SOURCEREE

NATIONAL SECURITY NEWSLETTER

JULY 2023

- Regulation Must Focus on "Outcomes" not "Rules"
- While Burning Contractors and Suppliers, Nexius's Façade Exposed a Possible Terrorist Cell Site Security Hole
- Fore! Reasons Why the Committee on Foreign Investment in the United States won't Block the PGA Tour/LIV Golf Merger
- Decoding Chinese Politics

July 2023 Newsletter

National Security Investment Reviews

Issue 1: Regulation Must Focus on "Outcomes" not "Rules"

The Challenge of Dynamism in Geopolitics, Technology, and Standards Setting
Research by: John Lash, PhD

Issue: Cybersecurity regulations for critical infrastructure should represent an outcome-based proactive approach that governs the entire information technology supply chain, rather than a rules-based system that focuses primarily on "foreign adversaries" (including China). Establishing outcome-based requirements for reducing / mitigating risks, a rigorous process of ongoing monitoring and evaluation, and addressing the systemic threat landscape provides for a more secure, transparent, and accountable cybersecurity standard for critical infrastructure.

BLUF: **Focusing on specific countries of origin (i.e., "foreign adversaries") may prove to be counterproductive to the ultimate goal of securing critical infrastructure, as it shifts the focus from objective standards across the cyber ecosystem to country-specific risks.**

- To be clear, there are domain specific risks (i.e., technical threat vectors) as well as context specific risks (i.e., country-specific threats); however, does this focus consider appropriately whether this trusted status for allied nation companies overlooks the interconnectedness of the industry?
  - Does it include an evaluation of the extensive presence in China of the trusted companies, deep relationships with Chinese suppliers along the technology supply chain, and market access activities in China that these trusted companies conduct?
  - Does it consider the possibility of a malicious actor launching an attack through a trusted supplier (e.g., SolarWinds or Microsoft Exchange Server)?
  - To what extent, if any, is the risk assessment lowered for trusted suppliers or countries?

Microsoft Warns *China* Hackers Attacked U.S. Infrastructure: In May 2023, Microsoft reported that it uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises. In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible.

Outcomes vs Rules: Managing the evolution of technology with outcomes, not rules, deconstructs the issues into the most foundational elements, separates assumptions from facts, and constructs a view of a secure ecosystem from the ground up – providing flexibility to address the potential threats of new technologies, while not stifling innovation and progress.

The Key Question: What is the *outcome* that the government and industry are seeking to achieve? This should not be focused on a specific technology nor country of origin, but rather – how do we develop a standard to meet this desired outcome?

- A basic example of an "outcome-based" regulation: Speed limits on roads. The regulators wanted to control the "outcome" of "the maximum driving speed is X" – but in doing so, they did not place "rules" on which countries or manufacturers could produce vehicles, nor did they place a "rule" on horsepower or top speed capability of a vehicle.

The Risk of Overemphasizing Country-Risk: Risks exist in all vendors for information technology and networking equipment regardless of the country of origin. Decisions about how to manage risks related to information technology and network equipment providers should avoid being locked in a logic that focuses entirely on the fear and presence of a specific company or country, and rather on the associated risks, assessments, mitigation, costs, and consequences that are objectively applied industry wide.

However, as noted by Tom Wheeler, former Chairman of the FCC, while recognizing legitimate concerns raised by certain equipment in U.S. networks, the risks associated [with 5G] *should not focus exclusively on specific equipment suppliers or countries of origin*:

> ***The hyperbolic rhetoric surrounding the Chinese equipment issues is drowning out what should be a strong national focus on the full breadth of cybersecurity risk factors*** *[facing 5G. We should not confuse 5G cybersecurity with international trade policy].*
> *– Tom Wheeler, Former Chairman of the FCC*

The principles for secure development, deployment, and maintenance telecommunications equipment must follow universal security standards applied to all suppliers – regardless of where the product is manufactured or deployed – with the verification process continually updated to adapt and reflect the dynamic nature of the current cybersecurity environment.

Expert Perspectives: As part of the research process on these complex issues, experts in national security, cybersecurity, and technological innovation were interviewed, with key preliminary observations aggregated for further consideration. This line of inquiry established a focus on the pros and cons of country-specific risk reviews as compared to holistic cybersecurity strategies.

Cybersecurity Risk – Domain vs Country

- Systems need to be securely built with universal standards that are continually monitored. Voluntary frameworks, particularly for the Defense Industrial Base and for companies within critical infrastructure, are ineffective to accomplish goals of security. Stronger oversight mechanisms and regulatory controls are necessary in the cyber domain.
- Foreign adversaries, specifically China, have the capabilities to commit cyber espionage without the use of Chinese-origin equipment or networks. The capability to do so through so-called "trusted" suppliers or equipment is often more effective.
- A significant concern that should be raised is how governments and private sector entities are addressing cybersecurity requirements – how secure are the products, how are they evaluated, what are the standards?
- It is undeniable that risk taxonomies between countries are different, and as such they'll be treated differently; however, there needs to be a baseline risk assessment.
- The focus should be on "de-risking" rather than "de-coupling" from certain vendors based on headquarters, manufacturing, or development locations – particularly when supply chains and talent pools are interconnected across geographic domains.
- The cyber domain cannot be zero risk; what we need to look at is what can be done given the known constraints and make risk-informed decisions.

Issue 2: While burning contractors and suppliers, Nexius's facade exposed a possible terrorist cell site security hole

Source: https://wirelessestimator.com/articles/2023/while-burning-contractors-and-suppliers-nexiuss-facade-exposed-a-possible-terrorist-cell-site-security-hole/

Considerations:

- As Nexius used 'every trick' to keep contractors working, although the company knew they would never pay them, the wireless infrastructure developer reportedly continued scamming T-Mobile by using a Nexius-aligned company in Lebanon that was prohibited from accessing T-Moble's network – possibly exposing a network security threat to the nation's second-largest mobile operator, according to sources familiar with the ruse.
- When Nexius and its umbrella companies closed their doors earlier this year, MasTec Network Solutions (MNS) had already completed an arrangement with Nexius's secured lender, PNC Bank, to acquire Nexius's assets, but none of the debt owed to vendors, suppliers, and contractors. The deal had reportedly been put together in less than 30 days.
- T-Mobile uncovers Nexius's offshore tech support scam
    - To assist subcontractors' technicians and their techs in addressing their maintenance and installation tickets for carrier builds that Nexius was managing, the company developed a stateside team of around 15 technicians to assist with any PIM or other issues that occurred, as well as provide NOC support.
    - "At first," said one employee, "we became aware that Novelus was handling some of the tickets in Lebanon, and we were informed it was okay since it was a Nexius company."
    - However, he said although he worked with them because they needed to be more knowledgeable, he became unnerved that he might be training his replacement.
    - "I don't know what they were being paid, but it must have been at least one-third or less of what we made," said another tech. "We had a central server, a tool developed by Nexius called the remote server app (RSA), and I would take a ticket to work on and start adding my notes. Then when I refreshed it, the ticket had been taken by a Lebanese tech," he said. "This happened too often, and to others stateside as well."
    - According to two sources, Nexius continued to use Novelus for tech support. However, the software-centric company used a virtual private network or another method to spoof their location so that it appeared that support services were being conducted in the U.S.
- **AT&T was also managed offshore by Novelus**
    - Nexius and Novelus teams managed AT&T's trouble tickets and alarms without the carrier being concerned about Novelus's Beirut location.
    - However, it's possible that they weren't aware of Nexius's offshore participation or that it wasn't a concern. In late 2022 and early 2023, Nexius laid off many of its stateside network help desk technicians but continued supporting AT&T with its Lebanon technicians. Reportedly, Novelus is still used for their XTAC NOC, integration, RF, IT, and HR services and other platforms.
    - An AT&T media representative informed Wireless Estimator that they would find out if AT&T allows offshore technical assistance to provide services to U.S. companies maintaining their network cell sites and new builds. Still, they did not reply to multiple follow-up requests.
- **Cell site security could be easily compromised**

- According to three technicians interviewed by Wireless Estimator, cell site security should be a primary concern of carriers when they allow a contractor's support team to access the nodes in their cell site network to assist with trouble tickets.
- The techs had access to T-Mobile's nodes. Still, they were primarily dedicated to AT&T's sites and said they would assist their tower or subcontracted crews whenever there was an alarm or installation problem.
- Although they could often talk the crew through a procedure to manage the problems, they would frequently have to access the base station by logging into the carrier's network through a third-party application on their desktop that generated an encrypted password that would be used along with their assigned user identification number (UID). Once past a firewall, they would have complete control of the node's operational support system (OSS) and be able to view and manage all of the power settings, down tilt, PIM, and other levels and address and close an alarm.
- Although they're required to request permission from AT&T's NOC support to perform a soft or hard system lock, they maintain complete control of the site and would never shut off a site without permission; but they said they still kept full control.
- They explained that nothing would prevent them from simultaneously opening multiple sites in a cluster and locking them down. In addition, they could close down AT&T's FirstNet, the mission-critical wireless network for first responders and public safety professionals that doesn't compete with commercial networks.
- They said that they believed if a lousy actor had access to the OSS, they could create havoc and purposely collapse a wide area of cell coverage to carry out a criminal or terrorist act. They acknowledged that it is likely that AT&T, Verizon, T-Mobile, and other carriers have contingency plans in place to restore service if a malicious attack on any part of their network occurs. Still, they are convinced that it wouldn't be resolved immediately if a compromised technician set up their scripts, changed site configurations, deleted optical links, and put in place other barriers.
- They noted that often the carrier is only aware of a problem an hour or two later, mainly if the shutdown or other alarm occurs during their night-time maintenance window hours. "It's simple," said one technician, "Once you are allowed into the network, it's like someone giving you a key to the front door to their business. You're allowed to open doors elsewhere in the company, but when there is another locked door, it's not so difficult to force that open and steal whatever is in there or create mayhem."

- **U.S. State Department: It's easy for China to hack telecom infrastructure**
  - Although telecom hackers are more commonly focused on espionage, ransomware, and selling data, it's seldom that their effort is to disrupt network signals. However, the software-related infrastructure required to achieve 5 G's favorable capabilities invites a variety of security vulnerabilities and opportunities.
  - After learning last month that China could launch cyber attacks against critical infrastructure, as the U.S. State Department revealed, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) said it was working to understand "the breadth of potential intrusions and associated impacts."
  - "In these cases, the adversary is often using legitimate credentials and legitimate network administration tools to gain access to execute their objectives on a target network," said CISA's executive assistant director, Eric Goldstein, in a Reuters interview, adding credibility to the possible scenarios envisioned by telecom technicians that someone could use their credentials to create a significant outage or an even greater terrorist action.

Issue 3: Fore! reasons why the Committee on Foreign Investment in the United States won't block the PGA Tour/LIV Golf merger

Source: https://www.atlanticcouncil.org/blogs/new-atlanticist/fore-reasons-why-the-committee-on-foreign-investment-in-the-united-states-wont-block-the-pga-tour-liv-golf-merger/

Considerations:

Highlights

On June 6, the PGA Tour and LIV Golf announced their plans to merge. This surprise revelation set off a wave of anger from US politicians, professional golfers who had turned down lucrative offers from LIV Golf to play in their tournaments, and others who view the PGA Tour's new association with the Saudi Arabia Public Investment Fund (PIF), which owns LIV Golf, as unpatriotic and antithetical to democratic values.

The criticism stems from the kingdom's connection to the 9/11 attacks, its track record on human rights, and the high-profile killing of US-based journalist Jamal Khashoggi in 2018, very likely at the direction of Saudi Crown Prince Mohammed bin Salman. Some critics have started to search for potential regulatory tools to block the deal. Merger review, both in the United States and Europe, seems the most likely path. However, there are competing views on whether courts would be persuaded by anti-trust arguments given how highly concentrated professional golf already is and how most US professional sports leagues operate as de facto monopolies.

Several members of Congress, including Senator Ron Wyden (D-OR), Senator Mitt Romney (R-UT), and Congresswoman Maxine Waters (D-CA), have issued public calls for the Committee on Foreign Investment in the United States (CFIUS) to review the deal. CFIUS is an interagency committee that evaluates the national security implications of foreign acquisitions of US businesses. If CFIUS finds a national security risk, it can negotiate mitigation agreements with transaction parties to restructure deals in ways that sufficiently reduce those risks. It can also recommend that the US president prohibit the transaction. CFIUS has traditionally been restrained in its approach; only seven transactions have been prohibited through the CFIUS process since 1975, though a good deal more were voluntarily abandoned by parties after realizing that CFIUS found a national security risk that it did not deem mitigable.

So is CFIUS the answer to the prayers of those who wish to stop the PGA Tour/LIV Golf merger? Probably not. To understand why CFIUS is likely not able to stop this deal, even if US lawmakers may view the deal as distasteful, it's necessary to understand CFIUS's jurisdiction—which it likely has over this deal—and the investment prohibition authorities that CFIUS provides the US president.

The committee is wary of overextending its authority

First, CFIUS has jurisdiction over any foreign acquisition of a controlling stake in a US business, regardless of the US business activity. It also has the ability to review non-controlling transactions that confer special rights—such as access to non-public technical information or board observer

status—if foreign entities invest in critical technology, critical infrastructure, or sensitive personal data of US businesses. The cross-sectoral nature of CFIUS jurisdiction contrasts with the investment screening authorities of many other advanced economies, which often only allow review of transactions in specified sectors, such as critical infrastructure or defense materials.

Thus, as long as the merger deal—which apparently exists only conceptually at the moment—directly or indirectly confers a controlling stake of PGA Tour to PIF, CFIUS will be able to review the transaction. CFIUS likely would also be able to review even a non-controlling stake if the PGA Tour meets the definition of a sensitive personal data business. CFIUS operates mostly through a voluntary notification process, but it can also pull a concerning transaction into its orbit through a "non-notified" review.

Just because CFIUS has jurisdiction to review does not mean that it will block the transaction. CFIUS is designed to be a tool of last resort and to only intervene when national security is threatened. To act, the committee would have to find a risk arising from the transaction that threatened to impair US national security. While national security is not defined in the statute, the committee process is designed to be fact-based, deliberative, and restrained. Highly attenuated risk scenarios are unlikely to persuade the committee to recommend action.

Moreover, the committee is conscientious not to overextend its authority in order to retain process legitimacy, as it operates largely through the voluntary cooperation of transacting parties. It is careful to stay within its statutory authority to prevent legal risks that could narrow its ability to act in the future. And, as the United States is actively encouraging partners and allies to enact and strengthen their own investment screening mechanisms, it does not want to give the impression that broad use of such power is legitimate, for fear that doing so could lead to other countries harming US businesses operating abroad.

Data collection risks can be mitigated

The CFIUS process revolves around determining whether a transaction creates a national security risk, and if so, whether that risk can be adequately mitigated through a legal agreement with the parties. CFIUS evaluates the vulnerabilities to national security that a US business generates and the likelihood that the foreign entity will exploit those vulnerabilities or make it easier for a third party to do so.

One potential security vulnerability is the PGA Tour's collection of fans' data on its fans through ticket sales and its smartphone app. Since the 2018 legislative update to CFIUS, the committee has been increasingly concerned about how acquiring a US business could aid a threat actor in the collection, use, and sharing of sensitive personal data. Data collected on smartphone apps can be particularly concerning if the app allows for real-time geolocation of individuals and if the app's data collection does not adequately protect vulnerable populations. However, these concerns can easily be mitigated by preventing PIF or its agents from having access to such data. It is highly unlikely that the business rationale for the merger depends on PIF or LIV Golf being able to access these data, so it is likely a mitigation term to which the parties would agree.

Real estate concerns can be mitigated, too

Another issue is the roughly thirty golf courses the PGA Tour owns and operates through its Tournament Players Club (TPC) network. Some of these golf courses are located close to sensitive US government sites such as military bases. CFIUS views such "co-location" as risky because it can

create opportunities for surveillance. In 2012, for example, US President Barack Obama prohibited a Chinese investment in an Oregon wind farm over concerns that Beijing could use access to wind turbines to surveil a particularly sensitive military site close by. Again, however, the deal could easily be structured in a way in which PIF did not have access rights to these courses or the ability to choose venders to operate or maintain these locations.

Soft power is a soft argument

Some have argued that CFIUS should consider the "soft power" implications of golf tour ownership from which the Saudis could benefit. However, it is unlikely that CFIUS will be willing to make strong claims about national security risks on this basis. Nor should it. Soft power by its nature is diffuse. This means that the consequence of soft power on US national security is difficult to clearly express. A poorly articulated consequence reduces the ability of the committee to act. After all, the committee must find a "risk to national security arising from the transaction" to mitigate or recommend a presidential prohibition. Vague claims to "sportswashing" and generally burnishing a regime's brand do not meet this threshold. If CFIUS could block transactions on bad vibes alone, then it could pretty much block anything. And that would undermine the argument that CFIUS is a fact-based, non-partisan committee that narrowly and soberly assesses national security risk. This would have substantial negative consequence for the legitimacy of the process in the eyes of business, the public, and allies and partners.

In sum, there are many reasons to be angered by, or at least uncomfortable with, the PGA Tour/LIV Golf merger. Anti-trust may represent a legitimate hurdle to its execution. But CFIUS is not a trump card to prohibit every problematic foreign transaction, and it certainly is not an appropriate tool for blocking this particular merger given what we know about it. Rule of law means the law is not just a tool but also a constraint. And here, the rule of law will likely bind the United States against using CFIUS to block a transaction some lawmakers are wary of but does not rise to the level of a clear national security risk.

Issue 4: Decoding Chinese Politics

Source: https://asiasociety.org/policy-institute/decoding-chinese-politics

Considerations:

China is one of the most important but least understood countries in the world. Its decisions will shape the future of international business, diplomacy, and security. This product helps decode the "black box" of Chinese politics through interactive visualizations and explainer essays that map formal institutions, informal networks, key decision-makers, and major policy trends. The homepage analyzes China's top leadership, while subpages analyze specific policy areas: Economy and Trade; Energy and Environment; Finance; Foreign Affairs; Hong Kong, Xinjiang, and Tibet; Military; Security; and Technology

Decoding Chinese Politics has four main objectives: (1) to explain structures of decision-making power within the Chinese system; (2) to assess the impact of changes in China's leadership across key policy areas; (3) to evaluate General Secretary Xi Jinping's continuing level of personal, factional, and ideological control over the Chinese political system; and (4) to identify rising leaders within the next generation of Chinese leadership and assess their expected impact on Chinese politics and policy.

Currently, the project analyzes political institutions and leaders across ***eight key policy areas: Economy and Trade; Energy and Environment; Finance; Foreign Affairs; Hong Kong, Xinjiang, and Tibet; Military; Security; and Technology.*** The homepage analyzes the top leadership of the Chinese Communist Party, focusing on the 25-member Politburo and its 7-member Politburo Standing Committee.