CONVERGENCE

A Collective Defense Against Adversarial Capital
Standards and Policy Recommendations for FOCI Screening

Edited by Quantifind and the Convergence Working Group
QUANTIFIND
March 2024

Table of Contents

Summary

On March 6, 2024, Quantifind and Deloitte hosted a Convergence event on Adversarial Capital in Arlington, Virginia. The event convened leaders from multiple sectors including banks, investors, government, think tanks, nonprofits, and technology providers.* **The discussion centered around the challenges of the US Defense Industrial Base (DIB) in screening investments and partners for signs of adversarial capital, i.e., Foreign Ownership, Control, or Influence (FOCI) via Great Power Competitors.**

All of these sectors brought unique differentiating perspectives to the table, yet most agreed on three fundamental requirements for an adequate defense against the FOCI threats to the US Defense Industrial Base (DIB):

- **Clear FOCI definitions are needed** to support objective screening and defensible workflows. Definitions should be reinforced with clear historical examples of FOCI-related risks.
- **Automation of FOCI detection workflows is necessary** to keep up with the threat. Traditional tools and manual processes cannot address the scale and complexity of the problem. Analysts must be enabled with the latest technology to effectively reduce the burden of mundane tasks and prioritize limited bandwidth.
- **Incentives, policies, and regulations are required** for certain parties to act. Without regulation, some industries will continue to be driven by pure market incentives and not look to actively support national security initiatives.

The goal of this document is to provide specific and actionable recommendations for each of these requirements. This guidance may be considered in the near term by those already screening for FOCI risks today, including front-line analysts and the developers of the AI screening tools that those analysts use. The guidance can also be considered in the longer term by policy and lawmakers who, with proper consideration, can implement regulations that provide pragmatic clarity, motivation, and force.

*Disclaimer: This document does not represent the formal opinions of any attending organization.

Tags: Adversarial Capital, Industrial Base Resilience, Economic Security, Insider Threats, Foreign Malign Influence

Background

The Threats

- **Loss of Intelligence (Espionage):** Certain FOCI activities aim to support corporate and state-based espionage, insider threats, unintended or illegal tech transfer of critical technologies (IP, trade secrets, state secrets), and cyber exploits or intrusions into critical infrastructure.
- **Loss of Control (Supply Chain):** FOCI risks include those of sole-source dependence on adversary-controlled suppliers (where supply could be shut off or defects introduced during a conflict), as well as the establishment of infiltration points where systems could be hijacked or shut down directly.
- **Loss of Economic Assets:** An inadequate response to FOCI will result in the continued loss of jobs (over-dependence on offshoring), loss of investment money and time partnering with compromised partners, and loss of engagement from critical technology partners.

Sectors and Responsibilities

There are many stakeholders responsible for oversight and screening that can impact the Defense Industrial Base. Each of these groups has a different set of responsibilities and perspectives:

- **Investors:** Private and public investors, including venture capitalists (VC) and innovation agencies like AFWERX, Army Futures Command, and the Defense Innovation Unit (DIU).
- **Supply Chain Managers:** Those responsible for weapons systems and other critical supply chains, including Program Executive Officers (PEO), system integrators (SI), and government-industry partnerships.
- **Industry:** Tech Companies (hardware and software), contractors, original equipment manufacturers (OEM), and cleared groups with Insider Threat Programs.
- **Financial Service Providers:** International Banks under Know Your Customer / Anti-Money Laundering (KYC/AML) regulations (BSA, UK Bribery Act, Foreign Corrupt Practices Act) and broader operational risk constraints.
- **Overseers and Regulators:** Congressional Committees (e.g. China Committee, Financial Services), Financial Regulators (OCC, FinCEN), Committee on Foreign Investment in the United States (CFIUS) groups across government, Office of Secretary of Defense: Assistant Secretary of Defense for Industrial Base Policy (IBP), Service-specific offices (e.g. Army AT&L, SAF CDM/OCEA),

For consistency and effectiveness, cross-cutting policy should align the mission and standards among these stakeholders.

Recommendations

Standardized FOCI Definition

To enable effective screening, any program must be aligned with clear, operational, computable definitions of the risk at hand. To achieve these aims, we recommend a definitional framework that is based on the principles listed below. This guidance does not include a specific set of rules or an algorithm, but any automated system should take these factors into account.

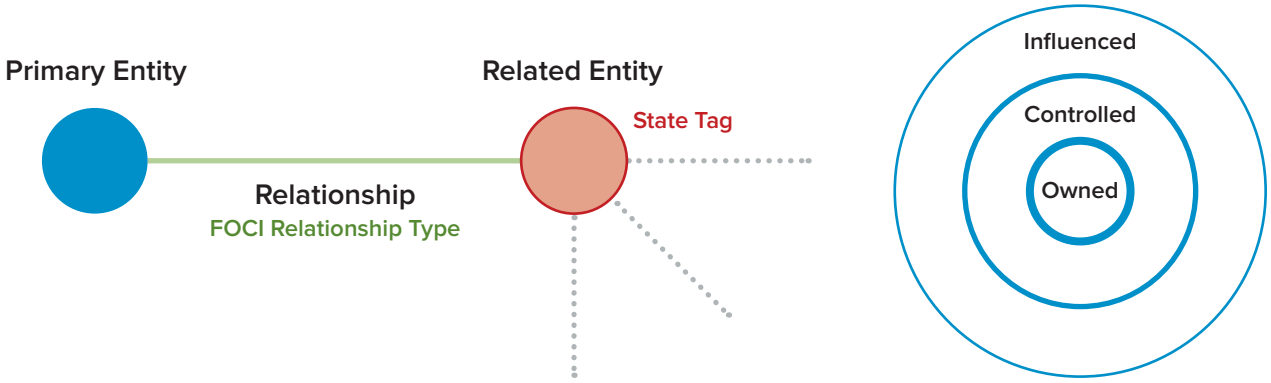

Figure 1: Relationship-Based Risk Framework and Tiered Approach for FOCI

Recommendations

Establish a Relationship-Based Risk Framework. All influence comes from relationships between entities. For every entity in question, an automated screening system should be able to identify relationships to other entities (from a wide variety of sources) and the direct risks of those entities (state or criminal associations), then combine these into a single risk-assessment framework. This procedure may need to be iterated to associate a primary entity with risk that resides multiple degrees out in its influence network.

Consider Certain Definition Components. Several features should be considered on top of any given relationship. These contextual factors may come from different sources. The following feature classes are described in more detail in the Appendix.

- **Relationship Types:** Many relationship types need to be considered across the FOCI spectrum, from hard ownership to soft influence (See Figure 1). These stretch beyond simple ownership structures (where clear thresholds should be set) and into partnerships and associations of various kinds.
- **State Associations:** First, the countries of particular interest for FOCI need to be identified by the government explicitly. These are likely to include China, Russia, North Korea, and Iran, but should be made explicit and consistent with existing international sanctions policy. The end node in a discovered relationship risk may be either state-controlled or compellable by the state. These state affiliations could include state-owned enterprises (SOE), sovereign wealth funds, and military organizations. Countries vary widely and country-specific guidance should be given for each country, including entity names and country-specific entity categories (e.g. the PLA in China or private military companies in Russia).
- **Behaviors and Correlated Risks:** Beyond state control, certain other risk patterns should be considered as further context. These include previous associations with criminal typologies (e.g. corruption, espionage) or complex ownership structures meant to obfuscate influence. These also include known precursor signals to accepting adversarial capital, such as signs of poor financial health. The identification of these risks on top of state control may provide the necessary color or motivation to analyze a case more deeply or take further action.

- **Industry Types:** Certain industries (commodities, textiles, etc.) can be made exempt from scrutiny, given the fact that the global economy depends upon them and they may hold no strategic relevance. However, certain other industries (critical and emerging technologies, scarce resources, weapons systems) should be identified, leading to increased scrutiny.

Document and Deploy Test Cases. A database of real-world examples should be created to help train and test both automated systems and human investigators. This reference database should include cases that do and do not count as legitimate historical examples of adversarial capital. Any risk definition system should be measurable and consistent with this reference data set and documented in "Risk Cards" that explicitly lay out rules for inclusions, exclusions, and edge cases. The resulting definition should be validated by users in multiple sectors to foster alignment and collaboration between, for example, government agencies and financial institutions.

Produce a Tiered Approach. Ultimately the system should provide suggestions to an analyst who is responsible for making a FOCI-based risk assessment. A tiered output system is recommended for the sake of clarity, categorical simplicity, and ease of integration into existing screening methodology. The level of intervention or avoidance may correspond to these tiers. For example, Tier 1 could indicate that an entity is a direct threat, such as a sanctioned entity from an adversarial nation. Tier 2 might indicate that an entity is compromised through a relationship, e.g. an SOE or an entity under the direct control of a sanctioned Russian organization, mandating an unambiguous intervention. Tier 3 could indicate significant relationships to entities of concern (e.g. an investor or board member with domicile within the FOCI nation of interest). Finally, Tier 4 would not signal FOCI risk, but information that should be considered by an analyst (e.g. vulnerabilities due to financial health or a targeted industry). This tiered approach would help institutions take a variable but objectively laddered approach to resourcing, decisioning, and communication with liaison groups (e.g. banks passing assessments to regulators or law enforcement).

Automated Workflows

In principle, a definition based on the above principles could be used to screen entities for FOCI risk manually. In practice, of course, the scale and complexity of typical screening workflows necessitate automation. There are too many entities and data sets to screen, and too few resources to maintain existing practices. In other words, the objective definition is necessary, but more is needed for an effective screening program. Any automated system that assists a human in making decisions on FOCI should have the following characteristics.

Recommendations

Default to Continuous Monitoring: Automation is needed for one-time screening (onboarding) of entities before any investments or coupling into supply chains are made. However, once is not enough. Given the dynamic nature of business partnerships and status, companies with government contracts must be continuously monitored to identify unexpected infusions of adversarial capital and control. The screening defense must occur both before investment or purchase, but continuously afterward because a given company or component may start clean and become compromised at unknown points in the future.

Use Trained and Validated Models (Machine Learning): To effectively pull signals from vast amounts of complex unstructured data, trained algorithms are necessary. These models must perform low-level tasks (natural language processing, name science, entity resolution, risk labeling, relationship extraction, knowledge graph production) to produce features that roll into high-level, defensible assessments of FOCI consistent with the established definitions. All algorithms should be tested and monitored for continued quality using best practices in MLOps (machine learning operations).

Use Open Source First

- While classified or sensitive information has value, open-source information should form the first line of defense against adversarial capital. Systems should focus on publicly available information (PAI) and commercially available information (CAI), as a first resort both because it contains the necessary coverage and because it is sharable.

- There is no one data set to cover everything, so any adequate system should pull from many databases including Structured+Unstructured Data and PAI+CAI, with the prioritization of certain "table stakes" data sets such as sanctions, corporate registrations, and prominent news sources.

Establish a Data Sharing Mechanism

- The use of open source is necessary to enable shareability, but not enough to make it happen. There needs to be a means of sharing FOCI discoveries across government agencies and possibly beyond. This would support a collective defense to adversarial capital and reduce redundant workflows.
- The sharing mechanism could start in small communities of interest. For example, government-based innovation funding organizations (e.g. DIU, AFWERX, AAL) could establish a central means to share information regarding the results of their company vetting processes. This could then expand, when successful, to more generalized sharing mechanisms.

Design for Trust and Tradecraft Compliance

- **Human-Centered:** While AI is important, there must always be a human-in-the-loop who is responsible for validating results and making the final determination of a risk assessment. The best algorithms can be compromised with poorly designed interfaces that fail to establish trust with an analyst and stay consistent with existing compliance and tradecraft rules.
- **Provenance:** All data provided to investigators should come with provenance and access to root information to allow them to determine accuracy for themselves. Additionally, the system could rate each source by trustworthiness based on objective metrics.
- **Explanatory AI:** Any model result should explain its reasoning and the system should allow the analyst to, again, override the automated determination.

Incentives and Policies

The government should not play the only role in defending against adversarial capital and other threats to economic security. However, certain agencies can help by providing clear policies and regulations that support larger strategies to align the efforts and incentives of multiple sectors against the threat.

Recommendations

Continue to Provide Alternatives for Resilience and Remediation

- **Provide Alternatives for Components:** Strategies that support on-shoring and friend-shoring of critical components should be augmented with services that help manufacturers find alternatives for certain critical system components and resources.
- **Provide Alternatives for Capital:** Similarly, the government should help provide alternatives to adversarial investors by promoting trusted capital resources (e.g. U.S. Government-friendly, mission-oriented investors).

Establish Sensible Regulations for Each Sector

- **Definitional:** As detailed above, the federal government needs to define, through executive order or law, what comprises adversarial capital and FOCI so that both the public and private sectors can address it appropriately and align with national security objectives and expectations. Both the definition and process should be broadly consistent with the principles laid out above.
- **Private Investors:** VCs are not compelled to disclose their partners. The government should educate and require private investors to disclose limited and general partners in a secure way that respects their need for privacy.

- **Banks:** Without regulation, banks are not incentivized to divest certain FOCI relationships, the same way that they are not incentivized to divest all money launderers prior to regulation. Further, most financial institutions will not be willing or able to distinguish FOCI-related screening from currently mandated sanctions screening. Addressing FOCI risks through the rulemaking process could be seen as duplicative with existing legislation and regulations, such as the Corporate Transparency Act's reporting of ultimate beneficial ownership (UBO). To avoid the overhead of implementing an entirely new regulatory system, FOCI risks should be addressed within the existing BSA regulations for KYC/AML and aimed at the largest, most sophisticated financial institutions. (The tiered definition below supports this notion, starting from sanctioned entities and extending to relationships with sanctioned entities or foreign states under sanctions.) Some banks may even be incentivized to provide FOCI-related screening as a service to their clients as a competitive advantage or revenue stream.
- **Industry:** The government should require self-audits by industry (e.g. manufacturers, suppliers) to access or continue receiving funding through certain programs. Similar to banks, the government needs to provide incentives for their partners, who often have more information access and technical capability, to screen their own providers. For example, access to participation in certain government-funded programs could be restricted to those who participate in self-screening processes.

Copy Analogous Models for Self-screening

- **Distributed Effort:** It is unrealistic to assume any central agency will be responsible for broadly screening for signs of FOCI risk across all sectors. Even within government, there will likely continue to be many parties responsible for screening for multiple reasons, e.g. all CFIUS elements for the applicable agencies, or the different islands of innovation investment. For more intricate supply chain systems, the government will need more bandwidth and the required data access to effectively perform a deep screening at multiple levels.
- **Self Audits:** Therefore, for practical reasons, it is likely that certain groups (e.g. banks, manufacturers) will have to self-screen for signs of risk. Certain government agencies will play the role of "credible threat" to keep those agencies honest via spot checks over open source information.
- **Analogous Models:** This trust-but-verify approach has proven to be pragmatic and successful in other realms. For example, for software vulnerability testing some standardized systems and products allow software companies and their internal compliance teams to screen their codebase against databases containing known vulnerabilities and exploits. The company takes on the work of screening while their partners, government or otherwise, recognize the standard that they are using to screen, and can dig deeper only when necessary. Although it necessitates operating at a higher level of business relationships, as opposed to code, there is no reason why a similar approach cannot work for FOCI self-audits in the investment and supply chain worlds.
- **Incentivize Self-Screening:** The government should focus more on carrot than stick for compliance with FOCI rules. Certain, otherwise non-motivated partners should be incentivized to self-screen, knowing that the government can help with remediation of the risks, as opposed to unhelpful punishment and associated delays. While regulations are never fully welcome, partners can recognize their inevitability and be incentivized to "get ahead of them" to help make progress on indisputable threats.

Potential Failure Modes

The effective implementation of automation-assisted screening for FOCI risks will take careful attention to detail. The challenge is not just about identifying and remediating the threat but also about avoiding several potential pitfalls that could make the situation worse. Here we attempt to lay out several failure modes that could potentially violate law, ethics, and general practices of responsible AI.

A poorly implemented strategy runs the risk of:

- Stifling legitimate investments and business with entities in competitive nations.
- Stifling partnerships between government and private companies by creating paranoia and a fear of ineffective regulation.
- Biasing unfairly against individuals or organizations with legitimate associations with competitive countries. This may come from poor analysis of names or the use of illegitimate data.
- Giving an investigator a false sense of confidence with insufficient evidential provenance. Or giving too much confidence with misinterpreted system results. A system may also create the illusion of objectivity if it is used to support arbitrary and subjective judgments.
- Relying on non-computable concepts. For example, the intent of an investment is often impossible for a system judge and is dynamically shifting in any case. The system should properly hand off analytic assessment to a human to judge the intent and degree of a threat based on objective findings. (However, the system can train on historical examples and discover learned features that correlate with known intent after the fact to suggest potential red flags in present cases.)
- Flooding analysts with false positives or useless reports. Similar regulatory filing systems (e.g. suspicious activity reports) are plagued with this problem. To “play it safe” overly inclusive risk-averse rules are set that “pass along” useless alerts, hence overwhelming downstream assessments and taking bandwidth away from higher-priority cases.

Any given system and set of policies will not solve any of these issues perfectly but will need to recognize these issues and address them adequately. The ultimate implementation should make a calculated risk assessment that properly balances these concerns with the efficiency and effectiveness improvements gained from a technology-supported process.

Conclusion

Our nation-state competitors want leverage over the United States and our allies. They want leverage over both the military and our critical industries in the US Defense Industrial Base (DIB). They want to establish foreign ownership, control, or influence (FOCI) through technological and intelligence superiority, both through illicit means like espionage, and fully legal means that require the cooperation of our companies, intentional or not.

This threat should motivate all involved parties to cast sunlight on their activities through both better monitoring technology and better policy. This cannot wait until when we absolutely need it during times of conflict when it will likely be too late.

The collective solution to the adversarial capital problem will need to be sufficiently detailed to meet the complexity of the problem. Any FOCI definition (as further delineated in the Appendix below) can be subtle to interpret in real-world situations. There are many stakeholders spread across sectors, all with different core missions and motivations. Our adversaries are incentivized to keep making it more complex, shielding their influence through complicated networks of control.

While there will not be a perfect solution, there is now a window of opportunity to create realistic standards and policies that make us significantly safer and more robust as a nation. We hope that, through some of the pragmatic guidelines outlined in this whitepaper, we can collectively make progress in exposing and remediating critical risks in ways that are both responsible and effective. **If you would like to join the discussion or join Convergence for future events, please reach out to convergence@quantifind.com.**

Appendix: Definition Components

This appendix contains further detail on which factors should be considered in any operational definition of adversarial capital or FOCI. Again, we are not proposing any explicit algorithm or tiered risk approach as suggested above. However, these factors should be considered in the implementation of any such algorithmic definition. Without the due consideration of each of these components, any algorithm or process is likely to be less than effective to an investigator on the frontline of evaluating potential risks.

Country Associations

The first question that bridges between abstract FOCI and adversarial capital is: Which foreign countries count as adversaries?

One attitude to take is that the base definitions and algorithms should be independent of the country, allowing us to consider the FOCI definition for any country. In principle, we could even talk, symmetrically, about US FOCI in other countries, and how that impacts our strategy. This attitude should be taken (to a degree) to build a system with definitions that make sense and are not "overfit" to any one country. We could also, less provocatively but sensibly, call the adversaries "competitors" and open it up to more countries.

However, realistically, any FOCI analysis will pay particular attention to certain critical competitors, likely including China, Russia, North Korea, and Iran. Recognizing this, the US government could choose to specifically name certain countries (in a specific regulation or executive order), or do so indirectly through anchoring off pre-existing official sanctions lists (following OFAC) where the presence of these countries is obvious. Our allies, either Five Eyes or NATO, should not be targeted as FOCI, but not fully removed from any analysis because many adversaries work through these allies or the US itself.

The next question is which kinds of entities in these countries are we concerned about? Here's a sample list of example state affiliations that may cause concern:

State Owned Enterprises

Sovereign Wealth Funds

Military and Intelligence Entities

- Public (People's Liberation Army, PLA)
- Private (Private Military Companies, PMC/ChVK)

Influence Operations

- Talent Programs
- Disinformation Campaigns
- Belt and Road and other Economic Campaigns

This kind of list should be paired with a list of company types that are explicitly not of concern. And this general list should also have a version for each country of interest, because of the variability of organization types and specific concerns on a country-by-country basis.

Industry Types

Similarly, any complete analysis should consider the industry of the companies involved. Some industries are of more concern and others are of less concern, if not exempt. Here is an incomplete list in either category:

Include: Industries of More Concern

- Critical and Emerging Technologies (CET) as defined by the White House
  - "...a subset of advanced technologies that are potentially significant to U.S. national security."
  - E.g. AI, Robotics, Biotech, Directed Energy, Semiconductors, ...
- Other
  - Certain screening organizations may want to expand or filter the CET list and consider one of many possible perspectives given their authorities and mandate.
  - E.g. Defense and Cybersecurity, Mining and Resources, Healthcare and Pharmaceuticals, Critical Infrastructure

Exclude: Industries of Less Concern

- Commodities
- Textiles

Some companies conceal their true industry in various ways, an inconsistency that should also be investigated at the algorithmic or human level.

Relationship Types

Some relationship types are also of more interest than others in the FOCI spectrum. Hard ownership is on one side of the relationship type spectrum, while something like "attended the same conference" may be on the other, weaker influence side of the spectrum. Here is an incomplete listing of relationship types that should be considered in any classification system:

Ownership

- Direct and Indirect (e.g. through shell companies)

Financial

- Investment
  - Typical scenarios involve situations where foreign-controlled organizations invest in an entity of interest (e.g. a US technology vendor). However, other controlling relationships of concern may go the other way, including US entities that invest in foreign companies that may, intentionally or not, build up adversarial state capacity and indirectly support foreign SOEs by providing capital and legitimacy.
- Debt

Partnerships

- Joint Ventures
- Supplier
- Introducer (deal broker, matchmakers, lobbyists, those taking finder's fees)
- Co-authors, Research Partners, Collaborations

Customers

- Especially non-diversified, sole dependency
- Trade partners

Employment

- Consultants
- Formal and informal relationships

Personal

- Close familial or friend relationships

Historical

- Are former relationships also of interest? (likely depends on context and may be left to the investigator)

Correlated Risks and Behaviors

There are many risks associated with FOCI that need to be considered in any complete analysis. Some of these risks are the "true threats" that FOCI is meant as a potential proxy for (e.g. espionage), some are predictive of vulnerability to FOCI (e.g. financial health), and others indicate attempts to evade detection (e.g. shell company). The recognition of any of them will give needed context and cast a more complete light on an entity as compared to only the detection of foreign investment relationships.

National Security

- **E.g. Espionage:** One of the main threats of FOCI is access to and transfer of critical IP, trade secrets, or state secrets. If an entity is associated with espionage or corporate espionage, it will likely continue to be. And even if an entity is not directly tied to such activity, having close associates who have been should be considered a red flag.
- Also see: Weapons Trafficking, Dual Use Materials

Financial Health

- **E.g. Bankruptcy:** Companies do not always take foreign investment because they want to, they take it because they have no other choice. Recognizing when an organization is in turmoil, or near bankruptcy, can point to vulnerabilities that need to be known to any close partner.
- Also see Executive Exit, Layoffs, ...

Financial Crimes (and Other Criminal Behavior)

- **E.g. Corruption:** Previous instances of corruption, bribery, or other financial crimes are likely to be of concern when associated with FOCI signals.
- Also see Money Laundering, Fraud, Patent Infringement, Counterfeit.

Natural Security

- **E.g. Illegal Fishing:** Various environmental risks are often tied to FOCI behavior. For example, illegal fishing vessels operate through a complex web of intermediaries that conceals their state associations and effectively launders the goods into accepted marketplaces.

Suspicious Structures (and Anomalous Behavior)

- **E.g. Shell Company:** Any sign of obfuscation, including overly complex corporate structures and offshore locations in tax havens, is a red flag that should be added to any FOCI analysis.
- Analogously, for individual behaviors, one can look for suspicious anomalies such as those included by insider threat education programs, including sudden changes in wealth, travel patterns, or communication patterns.
- In general, any significant anomalous data signal should be called out, including mismatches between public representations (e.g. stated industry) and actual operations (e.g. activity via shipping logs).