney General William P. Barr called their efforts "a deliberate and sweeping intrusion into the private information of the American people."

The 2017 breach gave hackers access to the personal information, including Social Security numbers and birth dates, of about 145 million people.

## USTR Revises \$7.5 Billion Award Implementation Against EU in Airbus Case

02/14/2020

Washington, DC – Under President's Trump leadership, the United States won the largest award in WTO history on October 2, 2019 when it was authorized to take countermeasures on \$7.5 billion in goods after a victory in its unfair trade practices case against the European Union, France, Germany, Spain, and the United Kingdom. Pursuant to U.S. statute, the United States Trade Representative is now issuing a Notice in the Federal Register making adjustments to its WTO-authorized retaliation action, which was implemented on October 18, 2019. The United States is increasing the additional duty rate imposed on aircraft imported from the EU to 15% from 10%, effective March 18, 2020, and making certain other minor modifications.

To read the Notice, click [here](#).

For additional background, click [here](#).



## Airbus Agrees to Pay over \$3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case

Airbus SE (Airbus or the Company), a global provider of civilian and military aircraft based in France, has agreed to pay combined penalties of more than \$3.9 billion to resolve foreign bribery charges with authorities in the United States, France and the United Kingdom arising out of the Company's scheme to use third-party business partners to bribe government officials, as well as non-governmental airline executives, around the world and to resolve the Company's violation of the Arms Export Control Act (AECA) and its implementing regulations, the International Traffic in Arms Regulations (ITAR), in the United States. This is the largest global foreign bribery resolution to date.

Airbus entered into a deferred prosecution agreement with the department in connection with a criminal information filed on Jan. 28, 2020 in the District of Columbia charging the Company with conspiracy to violate the anti-bribery provision of the Foreign Corrupt Practices Act (FCPA) and conspiracy to violate the AECA and its implementing regulations, the ITAR. The FCPA charge arose out of Airbus's scheme to offer and pay bribes to foreign officials, including Chinese officials, in order to obtain and retain business, including contracts to sell aircraft. The AECA charge stems from Airbus's willful failure to disclose political contributions, commissions or fees to the U.S. government, as required under the ITAR, in connection with the sale or export of defense articles and defense services to the Armed Forces of a foreign country or international organization. The case is assigned to U.S. District Judge Thomas F. Hogan of the District of Columbia.

"Airbus engaged in a multi-year and massive scheme to corruptly enhance its business interests by paying bribes in China and other countries and concealing those bribes," said Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division. "This coordinated resolution was possible thanks to the dedicated efforts of our foreign partners at the Serious Fraud Office in the United Kingdom and the PNF in France. The Department will continue to work aggressively with our partners across the globe to root out corruption, particularly corruption that harms American interests."

"International corruption involving sensitive U.S. defense technology presents a particularly dangerous combination. Today's announcement demonstrates the Department's continuing commitment to ensuring that those who violate our export control laws are held to account," said Principal Deputy Assistant Attorney General David P. Burns of the Justice Department's National Security Division (NSD).

*(\*Continued On The Following Column)*

"The resolution, however, also reflects the significant benefits available under NSD's revised voluntary self-disclosure policy for companies that choose to self-report export violations, cooperate, and remediate as to those violations, even where there are aggravating circumstances. We hope other companies will make the same decision as Airbus to report potential criminal export violations timely and directly to NSD so that they too can avail themselves of the policy's benefits."

"Today, Airbus has admitted to a years-long campaign of corruption around the world, said U.S. Attorney Jessie K. Liu of the District of Columbia. "Through bribes, Airbus allowed rampant corruption to invade the U.S. system. Additionally, Airbus falsely reported information about their conduct to the U.S. government for more than five years in order to gain valuable licenses to export U.S. military technology. This case exemplifies the ability of our prosecutors and law enforcement to work with our foreign counterparts to ensure that corruption around the world is prevented and punished at the highest levels."

"Airbus SE, the second largest Aerospace company worldwide, engaged in a systematic and deliberate conspiracy, that knowingly and willfully violated U.S. fraud and export laws," said Special Agent in Charge Peter C. Fitzhugh of U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) New York. "Airbus's fraud and bribery in commercial aircraft transactions strengthened corrupt airlines and bad actors worldwide, at the expense of straightforward enterprises. Additionally, the bribery of government officials, specifically those involved in the procurement of U.S. military technology, posed a national security threat to both the U.S. and its allies. The global threats facing the U.S. have never been greater than they are today, and HSI New York is committed to working with our federal and international partners to assure sensitive U.S. technologies are not unlawfully and fraudulently acquired. As this investigation reflects, national security continues to be a top priority not just for Department of Homeland Security, but for HSI New York." The Company's payment to the United States will be \$527 million for the FCPA and ITAR violations, and an additional 50 million Euros (approximately \$55 million) as part of a civil forfeiture agreement for the ITAR-related conduct, and the department will credit a portion of the amount the Company pays to the Parquet National Financier (PNF) in France under the Company's agreement with the PNF. In addition, the Company has agreed to pay a \$10 million penalty to the U.S. Department of State's Directorate of Defense Trade Controls (DDTC), of which the department is crediting \$5 million. In related proceedings, the Company settled with the PNF in France over bribes paid to government officials and non-governmental airline executives in China and multiple other countries and the Company has agreed to pay more than 2 billion Euros (more than approximately \$2.29 billion) pursuant to the PNF agreement.

*(\*Continued On The Following Page)*

As part of this coordinated global resolution, the Company also entered into a deferred prosecution agreement with the United Kingdom's Serious Fraud Office (SFO) over bribes paid in Malaysia, Sri Lanka, Taiwan, Indonesia and Ghana, and the Company has agreed to pay approximately 990 million Euros equivalent (approximately \$1.09 billion) pursuant to the SFO agreement. The PNF and SFO had investigated the Company as part of a Joint Investigative Team.

According to admissions and court documents, beginning in at least 2008 and continuing until at least 2015, Airbus engaged in and facilitated a scheme to offer and pay bribes to decision makers and other influencers, including to foreign officials, in order to obtain improper business advantages and to win business from both privately owned enterprises and entities that were state-owned and state-controlled. In furtherance of the corrupt bribery scheme, Airbus employees and agents, among other things, sent emails while located in the United States and participated in and provided luxury travel to foreign officials within the United States.

The admissions and court documents establish that in order to conceal and to facilitate the bribery scheme, Airbus engaged certain business partners, in part, to assist in the bribery scheme. Between approximately 2013 and 2015, Airbus engaged a business partner in China and knowingly and willfully conspired to make payments to the business partner that were intended to be used as bribes to government officials in China in connection with the approval of certain agreements in China associated with the purchase and sale of Airbus aircraft to state-owned and state-controlled airlines in China. In order to conceal the payments and to conceal its engagement of the business partner in China, Airbus did not pay the business partner directly but instead made payments to a bank account in Hong Kong in the name of a company controlled by another business partner.

Pursuant to the AECA and ITAR, the DDTC regulates the export and import of U.S. defense articles and defense services, and prohibits their export overseas without the requisite licensing and approval of the DDTC. According to admissions and court documents, between December 2011 and December 2016, Airbus filed numerous applications for the export of defense articles and defense services to foreign armed forces. As part of its applications, Airbus was required under Part 130 of the ITAR to provide certain information related to political contributions, fees or commissions paid in connection with the sale of defense articles or defense services. The admissions and court documents reveal, however, that the Company engaged in a criminal conspiracy to knowingly and willfully violate the AECA and ITAR, by failing to provide DDTC with accurate information related to commissions paid by Airbus to third-party brokers who were hired to solicit, promote or otherwise secure the sale of defense articles and defense services to foreign armed forces.

*(\*Continued On The Following Column)*

As part of the deferred prosecution agreement with the department, Airbus has agreed to continue to cooperate with the department in any ongoing investigations and prosecutions relating to the conduct, including of individuals, and to enhance its compliance program.

For the FCPA-related conduct, the department reached this resolution with Airbus based on a number of factors, including the Company's cooperation and remediation. In addition, for the FCPA-related conduct, the U.S. resolution recognizes the strength of France's and the United Kingdom's interests over the Company's corruption-related conduct, as well as the compelling equities of France and the United Kingdom to vindicate their respective interests as those countries deem appropriate, and the department has taken into account these countries' determination of the appropriate resolution into all aspects of the U.S. resolution.

With respect to the AECA and ITAR-related conduct, the department reached this resolution with Airbus based on the voluntary and timely nature of its disclosure to the department as well as the Company's cooperation and remediation.

HSI's New York Field Office Counter Proliferation Investigations Group is investigating the case. Deputy Chief Christopher Cestaro, Assistant Chief Vanessa Sisti and Trial Attorney Elina A. Rubin Smith of the Criminal Division's Fraud Section, Deputy Chief Elizabeth L. D. Cannon and Trial Attorney David Lim of the National Security Division's Counterintelligence and Export Control Section, and Assistant U.S. Attorneys Michelle Zamarin, Gregg Maisel, David Kent and Karen Seifert of the District of Columbia are prosecuting the case. The Criminal Division's Office of International Affairs provided assistance.

The Department of Justice acknowledges and expresses its appreciation of the significant assistance provided by France's Parquet National Financier and the UK's Serious Fraud Office. The Fraud Section is responsible for all investigations and prosecutions of the Foreign Corrupt Practices Act, and conducts other investigations into sophisticated economic crimes. The Counterintelligence and Export Control Section supervises the investigation and prosecution of cases involving the export of military and strategic commodities and technology, including cases under the AECA and ITAR.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at [www.Justice.gov/Celebrating150Years](http://www.Justice.gov/Celebrating150Years).

## Consumers confused by distinction between biobased and biodegradable plastics

By:

Clare Goldsberry

The difference between biobased and biodegradable plastics is confusing to the average consumer, to say the least. When I read a new report claiming that consumers are demanding “environmentally friendly” packaging, I had to wonder if they actually know what they are demanding.

The latest global survey commissioned by ING Research shows “consumer attitudes have reached a tipping point, leading them to avoid brands that don’t prioritize sustainability and environmental issues. Despite demanding change, customers will still engage in the linear ‘convenience economy’ model of ‘take, make and waste’ unless companies offer a more seamless transition toward the ‘circular economy,’” said the report, “Learning from consumers: How shifting demands are shaping companies’ circular economy transition.”

Consumers generally want the products they buy to be “environmentally friendly,” but many studies have shown that consumers won’t pay more for these products, and that consumers overall are not educated enough to know the various options being offered by brand owners. Many terms are bandied about that add to the confusion—biobased/bioplastics, biodegradable and compostable, recycled content and recyclable. These terms often are ambiguous.

For example, almost anything can be recycled in one way or another. But is it truly recyclable in a way that recovers the value of the material so that it is used in more products?

Compostability is a real conundrum: Where can a product be composted? How long will it take? Does compostable plastic really break down into actual soil, as some claim?

Terravive, a Richmond, VA–based startup founded by Julianna Keeling, promises to solve the world’s plastic waste problems by developing a class of polymers similar in function to polyethylene. Keeling’s research has resulted in a line of products that look like plastic, “but can break down in any natural environment the same way a leaf or orange peel would, hence the name Terravive from the Latin words for Earth and life. Quoted in an article in American Innovation, Keeling said, “it’s all about the idea that the Earth can sustain itself. We use materials that have the ability break down in soil, so in your backyard, in an industrial compost, in a landfill, in the ocean, waterways—no matter where [the products] end up, as a consumer you can rest assured that [they] are going to break down cleanly and fully.”

*(\*Continued On The Following Column)*

That’s a big promise for a plastic-like material similar to polyethylene that has been proven to fragment—but not break down completely—in soil or other environments. It appears from the article that Terravive is a biobased plastic, or bioplastic, but as a recent market study from Ceresana notes, “bio” is not always compostable.

“Bioplastics can be used in a growing number of application areas,” explained Oliver Kutsch, CEO of Ceresana, who noted that polylactic acids, starch blends, cellulose and other bioplastics achieve significantly higher growth rates than conventional plastics made of mineral oils or natural gases. The report’s summary quickly points out, however, that “bio is not always compostable.”

“Two groups of materials are called bioplastics, although they are not necessarily identical: There are biodegradable plastics that can be composted, as well as bio-based plastics that are made of renewable resources but are not biodegradable. Biodegradable plastics, such as polylactic acids (PLAs) and polymers based on cornstarch, reached a market share of 56% of the total market for bioplastics in 2018. Ceresana predicts volume growth of 7.1% per year up until 2026 for this product group. Biobased plastics such as polyethylene, PET or PA made of sugar cane, which are not biodegradable, are expected to experience weaker growth, at 5.1% per year.

At the International Elastomer Conference in Cleveland last year, Ramani Narayan, distinguished professor at Michigan State University, stated in his keynote address that biobased and biodegradable are useless terms “unless people understand what they mean and how they work scientifically.” The keynote, “Biobased, biodegradable polymers may not be as eco-friendly as you think,” was reprinted in the Oct. 8, 2019, edition of Rubber & Plastics News.

“It is wrong, misleading and deceptive to use ‘biodegradable’ in an unqualified way,” Narayan said, noting that the “careless use of the term in advertising is forbidden by the Federal Trade Commission and the state of California,” which “fined Amazon \$1.5 million for advertising bogus ‘biodegradable’ products on its website.”

Narayan then explained that “biobased signifies whether the carbon content in any substance comes from organic sources, such as plants and agricultural sources, rather than fossil sources such as oil and coal.” A product promoted as “biobased” doesn’t make it “biodegradable,” according to Narayan. “Biobased addresses a product’s origins, while ‘biodegradable’ addresses end-of-life issues,” he said. “One does not equate the other.”

“Biodegradability is as complex as the types of polymer chemistry and types of microbes that degrade the polymer chemistry,” explained Salvatore Monte, President of Kenrich Petrochemicals Inc. (Bayonne, NJ), a producer of coupling agents, plasticizers and specialty chemicals.

## U.S. weighs blocking GE engine sales for China's new airplane: sources

(Reuters) - The U.S. government is considering whether to stop General Electric Co from continuing to supply engines for a new Chinese passenger jet, according to people familiar with the matter, casting uncertainty over China's efforts to enter the civil aviation market.

The potential restriction on the engine sales - possibly along with limits on other components for Chinese commercial aircraft such as flight control systems made by Honeywell International Inc - is the latest move in the battle between the world's two largest economies over trade and technology.

The issue is expected to come up at an interagency meeting about how strictly to limit exports of U.S. technology to China on Thursday and at another meeting with members of President Donald Trump's Cabinet set for Feb. 28, sources said.

The White House and the U.S. Commerce Department, which issues licenses for such exports, declined to comment, as did a GE spokeswoman. The departments of Defense, State, Energy and Treasury did not respond to requests for comment.

For years, the United States has supported American companies' business with China's budding civil aviation industry.

The government has provided licenses that allow those companies to sell engines, flight control systems and other components for China's first large commercial aircraft, the COMAC C919. The narrow-body jet has already engaged in test flights and is expected to go into service next year. COMAC is an acronym for Commercial Aircraft Corp of China Ltd.

But the Trump administration is weighing whether to deny GE's latest license request to provide the CFM LEAP-1C engine for the C919, people familiar with the matter said, though GE has received licenses for the LEAP engines since 2014 and was last granted one in March 2019.

The CFM LEAP engine is a joint venture between GE and France's Safran Aircraft Engines. The proposal to halt the deliveries of the engines was also reported on Saturday by the Wall Street Journal.

Safran did not immediately respond to a request for comment, and French government officials could not be reached for comment.

*(\*Continued On The Following Column)*

Aside from aircraft engines, flight control systems are up for discussion at the February meetings. Honeywell International has received licenses to export flight control systems to COMAC for the C919 for about a decade, and one was approved in early 2020, according to a person familiar with the matter.

But future permission for such sales for COMAC's passenger aircrafts may be up for debate. Honeywell also has been seeking a license for flight control technology to participate in the development of the C929, China's planned wide-body jet venture with Russia, the person said.

The flight control system operates moving mechanical parts, such as the wing flaps, from the cockpit.

A spokeswoman for Honeywell declined to comment.

An aerospace trade group official said his organization would like to weigh in on any policy shifts.

"If there are any changes, we would hope they would engage with us, as they've done before," said Remy Nathan, vice president for international affairs at the Aerospace Industries Association.

At the heart of the debate over a possible crackdown on the sale of U.S. parts to China's nascent aircraft industry is whether such shipments would fuel the rise of a serious competitor to U.S.-based Boeing Co or boost China's military capabilities.

People familiar with the matter said some administration officials are concerned the Chinese could reverse engineer some items, though others say an abundance of LEAP engines in China has not brought that about to date.

If the United States were to move ahead with the measure, one person familiar with the matter said, China could retaliate by ordering more planes from Airbus SE, rather than crisis-hit Boeing, which relies on China for a fourth its deliveries.

The Trump administration's meetings about technology issues also are set to include a discussion of whether to impose further restrictions on suppliers to Huawei Technologies, the world's largest telecommunications equipment maker, which is on a U.S. trade blacklist.

## Beijing's backdoors into infrastructure and technology have a name...and a far-reaching purpose

U.S. national security advisor Robert O'Brien recently sought to shut down debate about whether China tech giant Huawei installs "backdoors" in its gear. "We have evidence," O'Brien announced on February 11, 2020, that wireless networks around the world have been compromised with access points that Beijing mandates. Well known are the concerns this raises for sensitive public and private sector data. Less understood is just how comprehensive Beijing's strategy is—and how extensive its reach.

### Issue

The Communist Party of China (CPC) directs the insertion of economy-wide commercial and communication infrastructure with "embedded and reserved interfaces [内部嵌入和预留接口]" that wire the world for access by PRC intelligence and security forces in service of Beijing's technological and geostrategic goals.

### Implications

Beijing's potential to command and control key economic and information flows compromises public and private sectors and alters the character and trajectory of open markets and honest global governance.

### Actions

Commercial entities need to assess their connectivity to PRC entities from a continuity of operations perspective and for information security purposes. Governments need to illuminate and effectively communicate CPC disruptive capabilities to the private sector, forging opportunities to act on shared interests.

### WE SAY BACKDOORS, BEIJING SAYS RESERVED INTERFACES

The CPC is using internal government directives to mandate that Peoples Republic of China (PRC) manufacturers of information and communication hardware embed and reserve access for CPC agents at times of its choosing into a wide swath of sectors, including major infrastructure, industrial, and service systems. "Backdoors" is the common parlance in English. The CPC refers more explicitly to "embedded and reserved interfaces [内部嵌入和预留接口]," or close derivative terms, which likely include other vulnerabilities beyond backdoors that can be inserted and exploited by CPC actors. These interfaces hard wire an information-technology dependent world for seamless access and abuse by PRC intelligence and security forces. Here's what we know:

*(\*Continued On The Following Column)*

Since about 2015 and in conjunction with CPC General Secretary Xi Jinping's Military Civil Fusion (MCF) program to make PRC defense and intelligence an all-of-society enterprise, Beijing's central and provincial commissions and military commands have issued directives mandating the structural tapping of devices and systems across economic sectors. The CPC's official daily from March 2015 calls for "the implementation of defense requirements through embedded and reserved interfaces" [内部嵌入和预留接口]. This report follows remarks that month by Xi to a PLA delegation at the National People's Congress where he called for the in-depth implementation of MCF strategy in the interest of building a strong and resurgent military.

"Reserved interfaces" or "interfaces" are common terms in computing and IT literature, but here the term defies the common technical engineering objective of assuring interoperability. The backdoors Xi mandates must grant CPC agents convenient future data collection and operational access across transportation, information and communication, Internet of Things (IoT), and other "smart" infrastructure. ECONOMIC, NATIONAL SECURITY IMPLICATIONS FOR THE U.S. AND OTHERS

"Reserved interfaces" provide Beijing with global capabilities to command and control key economic and information flows. They also allow for penetration of U.S. and allied systems and institutions to collect intelligence, disrupt operations, steal economic advantage, and co-opt them for the PLA's operational purposes whenever requested. A raft of PRC laws and strategies—like MCF, which also includes relevant economic mobilization for defense plans, and Made in China 2025—require it.

These actions and laws in turn facilitate Beijing's economic development and geostrategic strategies. For example, the "Innovation Driven Development Strategy," a keystone PRC plan to boost China's status as a technological superpower, benefits from industrial-scale acquisition of foreign technology and know-how, by any and all means.

Embedded and reserved interfaces threaten the United States and the global economy much more than simply providing the CPC additional espionage and data accumulation opportunities. Intent is also a significant factor. Recall in 2019 when electric vehicle pioneer Tesla, a commercially resourced company, remotely added battery capability to cars in Hurricane Dorian's path. But imagine what a state-resourced actor with malevolent intent could accomplish. With backdoors, for example, the CPC now has the capability to attenuate systems that connect to a wide range of remote controllers.

*(\*Continued On The Following Page)*

## Mojo Vision Sees Augmented Reality's Future Through Contact Lenses

Even if you're a fan of cyberpunk science fiction, the idea of contact lenses with augmented reality (AR) capability seems sufficiently out of reach for today's technology. Some might even call the task of creating such a thing impossible. And that's the way the team at Mojo Vision likes it.

Attendees at CES 2020 got their first glimpse of the technology Mojo Vision is developing – contact lenses that act as miniature displays – essentially giving wearers a heads-up display akin to something out of Black Mirror. The prototype on display wasn't wearable, but it did showcase that the company is able to project images onto a contact lens form factor. Founded by a team of engineers and serial entrepreneurs, Mojo Vision is arguably one of the more bold companies to enter the AR and mixed reality (MR) space. Should they achieve their goal, the company's founders believe they can completely transform the technological landscape. Shimadzu's AGX-V Series testers combine world-class performance with optimal operability and enhanced safety features for both QC and R&D applications. Intuitive software improves productivity while allowing easy creation of methods. Speaking with Design News, Mike Wiemer, the CTO and co-founder of Mojo Vision, said the origins of the company came simply from the search for "a good problem to solve." His search for new business opportunities led him to meet Drew Perkins, a serial entrepreneur with a background in photonics as well as optical and networking technologies, and Michael Deering, whose engineering background includes developing graphics hardware as well as VR/AR technologies. Perkins and Deering would go on to become Mojo Vision's CEO and CSO respectively.

**NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.**

**Reproduction for private use or gain is subject to original copyright restrictions.**

Through embedded interfaces a remote actor could stop a ship bridge from raising as ocean traffic approaches and cause a collision that catastrophically interrupts ocean to river or port traffic.

Remote controllers could cause engines in power plants to overspeed, overheat, and damage their capability to generate electricity for hospitals, factories, storage facilities, server farms, offices, and neighborhoods.

Potentially fatal catastrophes attach to systems that manage access to traffic lights, tunnels and bridges, airports, and dams.

NEXT STEPS FOR PRIVATE, PUBLIC SECTORS

All of this puts the reported security vulnerabilities in Huawei gear in a new light. For example, in a 2019 report, the UK's Huawei Cyber Security Evaluation Centre warned that Huawei had failed to address concerns about its software development and engineering practices. It also noted that the country's National Cyber Security Centre did not "believe that the defects identified are a result of Chinese state interference."

"Believing" is no longer good enough. Both business and government should revisit assessments like this given what we now know about "reserved interfaces."

And until further information comes to light on the extent the CPC has succeeded in implementing its plans, any PRC part, product, firm, subsidiary, or partner should be viewed as a potential vector, wittingly or not.

Companies should review the extent they are dependent on PRC firms, not only for supply chain risks but also for vulnerabilities in their command and control, economic, technology, and information security.

Traditional infrastructure like ports and associated logistics operations should review and address vulnerabilities in sensitive transportation information, to include U.S. military movements.

Infrastructure operations—airports, power plants, subways, bridges, financial exchanges, etc.—could suffer annoying to catastrophic impairments due to foreign sovereign interference. They must balance hardening systems with assuring resilience as well.

Both private and public sectors must increasingly engage with each other constructively to understand and respond to this shared risk.

*"Some people dream of success while others wake up and work hard for it."*