SHIELD
by SOURCEREE

What's Inside

CFIUS Newsletter

October 2020

National Security Strategy for Critical & Emerging Technologies (CET)

The Feasibility of Game Theory Approaches: An Investigative Study of Threats to U.S. National Security from Foreign Investment

SOURCEREE

Authors: Adam Murphy & John Lash

National Security Strategy for Critical & Emerging Technologies (CET)

In October 2020, the White House released the National Security Strategy for CET. *"The National Security Strategy (NSS) lays out a vision for promoting American prosperity; protecting the American people, the homeland, and the American way of life; preserving peace through strength; and advancing American influence in an era of great power competition. It calls for the United States to lead in research, technology, invention, and innovation, referred to generally as science and technology (S&T), by prioritizing emerging technologies critical to economic growth and security."*

The National Strategy for Critical and Emerging Technologies outlines the steps the United States will take to preserve its competitive edge under two 'Pillars': Pillar I - Promote the National Security Innovation Base (NSIB), and Pillar II - Protect Technology Advantage. Within Pillar II, the strategy identifies the CFIUS process specifically, and allies' processes which are similar to those executed by CFIUS. Areas of interest regarding the strategy are highlighted below.

United States, China, Russia: New U.S. strategy for critical, emerging technologies signals increased political risks for companies.

U.S. President Donald Trump on 15 October 2020 signed the National Strategy for Critical and Emerging Technologies, which lays out U.S. goals for promoting and protecting U.S. technological capabilities.

- The National Strategy sets the goal of U.S. leadership in CETs in the context of competition with China and Russia.
- It indicates elevated political and regulatory risks for technology companies, referencing export controls (current U.S. export control reforms underscore a hard line towards China) and "secure" supply chain measures that will hinder cross-border technology trade
    - **Analysis**: Calls to diversify China supply chains reflect rising political risks, major reshoring is unrealistic
- The strategy could also require U.S.-based technology companies to consider U.S. national security interests in their technology development and in cooperation with foreign partners in countries like China.
- Even with a prospective change in administration, the strategy reflects the trajectory of elevated political and regulatory risks for technology companies.

Competition for Technological Leadership

Consistent with prior U.S. government policy documents, the CET strategy identifies China and Russia as technological competitors and frames the competition as one in which the U.S. and its allies use technologies and technology governance to "promote democratic values". European Union leaders have used similar terminology around technology policies, suggesting a basis for closer US-EU technology cooperation in the coming years.

The document stresses that the U.S. seeks to be the world leader in the highest-priority critical and emerging technologies, and that either the U.S. or its close allies should lead in high-priority CETs. However, the document does not prioritize specific technologies, suggesting this may change over time.

Evaluation 1: The U.S. points towards growing the workforce and attracting foreign talent. However, it does not address the issues with Chinese researchers at leading universities or the development of a more cooperative, coordinated, and unified approach at an institutional level.

Evaluation 2: There is a lack of specific financial targets and/or details of tactical implementation. Lack of specificity on subsidies or U.S. government financial support to specific industries.

Raising the Bar for Political Risk

For companies, particularly those with business interests in both the U.S. and China, the strategy signals further political risk to their operations. The strategy mentions export controls, which suggests further regulations restricting exports of CETs are likely beyond the narrow restrictions (e.g. bilateral technology trade likely to face further restrictions despite narrow focus of latest rules) in this area imposed to date. Similarly, calls to secure supply chains are likely to lead to further requirements on technology companies operating in the U.S. to limit manufacturing and sourcing in countries like China, including restrictions like those outlined in the so-called "Clean Network" framework in mid-2020 (Executive Orders targeting Chinese applications heighten uncertainty, but functional impact remains unclear).

Given the prominence assigned to protecting U.S. intellectual property, research, and development (R&D) activities by U.S. organizations in China are also likely to come under closer scrutiny. The strategy reaffirms U.S. concerns about China's military-civilian fusion, signalling closer audits of military end use/user restrictions already signalled in other U.S. policies. Finally, U.S.-based technology companies will face requirements to incorporate security design into their technologies.

Bipartisan Pressure

A prospective change in U.S. administration in 2021 is unlikely to significantly alter the trajectory towards tighter regulation of advanced technologies. Like the administration, opposition Democrats support export controls for sensitive technologies as well as initiatives to re-shore supply chains. Both parties are particularly sensitive to control and exploitation of personal data of U.S. citizens. Democratic presidential candidate former vice president Joe Biden (2009-17) also generally supports leveraging multilateral initiatives with like-minded allies and partners in Europe and Asia.

That said, a Democratic administration would likely be different in three key areas:

First, it would be more welcoming of high-skilled immigration as a way of meeting innovation and workforce objectives – a key demand of the tech sector. The administration in June suspended issuance of high-skilled work visas in response to COVID-19 and on 6 October 2020 released tighter rules intended to limit high-skilled migration – which were promptly challenged in court by a consortium of tech companies.

Second, Biden's economic recovery plan envisions major investments in domestic R&D, focusing on "green" technologies, and emphasises incentives over mandates in bringing supply chains back to the U.S. As a result, a Biden administration may be more receptive to input from the technology industry when designing export controls and other regulations.

Third, Biden views the relationship with China as one of competition – not conflict.

- Economic security as national security.
- To win the competition for the future against China or anyone else, the United States must sharpen its innovative edge and unite the economic might of democracies around the world to counter abusive economic practices.
- Biden administration is expected to continue to scrutinize Chinese inward investment flows to the U.S., particularly in high-tech sectors and make it harder for U.S. firms to export sensitive technology.

Critical and Emerging Technologies List

The Critical and Emerging Technologies list reflects the 20 technology areas that United States Government Departments and Agencies identified to the National Security Council staff as priorities for their missions. The list will be reviewed and updated annually via the interagency process coordinated by the National Security Council staff. The technology areas are arranged alphabetically.

1. Advanced Computing
2. Advanced Conventional Weapons Technologies
3. Advanced Engineering Materials
4. Advanced Manufacturing
5. Advanced Sensing
6. Aero-Engine Technologies
7. Agricultural Technologies
8. Artificial Intelligence
9. Autonomous Systems
10. Biotechnologies
11. Chemical, Biological, Radiological and Nuclear (CBRN) Mitigation Technologies
12. Communications and Networking Technologies
13. Data Science and Storage
14. Distributed Ledger Technologies
15. Energy Technologies
16. Human-Machine Interfaces
17. Medical and Public Health Technologies
18. Quantum Information Science
19. Semiconductor and Microelectronics
20. Space Technologies

The Feasibility of Game Theory Approaches: An Investigative Study of Threats to U.S. National Security from Foreign Investment

In October 2020, John Lash successfully defended his PhD thesis focused on the convergence of trade policy, economic espionage, and national security.

Key details from the research are summarized below; we would welcome the opportunity to provide a full debrief to any interested agency. A whitepaper summarizing the recommendations of the study is forthcoming, and the full dissertation will be available for review upon copyright and publication in November 2020.

Research Significance:

- This research, which included insights from leaders in government, the private sector, and academia, identifies and outlines critical observations and implications for policymakers to establish stable national security and growth oriented economic policies.
- All governments must consider their nations place in progressing towards the next industrial revolution. This advancement includes evaluating how global competition creates technological and economic resilience, security, and innovation.

Key reflection points include:

- How to create consistent and transparent standards
- Evaluating to what extent governments participate in the capital markets
- How and where capital and resources are allocated
- By what measure are the consequences of action (or inaction) judged over time

Summary:

- The age of intelligent warfare has created a fully integrated cyber, economic, and information state of adversarial capabilities within an emergent threat landscape.
- The landscape is shaped by multidimensional strategic interactions of globalization, vis-à-vis foreign direct investment (FDI), that are framed by the traditional guidelines of collaborative game theory.
- However, a modernized pure-conflict game theory model may be necessary to secure the interests of the United States.
- The complex concept of power within the broad scope of globalization and national security requires an evaluation which adequately addresses the threat environment in the 21st century – a modernized pure-conflict game theory model where investments, which create direct and indirect power over other nations, are weaponized.

Research Participants:

- The participants have collective involvement in more than 1,000 transactions under CFIUS jurisdiction with cumulative transaction value in excess of 500 billion dollars.

Participant Profiles:

- **USG:** The government officials are distinguished by more than 200 years of aggregate military, government, and intelligence community service, including having held senior leadership positions at the National Security Council (NSC), the Joint Chiefs of Staff (JCS), the National Security Division (NSD) at the U.S. Department of Justice (DOJ), the Foreign Investment Risk Management division at the U.S. Department of Homeland Security (DHS), the U.S. Department of Commerce, the National Security Agency (NSA), the Central Intelligence Agency (CIA), as well as other defense and security agencies.
- **Private Sector:** The private sector participants in this research included U.S. entrepreneurs and company founders who have received foreign direct investment which resulted in a national security investment review. The sample also included investors, consultants, academics, and legal advisors based in the U.S., China, and the broader Asia-Pacific region to provide broad perspective on the issues addressed by this research.

Primary Themes:

- **Preference** for a global collaborative effort for the design, development, and enforcement of standards for interactions between nations as it relates to the convergence of national security and trade policy.
- **Desire** to preserve and expand the U.S. domestic ecosystem which encourages, facilitates, and incentivizes innovation in key national security industries.
- **Concern** for the lack of a defined U.S. industrial policy, technology policy, and funding for essential research and development.
- **Acknowledgement** that the domain of national security includes both economic security and technology policy.

Application for Policymakers:

- The domain of national security includes both economic security and technology policy.
- A global collaborative effort, in the form of collective pressure, is necessary for the design, development, and enforcement of standards for interactions between the United States and China as it relates to the convergence of national security and trade policy.
- The United States must preserve and expand incentives for a robust domestic ecosystem which encourages, facilitates, and promotes innovation in key national security industries, including the expansion of public private partnerships.
- The United States would benefit from the establishment of an effective industrial policy and technology policy. These policies would define parameters for the funding of essential research and development, as well as encouraging meaningful updates to factors impacting U.S. global competitiveness such as education and immigration.

Outcome:

The U.S. must address these wicked problems through the development of holistic solutions that balance the economic realities of the capital markets and the fundamental national security concerns. This research suggests that the development of a modern game theory investment security model be utilized to address the complex convergence of economic modernization and the national security impact of foreign direct investment.

Protected by

SHIELD
by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

SHIELD VISION

Software platform for on-demand supply chain risk assessments and financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business intelligence reports on critical suppliers