NATO COMMITTEE BRIEFING

NATO Resilience Committee

Information Communications Technologies (ICT) Supply Chain Strategy

RADM (RET.) MARK MONTGOMERY

Executive Director
CSC 2.0

Senior Director
FDD's Center on Cyber and Technology Innovation

Brussels, Belgium
March 31, 2023

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

In its March 2020 report, the U.S. Cyberspace Solarium Commission called on the U.S. government to take steps to reduce critical dependencies on untrusted information and communications technologies (ICTs). In addition to recommendations to improve intelligence and information sharing around supply chain risks, core to the Commission's recommended approach was the creation of an ICT industrial base strategy "to ensure more trusted supply chains and the availability of critical information and communications technologies. The white paper produced by the Commission was its effort to further this recommendation and lay out a strategy and recommendations for implementation.

The Challenge

Put bluntly, in the context of supply chains for ICT, the United States has a China problem.

Over the past two decades, China has mobilized state-owned and state-influenced companies to grab a dominant position in markets for several emerging technologies, including the market for telecommunications equipment.

This is no accident but rather the result of a concerted, strategic effort by the Chinese government to capture these markets through a mix of government-led industrial policy; unfair and deceptive trade practices, including state-led intellectual property theft; the manipulation of international standards and trade bodies; a growing network of influence built on the back of diplomatic and trade negotiations; and significant investments in research and development in ICT.

As a result, the critical strategic competition between China and the United States and its friends and partners is taking place in an international system of commerce that—due to Chinese state intervention—is neither free nor fair, hampering the ability of American and partner companies to compete for global market share.

While our primary competitor in this space, China, has a comprehensive strategy—demonstrated by "Made in China 2025, the Civil-Military Fusion, and China Standards 2035—the United States lacks an overarching vision for how to compete with China on this front.

A myriad of activities, from Congressional action like the CHIPS and Science Act, and the US Telcom Act, to executive branch initiatives run out of the Departments of Homeland Security, State, Defense, Commerce, and elsewhere exist, the U.S. lacks a coherent and comprehensive national strategy to align these efforts in partnership with key allies and partners in the private sector.

In short, in our eagerness to do something about a very apparent challenge, the United States has leapt to action without a plan.

U.S. Critical Dependencies and Industrial Capacity

Despite a high demand for critical technologies such as telecommunications equipment and semiconductors, the United States lacks the key industrial capacities crucial to ensure the

reliability of its critical technology supply chain. Other countries, particularly China, have been willing to subsidize and support their domestic industries All of this has forced critical dependencies of the United States on other countries like China, Taiwan, and Japan.

The Materials that most concern us are on both the raw and processed areas.

The Raw Materials include:

Silicon: While an extremely abundant natural resource and with a U.S. supply almost meeting its total demand, refinement and processing required for use is still largely dominated by East Asian countries like China. In 2018, China produced 4.8 million metric tons of silicon, far out-pacing the next few competitors combined. Also, in 2018, the U.S. produced 430 thousand metric tons of silicon, which came close to meeting the U.S.'s total demand for silicon of 600 thousand metric tons.

Germanium: U.S. does not have the capacity to produce germanium and retains limited capacity to refine it for use in electronics systems, leaving the country with a critical dependency on foreign imports, in particular from China.

Rare Earth Elements (REE): As REE are rare to nonexistent within the United States and the U.S. possesses neither the ability to mine nor the ability to process REEs at scale, the U.S. has a critical dependency on other nations. China is the leading REE supplier by a wide margin, followed by Estonia, South Korea, Malaysia, and Japan. China has geographic and economic advantages in producing REEs and will likely not be overtaken by other nations for some time to come.

The Intermediate Goods include:

Semiconductors: In recent years, the U.S. has become increasingly reliant on foreign firms for the manufacturing and the testing, assembly, and packaging area of production for semiconductors. Production process includes: design, production and testing, and assembly and production Reliance on foreign firms has come about in part as a result of companies going "fabless" to focus their businesses on specific parts of the production process due to increasing research and development costs.[1] In 2016, about 87% of the worldwide fabrication capacity was located internationally—with the majority in Asia—and this number is expected to rise.

Telecommunications Equipment (Radio Access Network equipment and/or Local Area Network equipment): U.S. is highly reliant on the services and products of international suppliers for its networking equipment. The Main players are Nokia, Ericsson, China's Huawei and ZTE, and South Korea's Samsung. Cisco is the only remaining major telecommunications equipment manufacturer in the U.S. but does not provide all the equipment necessary to build a

[1] (CRS Report, 2016, pg 11); SIA discussion 7/24/2020

telecommunications network. Most U.S. internet service providers rely on Nokia and Ericsson as their primary equipment suppliers.

American High-Tech Manufacturing

As recently as 2000, the United States was home to the world's largest supplier of telecommunications equipment: Lucent Technologies. Throughout the 1990s and early 2000s, Lucent was a powerful integrator, producing everything from semiconductors and other components to finished network technologies.

In 2000, Lucent's revenues surpassed $40 billion, eclipsing its nearest competitors by nearly $10 billion. Built on the back of the storied Bell Laboratories, Lucent Technologies was the global leader in network technologies. However, from 2000 to 2006, poor management and steadily declining revenue ultimately resulted in a merger with the French telecommunications equipment provider Alcatel. A series of questionable business decisions led Alcatel-Lucent to gradually cede its incumbent advantage as a network technology provider, as it failed to keep pace with Nordic and Chinese competitors that were able to innovate faster and bring cheaper and more advanced technology to market sooner.

At its height, Lucent's robust manufacturing capability supplied more than just finished network equipment: it provided the component parts for a myriad of electronics, including semiconductors. With the demise of Lucent Technologies, the United States lost more than just a telecommunications equipment provider—it lost its only true integrator. Today, while U.S. corporations such as Intel, Micron, Texas Instruments, and Global Foundries retain some semiconductor fabrication capability in the United States, all of these companies also manufacture overseas, and "most new semiconductor manufacturing capability is located outside of the United States."

As for why this capability has atrophied, three main challenges confront attempts to rebuild U.S. high-tech manufacturing capacity: a lack of patient funding capital; high investment barriers to entry; and standards and intellectual property barriers to entry.

These challenges arise from the simple fact that the economics of the hardware industry are not as attractive as those of many other technology sectors. While private capital is flowing into some kinds of technology, firms on the cutting edge of hardware development and manufacture in the United States face a competitive market for financial capital.

In 2019, for the second straight year, the venture capital ecosystem invested over $136 billion in U.S. companies. However, a meager 2.8 percent, or $3.8 billion, was invested in hardware, a symptom of a growing long-term trend. Whereas hardware investment has faltered, software and biotech have seen steady increases year over year. When other viable options for short-term profitability, higher profit margins, and overall greater return on investment exist, patient capital from private funders dries up for hardware. Today, the financial capital market for high-tech investment in the United States reflects these conditions.

In short, challenge number one for policymakers is to assist in facilitating a market for patient capital directed to long-term investments in hardware and other critical technologies.

Strategy

Any strategy to secure America's high-tech supply chains must be built on a foundation of partnership. The U.S. government must **identify key partners** and the assets they bring to the equation and work to ensure that they are insulated from malign influence.

To identify key partners, the United States needs to take into account a few key considerations that will lead to natural partnerships: (1) Trustworthiness, (2) Influence of China, (3) Geography, and (4) Stability. The advent of 5G mobile networking technology has shown us that trustworthiness not only of underlying technologies but also the nation states that produce them is critical for ensuring U.S. cybersecurity. International agreements, incentives, partnerships, and more will be critical for strengthening U.S. relationships with allies and partners to build a more trustworthy and resilient supply chain. Examples include ASML and the Netherlands; and TSMC and Taiwan.

Together with partners, the U.S. government must:

- I**dentify critical materials and equipment** to conclude those technologies and materials crucial to ensuring the reliability of its critical technology supply chain.
  - Equipment is likely to include weapons systems and telecommunications equipment, but also general purpose computing equipment.
  - Semiconductors and chips are more complicated to produce and require more technical manufacturing capability
    - These components might require more technical manufacturing capability because repurposing existing manufacturing might not be feasible
    - Other components, like packaging, wires, and other conductors, are simpler to produce and existing manufacturing can likely be repurposed in a time of crisis to meet needs.
- Work to **ensure a minimum viable capacity** to produce these goods should global supply chains be disrupted.
  - This is a particularly important strategic goal that will ensure resilience of U.S.-reliant high-tech equipment in times of crisis
  - For some key materials and equipment, the U.S. does not have the ability to produce, leaving us vulnerable in times of crisis and reliant upon non-U.S. and sometimes untrusted partners to deliver (raw materials, some semiconductors, some cases of 5G networking equipment)
  - Make a decision on strategic reserves
- **Protect America and American firms from potentially compromised equipment**.
  - Each stage of the production process allows space for the introduction of vulnerabilities into parts of the high-tech supply chain
  - We must improve the ability for the United States to collect intelligence on supply chain risks and disseminate that information to government and private sector stakeholders, creating Critical Technology Security Centers to test the security of devices and

technologies, employing policy tools to retain our economic advantage, and financial assistance to facilitate the movement of ICT manufacturing
    - Domestic efforts are underway
        - Example: CISA leads and ICT supply chain risk management task force which is a public-private sector partnership to identify and develop risk
        - Example: The President's NSTAC Advisory Committee is similarly a collaboration between the govt and private sector to provide advices on supply chain risk management and cybersecurity
    - There needs to be more robust device and technology security testing to determine the vulnerabilities of products and mitigation strategies
        - In the short run—we may need to source equipment from manufacturers or locations that we aren't fully comfortable with. In those cases, we need to ensure that the equipment is tested so we at least know what we're working with and can compensate (or help companies who are leveraging said equipment compromise) for any insecurities accordingly.
        - The CSC separately recommended that the Congress fund three Critical technology Security Centers, selected and designated by DHS in collaboration with the Department of Commerce, Department of Energy, ODNI, and DOD to test the security of hardware, software, and that of industrial control systems in U.S. critical infrastructure
        - Bans and Tariffs on Critical or Pervasive Technology have yielded mixed results and need to be used in tandem with incentives and working with allies and partners to ensure trustworthiness
        - Financial assistance to move manufacturing outside of China. Firms have indicated that they're moving out of China regardless due to higher costs than other nations, and financial assistance like that used by Japan might help speed up the process.
- **Facilitate a domestic market for finished technologies**.
    - Domestic infrastructure investment tied to open standards.
    - Release of more mid-band spectrum
        - The rest of the world has decided on mid-band spectrum as the primary spectrum for 5G. The U.S. has not released enough spectrum to meet commercial 5G needs.
        - Equipment manufacturers (Nokia, Ericsson, Samsung) have been forced to build two versions of their equipment: one for the non-mid-band U.S. and one mid-band version for everyone else.
- Work with partners in the private sector and around the world to **ensure global competitiveness** of trusted firms in the face of Chinese state-backed competition.
    - First, policymakers must ensure that domestic or trusted components suppliers are price competitive against Chinese manufactured alternatives, otherwise U.S.-based final product assemblers and manufacturers will continue to rely on foreign sources.
    - Second, policymakers must ensure that final product assemblers and manufacturers for goods as disparate as smartphones and laptops to routers and radio equipment, are price competitive versus alternatives both at home and abroad, lest companies and individuals who deploy such equipment continue to opt for cheaper, Chinese alternatives, as they have in the past.
    - Third, the U.S. government should use trade agreements to help build domestic industry. International trade in goods and services has become a far more important and crucial

part of today's economic activity. Trade agreements help lay out the established practices for U.S. companies looking to conduct business in global markets by reducing barriers to U.S. exports and protecting U.S. interests abroad.

Summary

To address all of these risks and challenges identified in the ICT supply chain, the United States needs to create a high-tech industrial base strategy. The U.S. government should strive to facilitate the continued viability of high-tech manufacturing through light touch interventions that set the conditions in which innovation and industry thrive. The strategy laid out above is a good road map for the government to follow.