

Protecting risk management strategies for foreign investment in the United States from a national security perspective

Robert Lizak

Polish Academy of Sciences, Institute of Law Studies, Warsaw, Poland, and

Sebastian Skuza

Faculty of Management, University of Warsaw, Warsaw, Poland

Abstract

Purpose – In the current trade war between the United States and China, CFIUS's analysis of the risks of foreign investments to US national security has increased. The purpose of the article is to verify that access to data for the purposes of this risk analysis is difficult or impossible, and therefore it is not possible to assess strategic risk management, which increases the national security of the United States.

Design/methodology/approach – Data were extracted from a review of US federal law, including hard law and soft law. In addition, data for the study were extracted from US government documents of strategic importance and official and scientific documents produced by or for US federal government officials.

Findings – In analyzing the risk of foreign investment, there is great difficulty, and in some circumstances even an inability, to see the classified data underpinning the decisions made by CFIUS or the President, which enhances the national security of the United States.

Originality/value – In the wake of the US launching a trade war with China, the risk of foreign investment to US security has increased dynamically, thus increasing the need for CFIUS to analyze risk. However, vis-à-vis this analysis, there are great difficulties and, in some circumstances, even impossibilities in knowing the classified data underpinning the decisions made by CFIUS or the President of the United States, how national and global security risks are identified and assessed, and the model or tool used to assess the balance maintained between economic openness and national security protection. Consequently, the highest value of a foreign investment risk management strategy for US national security is to protect the strategy by preventing it from being assessed in detail and holistically.

Keywords Risk management, Strategic management, Foreign investment, National security law, Trade war

Paper type Research paper

Introduction

A review of the national security risks to the United States arising from its external economic interactions shows that they have been present since the inception of the American state (Sosin, 1963). Consequently, the legislator has often responded appropriately to prevent such risks from recurring or – through proper management – to minimize them. The situation is similar in the case of foreign investment risk, as a result of which authorities adopted several legal acts in the United States, starting from [The Defense Production Act of 1950](#), through the Executive Order 11,858, the Exon-Florio amendment of 1988, [the Foreign Investment and National Security Act of 2007](#) (FINSAs), up to the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). These acts formed the basis for the Committee on Foreign Investment in the United States (CFIUS) [1]. This institution is an interagency committee, chaired by the Secretary of the Treasury [2], designed to review foreign investment and facilitate a decision



by the President of the United States to prohibit a particular foreign investment in the United States based on a risk to national security (Wakely & Indorf, 2018) [3].

On March 30, 1954, the President of the United States, Dwight D. Eisenhower stated that the national interest in foreign economic policy was to achieve the highest possible level of trade and the most efficient use of capital and resources, in a manner consistent with national security that was cost-effective and fair to all, and that would directly strengthen America's allies economically and militarily because their strength was important to the security of the United States (Eisenhower, 1954). In his opinion, the foundation of the internal strength of the American economy was building a system of mutual benefits based on an appropriately high level of bilateral trade (Hiscox, 1999) [4]. Dwight D. Eisenhower added that fewer restrictions and controls, along with the increased efficiency resulting from expanded markets and the freer play of economic forces, were necessary to achieve a sufficiently high level of trade. Finally, he concluded that if the United States failed in its trade policy, it could fail in everything due to problems with domestic employment, living standards, security, and the solidarity of the free world.

The above discussion shows that national security largely depends on the condition of the American economy and the appropriate level of foreign trade, including foreign investments in the United States. It is therefore not surprising that for many decades the United States has had a strategy to protect the American economy, part of which is the strategy of managing the risk of foreign investments for national security (Helping the American Economy Grow, 2018–2022). Following a review of federal law, government documents, and literature, we distinguished three main pillars of the foreign investment risk management strategy. These pillars impact the effectiveness of the management process, which is intended to facilitate decisions on whether to allow a transaction to be conducted in the United States and, if so, whether, subject to certain conditions, to suspend or prohibit the transaction due to national security.

The first pillar of the U.S. foreign investment risk management strategy is the ability of CFIUS, especially the Director of National Intelligence, to analyze risks to USS national security on a national and global basis. We based the second pillar on the right to classify information, constituting the basis for decisions made in the CFIUS risk analysis. Finally, the third pillar concerns maintaining the balance between the openness of the economy and the protection of national security. According to the authors, in the case of each of the above-mentioned pillars, we encountered difficulty or even impossibility in determining the procedure and method of proceeding. On the one hand, this increases the flexibility of decision-makers in protecting national security. On the other hand, it reduces the transparency of the procedure and course of action and thus makes a detailed and holistic assessment of the foreign investment risk management strategy for the national security of the United States difficult or impossible. The assessment was even more difficult because while a review of the American legal system shows that there are many definitions of “national security,” due to their contextual nature, it is difficult to provide a clear answer to the question of what constitutes the subject of protection and why this subject is protected.

Bearing the above in mind, we attempted to confirm the hypothesis that the highest value of foreign investment risk analysis for national security is the protection of the risk management strategy, which consists in the difficulty or inability to become familiar with (1) classified information constituting the basis for CFIUS or the President's decision, (2) the method of identifying and assessing risks to national security in national and global terms, (3) the model or tool used to assess maintaining the balance between the openness of the economy and the protection of national security. We posed the above question because, in our view, the CFIUS risk analysis process has been set up to protect not only national security, a specific investment, industry, market, and the global position of the United States, but, above all, the risk management strategies of foreign investments. To confirm such a thesis, we found it justified to attempt to explain the term “national security,” present a synthetic presentation of the essence of the CFIUS risk analysis and then determine the scope, grounds, and reasons for the

difficulties or the impossibility of assessing the mode or method of proceeding in the three pillars founding the above-mentioned strategy. This article aims to provide an example of a balanced scorecard enabling the assessment of balance and the ability to maintain a balance between the openness of the American economy and national security.

The essence of the American definition of “national security”

The literature on the subject assumes that “national security” is protection against a physical attack from foreign countries or against a justified fear of such an attack (Quist, 1993a, b). The Supreme Court of the United States somehow upheld this narrow approach. For a specific case, the Court assumed that “national security” should cover only the activities of the federal government directly related to protecting the Nation against internal subversion or foreign aggression, and not those that contribute to the strength of the Nation solely through their impact on the general welfare (Cole v. Young, 1956). In turn, in a broad sense, “national security” may encompass many other factors (Developments in the Law, 1972; Emerson, 1982), including current assets and national interests, as well as the sources of power on which our future as a nation depends, such as political assets, provisions of the U.S. Bill of Rights, public authorities, international alliances, and economic assets that radiate around the world from a highly productive domestic economy supported by abundant national resources (Taylor, 1974). The Supreme Court added that an urgent need to protect the above-mentioned values legitimizes and makes the role of national security necessary.

The National Security Act of 1947 (NSA of 1947) does not define the term “national security.” Only the wording of § 1(5) of the Supreme Administrative Court of 1947 defines such concepts as “national intelligence” and “intelligence related to national security.” These terms refer to all intelligence, regardless of its source, including intelligence collected inside or outside the United States that relates to the affairs of more than one United States government agency. These matters include (1) threats to the United States, its citizens, property, or interests; (2) the development, spread, or use of weapons of mass destruction; and (3) any other matter relating to the national security or homeland security of the United States [5]. In turn, the wording of § 1703 (a) (1) of FIRRMA implies that we should interpret the term “national security” to include issues related to homeland security, including critical infrastructure (Reese, 2013) [6]. Even though this definition is included in an act of the rank of an act, it does not provide a precise answer to the question of what the definiendum is. A similar case goes for the definition of “national security” contained in Executive Order 12,356 of the President of the United States, according to which “national security” means the national defense or foreign relations of the United States (§ 6.1(e)).

Synthesis of foreign investment risk analysis for national security under CFIUS

The United States is the world’s largest foreign investor and recipient of foreign investment (Cimino-Isaacs & Sutter, 2024). The administration of the President of the United States has stated that it will ensure that the CFIUS risk analysis “remains responsive to the changing national security landscape and the nature of investments that pose related risks” (Executive Order 14,083). Generally, the risk analysis process begins with a notification to CFIUS by the parties to the transaction, except as specified in FIRRMA. In practice, transaction parties are motivated to voluntarily notify CFIUS because they seek to obtain a so-called safe harbor, i.e., avoid potential non-compliance with the results of the CFIUS risk analysis as a result of investment expenditure (Tipler, 2014). This is because unnotified transactions are subject indefinitely to future CFIUS risk analysis, which may result in the President’s decision to prohibit foreign investment, including ordering the sale of the subject of the transaction, even after incurring capital expenditure. Following the passage of FIRRMA, CFIUS increased resources to monitor unreported questionable transactions and initiate risk analysis. For example, in 2022, there were 154 declarations and 286 notifications submitted under the

CFIUS risk analysis, and authorities initiated 162 investigations based on them (Cimino-Isaacs & Sutter, 2024) [7].

Notification to CFIUS by the parties to the transaction may be made through a declaration, in which case the risk analysis takes up to 30 days, or a notification – up to 45 days. The scope of the notification determines the differences between a declaration and a notification, the CFIUS work schedule, and CFIUS’s ability to respond to a specific case. The declaration is obligatory in two cases. First, when a foreign government becomes the beneficiary of a “substantial interest” [8] in a company such as TID U.S. [9]. Second, the transaction involves a TID U.S. business that produces, designs or manufactures critical technology subject to licensing or export controls. CFIUS and the dedicated federal agency responsible for the area of the transaction conduct a risk analysis to determine the impact of the foreign investment on USS national security, relying on the risk analysis conducted by the Director of National Intelligence (DNI) and his Intelligence Community (IC). In its risk analysis, CFIUS considers the risks, vulnerabilities, and national security implications associated with foreign investment, including the volume of domestic production needed to meet projected defense needs; the extent of control of domestic industry and commercial activities by foreign nationals; impacting the potential sale of military goods, equipment or technology to a country that supports terrorism, the spread of missile technology or chemical and biological weapons; United States technological leadership in areas affecting national security; impact on critical infrastructure, including major energy assets and critical technologies.

CFIUS initiates an investigation that may last up to 45 days if it determines that a transaction: (1) threatens national security and the risk has not been minimized; (2) is controlled by a foreign government or would result in foreign control of any portion of United States critical infrastructure. CFIUS may extend the investigation for another 15 days if “extraordinary circumstances” arise. Importantly, CFIUS may negotiate and instruct the parties to adopt specific provisions or terms of the agreement that minimize risk, and a dedicated federal agency competent for the area of the transaction is responsible for monitoring compliance with the implementation of the newly adopted provisions or terms of the agreement [10]. Finally, if CFIUS determines that despite the risk of minimization actions taken, the transaction still poses a threat to national security, CFIUS may submit to the President of the United States a prohibition of the transaction unless the parties decide on their own to withdraw from it. The President of the United States has 15 days to decide from the moment CFIUS submits its recommendation (Cimino-Isaacs & Sutter, 2024) [11].

Analysis of foreign investment risks to national security in national and global terms

The DNI is responsible for the in-depth analysis of all national security risks from foreign investments under CFIUS [12]. The purpose of the analysis is to identify any identified gaps in the IC’s intelligence collection [13]. Risk analysis should be independent, objective, and consistent with all applicable directives, policies, analytical tools, and standards of the IC craft [14]. The DNI may also provide CFIUS with an assessment, separate from the risk analysis, of any operational impact of a given foreign investment on the IC’s operations and recommended actions by the IC that it has or will take to minimize such impact. It follows from the above that, in practice, the IC plays an important role in the CFIUS risk analysis because the risk analysis is based mainly on intelligence and counterintelligence data, as well as other essential data remaining in the IC resources, including military, police, financial and fiscal data, geospatial, etc.

As a rule, data collected by the IC for risk analysis constituting the basis for decisions made by CFIUS or the President of the United States are classified, if only due to their intelligence or counterintelligence nature, which means that it may be difficult to obtain not only source data but also methods of collecting them. This is hardly surprising because in the case of foreign investments, the risk to national security comes from the side of the transaction that has its roots in another country or even the government of another country is behind it (Foreign Economic Espionage in Cyberspace Report, 2018; CFIUS, Annual Report to Congress, 2023)

[15]. For example, the DNI report titled, “Venture Capital and Supply Chain Vulnerabilities” shows that one of the most potentially harmful vulnerabilities for a company is a foreign adversary impersonating a private investor, especially in transactions involving start-ups and venture capitalists (Venture Capital, VC) ([When the Invisible Hand \(. . .\)](#), 2023). It added that VC investors can gain a significant position in a company through investment opportunities, including capital expenditures (e.g., land and/or equipment purchases) or other operational or financial improvements to achieve growth. However, these seemingly benign transactions allow foreign adversaries to quietly insert board members, secure voting rights, and/or access confidential corporate data. In the DNI’s opinion, by masking the real “investor,” VC transactions may allow the transaction to be completely bypassed or approved by CFIUS ([O’Connor, 2019](#)).

Another example of foreign investments posing a high risk to the United States’ national security is transactions supported by the government of the People’s Republic of China (PRC) ([Saha, 2012](#); [Bateman, 2022](#)). The annual report of the government’s U.S.-China Commission shows that the following investments deserve special attention:

- (1) in technology areas prioritized by adversaries, including China’s 14th Five-year Plan, Made in China (2025), and other related initiatives;
- (2) to American companies that have received funding from the Department of Defense, Department of Commerce, Department of Energy, and other U.S. government institutions, other funds from the U.S. government for projects of critical importance to national security and competitiveness;
- (3) that can provide privileged access to expertise, business networks, and production methods critical to maintaining the economic and technological competitiveness of the United States ([Moran, 2009](#); [Report to Congress of the US.-China, 2023](#)).

As part of the CFIUS risk analysis, it may often turn out that national security risks concern not only the United States but also other countries, especially allied and partner countries, or critical data may remain in the resources of allies and partners ([Larson and Marchick, 2006](#)). If such a situation arises, the Chairman of CFIUS, in consultation with other members of the Committee, should establish a formal process for exchanging information with the governments of countries that are allies or partners of the United States to protect the national security of the United States and those countries. The exchange of information is intended to harmonize activities regarding (1) investment and technology trends that could pose a risk to the national security of the United States and its allies or partners; (2) specific technologies and entities purchasing such technologies; (3) holding regular consultations and meetings with representatives of the governments of these countries. Importantly, meeting the needs for ongoing information exchange also applies to the threat analysis stage conducted by the DNI, i.e., at the intelligence or counterintelligence stage. Despite many multilateral or bilateral agreements concluded between the United States and its allies and partners, the so-called Five Eyes Agreement ([Cox, 2012](#)), an Anglo-Saxon alliance of intelligence and counterintelligence services from Australia, Canada, New Zealand, Great Britain, and the United States ([Charter of the Five Eyes, 2017](#)).

Noteworthy, not all activities as part of the analysis of the risk of foreign investments for national security must relate to intelligence or counterintelligence activities. From the review of available public tools that can enable or facilitate this type of analysis, the most noteworthy is U.S. spending, which is the official and open source of federal data on public spending, including information on contracts, grants, loans, and public procurement [16]. The initiative came from the Bureau of the Fiscal Service, which manages central payment systems and public debt. For example, the total planned budget expenditure in 2023 was around USD 5 trillion and 800 billion ([Budget of the U.S. Government, 2023](#)). The creation of this type of tool using artificial intelligence not only facilitates the support of the budget expenditure management process and

enables the optimization of the federal government's accounting system but also comprehensively ensures the security of the American budget and economy, until and finally, national security (Lizak & Skuza, 2023).

The second example is the National Strategy for Global Supply Chain Security, which is a response not only to the fact that the global supply chain is becoming more and more complex and global, and therefore, on the one hand, is more and more exposed to disruptions, including natural hazards and accidents and malicious incidents. However, on the other hand, it is a tool that can enable or facilitate the strengthening of the global supply chain to protect the prosperity and interests of the Nation, secure the economic well-being, as well as the national security of the United States (The National Strategy for Global Supply Chain Security, 2021). The strategy's overarching goal is to strengthen the global network of transport, postal, and shipping routes, as well as the assets and infrastructure through which goods move from the production point to the final consumer. The strategy's two operational objectives include promoting the efficient and safe flow of goods and supporting supply chain resilience, which is based on integrating and galvanizing the efforts of the federal administration and the international community, as well as managing supply chain risks by identifying, assessing, and prioritizing actions.

On the openness and secrecy of data in the analysis of risks to national security

Four exceptions are introduced in FIRRMA that do not prohibit the disclosure of information collected as part of CFIUS's risk review process. First, information relevant to any administrative or judicial action or proceeding is public (Ralls v. CFIUS, 2014; Fitzpatrick, 2016). Second, information for Congress or any authorized committee or subcommittee of Congress cannot be limited. Third, information relevant to national security analysis or CFIUS activities provided, under the sole supervision of the CFIUS Chairman, to any agency of the federal government or any foreign government entity of a USS ally or partner should remain public. Moreover, authorities should provide information only to the extent necessary to ensure the achievement of goals related to national security and compliance with the requirements for the protection of classified information. Fourth, information to which the parties to the transaction have agreed to disclose is public.

The literature identifies several reasons which, on the one hand, support the need to ensure full disclosure of data in risk analysis by CFIUS, and, on the other hand, maintain the current model in which some data remains secret. The first group includes:

- (1) Continuous strengthening of trust in the market and investors;
- (2) Maintaining democratic accountability through transparency, which enables social and political control;
- (3) Regulatory predictability in economic transactions, especially enabling the comparison of the actual situation with the legal status;
- (4) Political stability of the concept of an open economy to foreign investment (Eisenhower, 1954);
- (5) The importance of information for public discussion and education (Quist, 1993a, 1993b).

The second group of premises, or rather criteria, for assessing the risk to national security related to the disclosure of information include:

- (1) Helping other nations develop new weapons, critical technologies, and critical infrastructure;
- (2) Helping other nations improve their weapons (Tolman *et al.*, 1945);

- (3) Assisting other nations in the production of weapons materials, especially chemical, biological, radiological, and nuclear weapons (CRBN),
- (4) Helping other nations to strengthen the efficiency of their raw materials policy and technological processes;
- (5) Adverse effects on USS foreign relations, arms control negotiations, or treaty obligations;
- (6) Any other impact or significance for national security;
- (7) Negative effects on the credibility of the classification program (Quist, 1993a, b),
- (8) Threat to operational security, including the risk management process or specific operations of special services of a defensive and offensive nature;
- (9) Making it difficult or impossible to make strategic decisions without the influence of external lobbying or political pressure.

Considering the statutory exclusion from data disclosure for CFIUS due to compliance with the requirements for the protection of classified information, it is reasonable to note that in American law, there are three conditions for the classification of classified information, the first two of which occur when the information is subject to classification and remain within the domain and control of the federal government. The third condition is met when the answer to the following question is affirmative: Should this information be classified because its unauthorized disclosure could reasonably cause harm to national security? (§ 1.1(a) (3) EO 12356, 1982). The answer to this question is that if authorities can reasonably expect harm to national security from the disclosure of information, then the information should be classified to prevent that harm from occurring. This is important because if classified data was used in the threat analysis prepared by DNI and then submitted to CFIUS, it will remain secret even if the four previously mentioned statutory cases occur, which do not prohibit the disclosure of data in the CFIUS risk analysis.

Assessment of maintaining balance and assessing the ability to maintain balance between the openness of the economy and the protection of national security

Following a review of publicly available sources, we could not isolate an official document of the federal government on the assessment of maintaining balance and the assessment of the ability to maintain a balance between the openness of the economy and the protection of national security. The first of these assessments would seek to retrospectively assess the effectiveness of the foreign investment risk management strategy for national security, which would enable it to provide feedback for continuous improvement of this strategy. The second assessment would make it possible to measure the potential or readiness to maintain balance, i.e., it would analyze the expected possibilities of dealing with future challenges and risks. In our opinion, both assessments are important because one allows for more accurate planning and preparation of effective risk management and strategic decision-making, and the other provides feedback on the results of actually undertaken actions. For CFIUS's risk assessment, a balancing assessment could provide insight into how to address the specific risks of foreign investment, and a balancing assessment could provide insight into how to prepare to identify risks associated with foreign investment.

There is no doubt that maintaining a balance between the openness of the economy and the protection of national security is a complicated process, at least due to factors that may influence this process, including, for example, diplomatic relations, international agreements, sources of capital, restrictive measures, data security, geopolitical conditions, condition of the economy, political pressure, public opinion, dynamics of technological development, lobbying, and corruption. On the one hand, these factors may significantly hamper the assessment of maintaining

balance and the assessment of the ability to maintain balance. On the other hand, they may collectively constitute the basis for creating a foreign investment risk matrix for national security. A review of the CFIUS annual activity report for 2023 shows that this type of assessment is not included, and therefore there are no conclusions arising from these assessments.

CFIUS's 2023 annual activity report shows that as the main form of foreign investment, USS mergers and acquisitions (M&A) accounted for a small percentage of the total number of such investments in the United States. For example, in 2023, the CFIUS risk analysis covered 35 M&A transactions involving investors from Kuwait, Lebanon, Qatar, and Saudi Arabia amounting to approximately USD 10.3 billion, while the total number of this type of transactions and their value in the United States amounted to 1,327 transactions worth USD 230.7 billion (CFIUS, *Annual Report to Congress*, 2023). Interestingly, the report answers two important questions. In response to the first question, whether there is credible evidence of a coordinated strategy for the acquisition of critical technologies, we read that one cannot present the results of the IC risk analysis in a public report. To the second question, whether foreign governments used espionage to obtain trade secrets related to critical technologies, the IC's answer was affirmative, and its justification only indicated that foreign governments most likely use several methods to collect data on U.S. critical technologies.

A review of the annual report on CFIUS activities led the authors to the conclusion that it is possible to isolate measures to assess the balance and assess the ability to maintain a balance between the economy's openness and the protection of national security, and then present them in the form of a balanced scorecard (Kaplan & Norton, 1992). According to R.S. Kaplan and D.P. Norton's balanced scorecard, which is an instrument of strategic management, allows decision-makers to illustrate the process from four perspectives: customer (how do customers perceive us?), internal (what do we need to excel at?), learning and development (can we continue to improve and create value?), financial (how do shareholders perceive us?). In turn, according to the authors of this publication, the goals and measures in the individual perspectives of the balanced scorecard under the CFIUS analysis could, in addition to the provision of national security, include:

- (1) Customer perspective (Lizak & Skuza, 2024):
 - Goal: maintaining investment attractiveness;
 - Meters:
 - Predictability and transparency of law;
 - Stability of energy prices and increasing its availability;
 - Investment resistance to potential new problems, crises, and threats;
- (2) Internal perspective:
 - Purpose: to ensure the efficiency and effectiveness of CFIUS risk analysis;
 - Meters:
 - Number of applications subject to CFIUS risk analysis;
 - Number and type of preventive or regulatory measures implemented;
 - Immediate response to the identification of risks associated with foreign investment;
- (3) Learning and development perspective:
 - Goal: development of competencies, infrastructure, and access to data and their analysis;
 - Meters:

- Investments in data analysis and AI technologies for risk analysis;
- Training employees in minimizing the risk to national security;
- Processing time of applications by CFIUS;

(4) Financial perspective:

- Goal: maintaining economic growth
- Meters:
 - Value of the inflow of foreign investments;
 - GDP growth rate relative to the value of foreign investments;
 - Costs of CFIUS risk monitoring and analysis, including actions taken by the IC.

Of course, the Balanced Scorecard and objectives and metrics presented above are illustrative and one may adapt them to the specific results of risk analysis or political priorities, as well as external variables such as global economic trends or geopolitical conditions. We cannot exclude a hybrid approach, i.e. a combination of approaches, methods, and analyses, to achieve an optimal assessment of the balance and ability to maintain a balance between the openness of the economy and national security.

Conclusions

Accounting for less than 5% of the world's population, Americans generate and earn over 20% of total global income, according to the Office of the United States Trade Representative. America is the world's largest national economy and a leading global trader ([Economy & Trade, 2024](#)). As already mentioned, opening world markets and expanding trade, initiated in the United States in 1934 and consistently continued since the end of the Second World War, played an important role in the pursuit of American prosperity. Although bilateral trade remained the engine of growth for the United States, in 2018, the authorities increased the tariff on several imported products, which was an expression of a change in trade policy towards the PRC and even the start of a trade war ([Benguria, Choi, Swenson, & Xu, 2020](#)). The U.S.-PRC trade war has the distinction of representing one of the largest and most abrupt shifts in trade policy in USS history, especially when compared to the leading role the United States has historically played in the process of liberalizing customs duties around the world ([Fajgelbaum & Khandelwal, 2021](#)).

Following a review of foreign investment risk management strategies in the United States from a national security perspective, we concluded that this trade war has seen a dramatic increase in the need for the ongoing use of CFIUS risk analysis. This is because, on the one hand, the United States is critical about maintaining the openness of the American economy to foreign investments, especially in the era of AI development, which ensures and will continue to ensure the position of the largest national economy in the world and a global hegemon. On the other hand, this openness may generate critical risks to national security from the most potent economic rival, i.e. the People's Republic of China. In such an operational situation, the role of CFIUS is colloquially to "separate the sheep from the goats." The preliminary assessment of the risk-based approach within CFIUS allowed us to hypothesize that CFIUS enables the protection of the national security of the United States against the risk of foreign investments but it did not allow us to determine whether it provides this protection.

First, IC collects the data used in the CFIUS risk analysis, which determines their confidential nature. This means that the secrecy clause covers data for risk analysis, its source, and the method of obtaining it. There is nothing extraordinary about this because it is difficult to imagine any other effective method of verifying the actual nature of foreign investments other than through intelligence or counterintelligence activities, which by their nature are

secret. This approach is supported not only by the ambiguous state and economic identity of the actual beneficiary of the foreign investment, as well as its ally or partner or a third party cooperating with it but also by the area or industry of the transaction, which in practice is often characterized by hermeticity or entry barriers. As previously mentioned, there is openly available data that is likely used in the CFIUS risk analysis, but its combination with classified data also causes the open data to become classified, much less the conclusions drawn from the combination of open and classified data. Here is a simplified version of your sentence with clearer syntax while keeping the meaning intact: Since the DNI, which leads the IC and includes intelligence and counterintelligence services, oversees the risk analysis of foreign investments, accessing information is nearly impossible. This includes not only the data used but also its sources, collection methods, risk identification process, risk model assessment, and the overall strategy for managing foreign investment risks to U.S. national security.

Second, following a review of the definition of “national security” in U.S. federal law, we concluded that, on the one hand, the scope of tasks related to national security is comprehensive, and on the other hand, extremely vague, not least because of the number of terms used, that are imprecise or undefined in U.S. law. This approach does not surprise the authors because, in their opinion, the term “national security” is characterized by complexity and a multi-aspect nature, starting from the relationship of this term with military risk through economic, social, and political to ecological and cybersecurity risks, which are dynamically evolving and their character changes, as does the environment. We must also mention that the term “national security” is susceptible to a variety of interpretations, not only to achieve a specific political goal but also to the national interest, history, culture, and current priorities. All this means that “national security” covers a wide spectrum of issues best interpreted in a specific context, as they are difficult to include in a single and universal definition.

Third, the greatest challenge for the United States in managing foreign investment risk is maintaining the balance between the economy’s openness and the protection of national security. As already mentioned, we could not find an official government document on the assessment of maintaining balance and the assessment of the ability to maintain a balance between the economy’s openness and the protection of national security. Several fundamental questions arise here, including what model or tool to use to assess balance or the ability to maintain balance, what goals and measures to adopt, and what critical weights to establish to determine an undesirable deviation of the scales if this situation were compared to a weighing scale. A review of the annual report on CFIUS’s activities shows that it only contains statistical data that does not refer to the relationship between the openness of the economy and national security. *Prima facie*, it seems that for now there is no need to develop a cyclical assessment of balance or the assessment of the ability to maintain balance because, on an annual basis, there is hardly a situation in which a single investment could threaten this balance. Moreover, each foreign investment has different characteristics. Hence, one should conduct the risk analysis *in concreto*. We cannot exclude that such an assessment was made before the above-mentioned increase in tariffs in 2018, which constituted a significant change in the United States trade policy. Nevertheless, a review of the annual report on CFIUS activities led us to the conclusion that it is possible to separate goals and measures to assess the balance and the ability to maintain a balance between the economy’s openness and the protection of national security, an example of which is presented in the basic form of the balanced scorecard.

Fourth, although the publication concerns the analysis of the risk of foreign investments for national security in the United States, it is impossible not to mention that the legal framework for monitoring foreign direct investments in the European Union established in 2019 could take a cue from the American model, especially in the context of collecting information for the protection of foreign direct investments and coordinating the exchange of information within the federal administration structure (Regulation (EU) 2019/452). On the one hand, we cannot exclude that this pattern is already in use, as work is underway in the EU to change the legal framework in this area ([Opinion of the EESC, 2024](#)), and one of its important provisions is the establishment by Member States of the obligation to introduce monitoring mechanisms

investments, which will translate into strengthening database resources on this type of investments ([Proposal for a Regulation, COM \(2024\) 23 final](#)). In theory and practice, scholars noticed that the current legal framework in the EU was considered too general and vague, not allowing for harmonization and giving the system a decentralized character ([Czapracka, Gac, Gubański, & Małobęcki, 2022](#)), which translates into a significant diversity of national legal acts regulating this matter, which in turn constitutes a huge challenge for investors conducting transactions within the EU ([Długosz, 2022](#)). Moreover, unlike CFIUS, the European Commission does not have the competence to independently check or block foreign investments. On the other hand, the opinion on the draft new EU act regulating the monitoring of foreign investments in the EU noted that the new regulation should avoid creating the impression of unjustified protectionism, which could constitute ammunition for those who want to discredit the EU's commitment to an open economy. It added that transparency and predictability are non-negotiable. *Prima facie*, one may get the impression that the legal framework for the protection of foreign investments in the EU will not be a temporary solution for the pandemic crisis, as originally assumed, and will not be as offensive as in the United States.

To sum up, we positively confirmed the formulated hypothesis because in the CFIUS risk analysis, there are great difficulties, and in some circumstances, it is even impossible to get acquainted with the classified data that constitute the basis for decisions made by CFIUS or the President of the United States. The situation resembles familiarization with the way of identifying and assessing national security risks from a national and global perspective, as well as with the model or tool used to assess maintaining the balance between the economy's openness and the protection of national security. In the latter case, it seems that for now, there is no need to prepare such an assessment periodically and publish it. Here is a simplified and corrected version of your sentence with the same meaning and proper sentence flow: The confirmation of the hypothesis indirectly supports the statement that, since access to key aspects of CFIUS risk analysis may be difficult or impossible due to secrecy imposed by the involvement of intelligence and counterintelligence services within the Intelligence Community, the highest priority of the foreign investment risk management strategy is to protect itself. This is achieved by preventing detailed and holistic assessments, ensuring national security for the United States.

Notes

1. As long as the above acts are of the greatest importance for the discussed issue, they are not the only legal acts regulating international trade and aimed at minimizing risks to the national security of the United States. See [The Trading with the Enemy Act of 1917](#), the 65th United States Congress, Public Law 65–91, 40 Stat. 411, October 6, 1917; [The International Emergency Economic Powers Act](#), the 95th United States Congress, Public Law 95–223, 91 Stat. 1,625, December 28, 1977; [The Export Administration Act of 1979](#), the 94th United States Congress, Public Law 94–329, 90 Stat. 729, June 30, 1976; [The Export Administration Act of 1979](#), the 96th United States Congress, Public Law 96–72, 93 Stat. 503, September 29, 1979.
2. The committee includes the Secretary of the Treasury (Chairman), the Secretaries of the Departments of State, Defense, Homeland Security, Commerce, and Energy; Attorney General; United States Trade Representative; Director of the Office of Science and Technology Policy. The Secretary of Labor and the Director of National Intelligence serve as *ex officio* members. Representatives from five White House offices serve as observers or participants at CFIUS, and the Council of Economic Advisers and the National Security Council may participate as appropriate. The president may appoint other officials to serve as needed and on a case-by-case basis.
3. CFIUS analyses the risks of mergers and acquisitions that may result in foreign control of a U.S. company; certain investments involving critical technologies or critical infrastructure or sensitive personal data; certain real estate transactions.
4. We may identify the beginning of the openness of the American economy to foreign investment with the adoption of the [Reciprocal Trade Agreements Act of 1934](#) (the 73rd United States Congress,

Public Law 73–316, 48 Stat. 943, June 12, 1934). In practice, the Act ushered in an era of liberal and global U.S. trade policy that lasted throughout the twentieth century.

5. The wording of § 101(b) of the Supreme Administrative Court of 1947 established the scope of duties of the National Security Council, which included: (1) advising the President on the integration of domestic, foreign and military policies, policies relating to national security, so as to enable the Armed Forces and other departments and agencies of the United States Government to cooperate more effectively on matters related to national security; (2) assessing and estimating United States objectives, commitments, and risks with respect to United States actual and potential military power and making recommendations thereon to the President; (3) making policy recommendations to the President on matters of common interest to the departments and agencies of the United States Government concerned with national security; (4) coordinating, without assuming operational authority, the United States Government’s response to malign foreign influence operations and campaigns.
6. The term “homeland security” is no less difficult to interpret than the term “national security”. A review of government documents that define “internal security” shows that these definitions have the following: common elements:
 - the homeland security enterprise includes activities of federal, state, local and tribal governments, and the private sector that require coordination;
 - internal security may include protecting against specific and all threats and responding to these threats;
 - actions for internal security do not mean complete protection or complete reduction of the threat.
7. The President of the United States may exercise the authority to suspend or prohibit foreign investment, subject to a CFIUS risk analysis, when: (1) there is credible evidence that a foreign entity may engage in actions that threaten national security; (2) no other laws provide “adequate and appropriate authority” to protect against national security risks.
8. Pursuant to 31 Code of Federal Regulations § 800.248 – U.S. Enterprise TID means any enterprise that:
 - (a) produces, designs, tests, produces or develops one or more critical technologies;
 - (b) performs the functions set out in the Annex related to the critical infrastructure investment;
 - (c) maintains or collects, directly or indirectly, sensitive personal information about United States citizens.
9. Pursuant to 31 Code of Federal Regulations § 800.244(a) - Substantial interest means, in the context of the acquisition of an interest in a U.S. corporation by a foreign person, a direct or indirect voting interest of 25 percent or more, and in the context of a foreign person’s national or regional governments of one foreign country, subject to paragraph (b) of this section, a direct or indirect voting interest of 49 percent or more.
10. On October 22, 2022, the Treasury Department issued “CFIUS Enforcement and Penalty Guidelines” and on April 15, 2024, the Treasury Department published amendments to “Penalty Provisions, Provision of Information, Negotiation of Mitigation Agreements, and Other Procedures Pertaining to Certain Investments in the United States by Foreign Persons and Certain Transactions by Foreign Persons Involving Real Estate in the United States.” A Proposed Rule by the Investment Security Office, 31 CFR Parts 800 and 802.
11. Cases of blocking foreign transactions by the President of the United States by year and area: 1990 – Aviation and space; 2012 – Renewable energy sources; 2016 – Semiconductors, 2017 – Semiconductors, 2018 – Semiconductors, 2020 – Software, 2020 – Digital Platform, 2024 – Cryptocurrency miner.
12. See provision of § 12(1) (A) (i) FIRRMA. The Director of National Intelligence (DNI) is a member of the United States federal government required by the Intelligence Reform and Terrorism Prevention Act of 2004 to serve as the Executive Chief of the United States Intelligence Community and to direct and supervise the National Intelligence Program.
13. Pursuant to § 3 (a) (11) of FIRRMA in connection with § 3 (4) of the Supreme Administrative Court of 1947, the term “Intelligence Community” means 17 intelligence agencies and organizational units of the federal administration, including Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence Defense Intelligence Agency, Office of Intelligence and

Counterintelligence (Department of Energy), Office of Intelligence and Analysis (Department of Homeland Security), Bureau of Intelligence and Research (Department of State), Office of Intelligence and Analysis (Department of the Treasury), Office of National Security Intelligence (Drug Enforcement Administration), Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, Naval Intelligence, Space Force Intelligence.

14. In accordance with Intelligence Community Directive (ICD) no. 211 Intelligence Community Support to the Committee on Foreign Investment in the United States (CFIUS) Threat Analysis Process, the Community has established the National Intelligence Manager for Economic Security and Financial Intelligence, who is responsible at the working level for the Community's integrated approach in support of CFIUS, and also develops and coordinates a unified intelligence strategy to guide the collection and analysis of data related to the security of foreign investments, taking into account the priorities established in ICD no. 204 and National Intelligence Priorities, including plans and campaigns to integrate IC efforts and identified gaps in intelligence activities. See Intelligence Community Support to the Committee on Foreign Investment in the United States (CFIUS) Threat Analysis Process, ICD no. 211, September 4, 2022. Available from: <https://irp.fas.org/dni/icd/icd-211.pdf> (accessed: 30.08.2024); ICD no. 204, National Intelligence Priorities Framework, July 1, 2021; ICD no. 204, National Intelligence Priorities Framework, July 1, 2021.
15. According to the 2024 DNI Annual Analysis and the National Counterintelligence and Security Center's 2018 Report to Congress, foreign economic, industrial and cyber espionage by foreign actors such as China, Russia, Iran and North Korea against the United States continues poses a serious threat to the prosperity, security, and competitive advantage of the United States.
16. USAspending.gov is a government website containing current data on federal government spending and enabling verification of the purpose of public spending and its beneficial owners, <https://www.usaspending.gov/>

References

- Bateman, J. (2022). *U.S.-China technological 'decoupling'. A strategy and policy framework, with foreword by Eric Schmidt* (pp. 21–23). Washington, DC: Carnegie Endowment for International Peace.
- Benguria, F., Choi, J., Swenson, D. L., & Xu, M. (2020). *Anxiety or pain? The impact of tariffs and uncertainty on Chinese firms in the trade war*. In *Technical representative*. Cambridge, MA: National Bureau of Economic Research. doi: [10.3386/w27920](https://doi.org/10.3386/w27920).
- Budget of the U.S. Government (2023) *Fiscal year 2023, office of management and budget*. Washington: White House. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf
- CFIUS, Annual Report to Congress (2023). Committee on foreign investment in the United States, annual report to congress, report period: CY 2023; M&A at a glance, Paul, Weiss, Rifkind, Wharton & Garrison LLP, 2023 Year-end roundup. Available from: https://www.paulweiss.com/media/3984199/maag_2023_year_end_roundup.pdf
- Charter of the Five Eyes Intelligence Oversight and Review Council (2017). Available from: <https://www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf>
- Cimino-Isaacs, C. D., & Sutter, K. M. (2024). The committee on foreign investment in the United States. Congressional Research Service. IF10177, version 30, Updated May 17.
- Cole v. Young, 351 U.S. 536 (1956). U.S. Supreme Court. June 11, 1956.
- Cox, J. S. (2012). Canada and the five eyes intelligence community. Strategic Studies Working Group Papers. Canadian Defence & Foreign Affairs Institute and Canadian International Council.
- Czapracka, K., Gac, M., Gubański, J., & Małobęcki, I. (2022). Kontrola inwestycji zagranicznych – wstępna ocena polskiego ustawodawstwa i praktyki w kontekście europejskich i światowych trendów. *Internetowy Kwartalnik Antymonopolowy I Regulacyjny*, 11(4), 8–31. doi: [10.7172/2299-5749.IKAR.4.11.1](https://doi.org/10.7172/2299-5749.IKAR.4.11.1).

- Developments in the Law: The National Security Interest and Civil Liberties (1972). *Harvard Law Review*, 85(6), April, 1133. doi: [10.2307/1340060](https://doi.org/10.2307/1340060).
- Długosz, T. (2022). Kontrola inwestycji zagranicznych w Unii Europejskiej. Podstawowe zasady i tendencje. *Prawo i Więź*, 2(40). doi: [10.36128/priw.vi40.423](https://doi.org/10.36128/priw.vi40.423).
- Economy & Trade (2024). The office of the United States trade representative. Available from: <https://ustr.gov/issue-areas/economy-trade>
- Eisenhower, D. D. (1954). Special message to the congress on foreign economic policy. In G. Peters, & J. T. Woolley (Eds.), *The American Presidency Project*. Available from: <https://www.presidency.ucsb.edu/node/233632>.
- Emerson, T. I. (1982). National security and civil liberties. *Yale Journal of World Public Order*, 9, 78–79.
- Fajgelbaum, P., & Khandelwal, A. (2021). The economic impacts of the US-China trade war. doi: [10.3386/w29315](https://doi.org/10.3386/w29315), National Bureau of Economic Research. Working Paper No. 29315, September, Revised December 2021, JEL No. F0. Available from: <https://www.nber.org/papers/w29315>
- Fitzpatrick, C. M. (2016). Where ralls went wrong: CFIUS, the courts, and the balance of liberty and security. *101 Cornell Law Review*, 101(4), 1087–1112.
- Foreign Economic Espionage in Cyberspace Report (2018). The national counterintelligence and security center.
- Helping the American Economy Grow. (2018–2022). *Helping the American economy grow, strategic plan 2018-2022*. Washington, DC: U.S. Department of Commerce.
- Hiscox, M. J. (1999). The magic bullet? The RTAA, institutional Reform, and trade liberalization. *International Organization*, 53(4), 669–698. doi: [10.1162/002081899551039](https://doi.org/10.1162/002081899551039).
- Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard – measures that drive performance. *Harvard Business Review*, 70(1), 71–79.
- Larson, A. P., & Marchick, D. M. (2006). Foreign investment and national security. Getting the balance right. In *The Bernard and Irene Schwartz Series on American Competitiveness*. Council on Foreign Relations, CSR No. 18, July 32.
- Lizak, R., & Skuza, S. (2023). AI enables the control of public finances: US federal government initiatives. *Białostockie Studia Prawnicze*, 28(2), 185–190. doi: [10.15290/bsp.2023.28.02.11](https://doi.org/10.15290/bsp.2023.28.02.11).
- Lizak, R., & Skuza, S. (2024). The inflation reduction act as an element of shaping the US grand strategy and the UN strategy of global goals. *Białostockie Studia Prawnicze*, 29(1), 11–26. doi: [10.15290/bsp.2024.29.01.01](https://doi.org/10.15290/bsp.2024.29.01.01).
- Moran, T. H. (2009). *Three threats: An analytical framework for the CFIUS process* (pp. 1–65). Peterson Institute for International Economics. Washington, D.C..
- Opinion of the European Economic and Social Committee (2024). Proposal for a regulation of the European parliament and of the Council on the screening of foreign investments in the union and repealing regulation (EU) 2019/452 of the European parliament and of the Council, (COM (2024)23 final – 2024/0017 (COD)). *Official Journal of the European Union*, C series, C/2024/6027, Document 52024PC0023.
- O’Connor, S. (2019). How Chinese companies facilitate technology transfer from the United States. In *U.S.-China Economic and Security Review Commission*. Staff Research Report.
- Proposal for a Regulation, COM (2024) 23 final (2024). Proposal for a regulation of the European parliament and of the Council, COM(2024) 23 final, 2024/0017(COD), European Commission.
- Quist, A. S. (1993a). Chapter 5. Information-disclosure risks and benefits. In M. Marietta (Ed.), *Security Classification of Information*. Oak Ridge National Laboratory, April, U.S. Department of Energy.
- Quist, A. S. (1993b). Volume 2. Principles for classification of information. In M. Marietta (Ed.), *Security Classification of Information*. Oak Ridge National Laboratory, April, U.S. Department of Energy doi: [10.2172/6934153](https://doi.org/10.2172/6934153).
- Ralls corporation v. Committee on foreign investment in the United States (2014). U.S. Court of appeals — District of Columbia circuit, No. 13–5315, 13–5315, 758 F.3d 296.

- Reese, S. (2013). Defining homeland security: Analysis and congressional considerations. (8–10). Congressional Research Service R42462, Updated January 8.
- Reciprocal Trade Agreements Act of 1934 (1934). The 73rd United States congress, public law 73-316, 48 Stat. 943.
- Report to Congress of the U.S.-China Economic and Security Review Commission (2023). One hundred eighteenth congress. Washington. First Session.
- Saha, S. (2012). CFIUS now made in China: Dueling national security review frameworks as a countermeasure to economic espionage in the age of globalization. *Northwestern Journal of International Law and Business*, 33(199), 199–235. doi: [10.54648/BULA2012048](https://doi.org/10.54648/BULA2012048).
- Sosin, J. M. (1963). The Massachusetts acts of 1774: Coercive or preventive?. *Huntington Library Quarterly*, 26(3), 235–252. doi: [10.2307/3816653](https://doi.org/10.2307/3816653).
- The Defense Production Act of 1950 (1950). The 81st United States congress, public law 81-774, 64 Stat. 798.
- Taylor, M. (1974). The legitimate claims of national security. *Foreign Affairs*, 57(3), 577. doi: [10.2307/20038070](https://doi.org/10.2307/20038070).
- The National Security Act of 1947 (1947). The 80th United States congress, public law 80-253, 61 Stat. 495.
- The National Strategy for Global Supply Chain Security (2021). The national strategy for global supply chain security, The White House, Washington.
- The Export Administration Act of 1979 (1979). The 96th United States congress, public law 96-72, 93 Stat. 503.
- The Foreign Investment and National Security Act of 2007 (2007). The 110th United States congress, public law 110-49, 121 Stat. 246.
- The Trading with the Enemy Act of 1917 (1917). The 65th United States congress, public law 65-91, 40 Stat. 411.
- Tipler, C. M. (2014). Defining ‘national security’: Resolving ambiguity in the CFIUS regulations. *University of Pennsylvania Journal of International Law*, 35(4), 1223–1236.
- Tolman, R. C., Bacher, R. F., Compton, A. H., Lawrence, E. O., Oppenheimer, J. R., Spedding, F. H., & Urey, H. C. (1945). Report of committee on declassification (p. 3). Memorandum to Maj. Gen. L. R. Groves. Oak Ridge, TN.
- Wakely, J., & Indorf, A. (2018). Managing national security risk in an open economy: Reforming the committee on foreign investment in the United States. *Harvard National Security Journal*, 9 (2), 7–10.
- When the invisible hand (2023). *When the invisible hand turns into a sleight of hand: Understanding how venture capital is used to create vulnerabilities in the supply chain, venture capital and supply chain vulnerabilities*, National Counterintelligence and Security Center. Washington, DC: Office of the Director of National Intelligence. Available from: <https://www.dni.gov/files/NCSC/documents/supplychain/Final%20VC.pdf>

Further reading

- Cheh, M. M. (1982). Government control of private ideas – striking a balance between scientific freedom and national security. *Jurimetrics Journal*, 23(32), 16, note 106.
- Executive Order 11858 (1975). Foreign investment in the United States, 40 FR 20263, 3 CFR.
- Executive Order 12356 (1982). National security information, 47 FR 14874.
- Executive Order 14083 (2022). Ensuring robust consideration of evolving national security risks by the committee on foreign investment in the United States.
- FAQ (2023). FAQ Foreign Direct Investment Screening in France, Ministère de l'économie, des finances et de la relance.
- Intelligence Community Directive no. 204 (2021). National intelligence priorities framework, July 1.

- Intelligence Community Directive no. 211 (2022). Intelligence community support to the committee on foreign investment in the United States (CFIUS) threat analysis process, September 4. Available from: <https://irp.fas.org/dni/icd/icd-211.pdf>
- Regulation (EU) 2019/452 (2019). Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, *Official Journal of the European Union*, L1 79/1.
- The Authorization Act (2018). The authorization act for fiscal year 2019, title XVII, public law 115-232, 132 Stat. 1636.
- Exon–Florio Amendment (n.d.). The Exon–Florio amendment 50 United States Code, app 2170.
- The Export Administration Act of 1979 (1976). The 94th United States congress, public law 94-329, 90 Stat. 729.
- The Foreign (n.d.). The foreign investment risk review modernization act of 2018 In John, S. (Ed.), *Mccain National Defense*.
- The International Emergency Economic Powers Act (1977). The 95th United States congress, public law 95-223, 91 Stat. 1625.
- The United States Bill of Rights (1791). 1st United States congress, mainly J. Madison.

Corresponding author

Robert Lizak can be contacted at: robertpol25@wp.pl