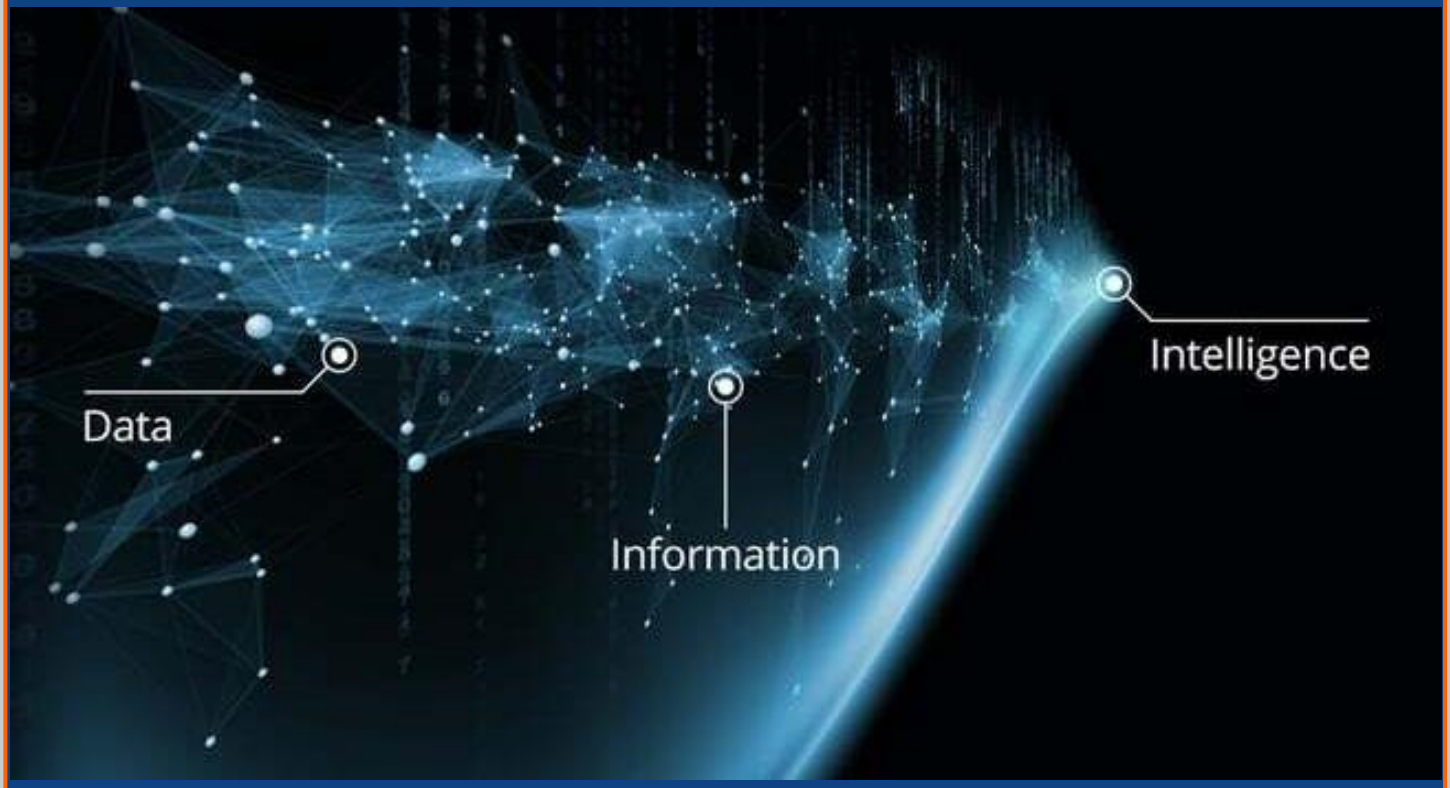
24
December
2024

O.S.S.I.S.Na.

Italian Observatory for the Security of the National Strategic Industrial System



Protection of the Defense industrial supply chain

Authors: DOMENICO PISCITELLI
DOMINIK KAMPMANN
DAVID SNEPP

CISINT
Centro Italiano di Strategia e Intelligence

MOODY'S

LIMITATION OF LIABILITY

www.cisint.org **ossisna@cisint.org**

INDEX

1. INTRODUCTON

In today's world, the defense sector has evolved into an extraordinarily complex and technologically sophisticated field. Modern threats extend beyond traditional warfare to include cyberattacks and many other forms of asymmetric conflict; a significant concern is the rise of disinformation campaigns, often fueled by Generative AI (GenAI). GenAI can automate the large-scale production of disinformation, enabling the rapid creation and distribution of vast amounts of false information. This can overwhelm fact-checkers and spread confusion. Additionally, GenAI can create bots and fake accounts to amplify disinformation by sharing and promoting it across social media platforms, giving the illusion of widespread consensus or popularity and further misleading the public.

The implications for Defense and Security are significant. The rapid spread of disinformation can undermine public trust in institutions, destabilize societies, and cause confusion during critical events, disrupt military operations, and erode the credibility of defense organizations.

1.1 Current and potential conflict zones: Ukraine, Middle East, Taiwan

The current and potential conflict zones are numerous and diverse, each highlighting the critical role of advanced technology in modern warfare and its broader impact on various sectors.

The war in Ukraine is highly relevant from a technological and industrial perspective due to its showcase of advanced warfare technologies like drones and cyber war operations, highlighting the critical role of cybersecurity. The conflict has disrupted global supply chains, particularly in the automotive, electronics, and energy sectors, leading to delays and increased costs. Additionally, as a key transit country for natural gas to Europe, Ukraine's instability has affected energy markets, prompting a search for alternative energy sources and investments in renewable energy.

In the Middle East, persistent tensions among regional actors continue to threaten global stability. The use of advanced surveillance systems, cyber warfare, and precision-guided munitions in these conflicts illustrates the growing reliance on technology to gain a tactical advantage. These developments have significant implications for the Defense industry and beyond, affecting supply chains, manufacturing processes, and innovation cycles in related sectors. In addition, resulting logistic challenges, including disrupted maritime trade in the Red Sea and use of the Suez Canal is forcing logistics companies to make use of alternative routes that circumnavigate the African continent. This results in increased costs and delivery times, significantly affecting the value chain. This is particularly relevant for the importation of high-tech goods (such as electronics and microchips) from production areas in the Far East, as well as petroleum products from the Arabian Peninsula and the Gulf countries.

Taiwan represents another potential flashpoint, and Western governments are concerned with China's increasing assertiveness in the region which may escalate the possibility of future conflicts. The strategic importance of Taiwan in global technology supply chains, particularly in semiconductor manufacturing, means that any conflict in this area could have far-reaching consequences for the global economy. The integration of advanced technologies in Defense strategies highlights the interconnectedness of military and civilian sectors, emphasizing the need for robust and resilient value chains.

Overall, these conflicts demonstrate that modern warfare is increasingly dependent on technological superiority. The ripple effects of this dependency extend beyond the battlefield, impacting the value chains of numerous other sectors, from manufacturing to information technology, and necessitating a comprehensive approach to national and global security.

1.2 The crucial role of industry in maintaining operational readiness

Industry plays a vital role in maintaining the operational readiness of military equipment. The ability to quickly produce, maintain, and upgrade military assets is essential to ensure that armed forces are prepared to face any threat. Public-private partnerships are fundamental in this context, as they enable the leveraging of expertise, innovation, and resources from the private sector to enhance the effectiveness of military operations.

These partnerships facilitate the rapid development and deployment of innovative technologies, ensuring that military equipment remains state-of-the-art. For instance, collaborations between Defense agencies and private tech companies have led to advancements in areas such as cybersecurity, artificial intelligence, and autonomous systems. By working together, public and private entities can accelerate the research and development process, bringing new capabilities to the field more quickly.

Moreover, public-private partnerships help in optimizing supply chains and logistics, ensuring that military forces have timely access to necessary equipment and spare parts. This collaboration is crucial for keeping the readiness and reliability of military assets, especially in times of crisis or conflict.

The integration of private sector efficiencies and innovations into military operations also drives cost-effectiveness. By adopting best practices from the commercial sector, Defense organizations can achieve better value for money, ensuring that taxpayer funds are used efficiently.

In addition, these partnerships foster a culture of continuous improvement and adaptability. The private sector's agility and responsiveness to market changes can help the military stay ahead of emerging threats and challenges. Regular interactions and joint initiatives between public and private entities create a dynamic environment where innovative ideas and solutions can be tested and implemented rapidly.

In this context, Moody's can be an important partner due to its ability to assist the Defense sector, particularly by providing them with specific tools to monitor and manage supply chain risks. Moody's experience in risk assessment and management can help ensure that supply chains remain resilient and secure, further enhancing the operational readiness of military force.

2. THE INITIATIVE WITH THE BRITISH GOVERNMENT: STRENGTHENING THE DEFENSE SUPPLY CHAIN PROTECTION

A fundamental pillar of the British government's strategy is becoming *"a centre of excellence for supply chain analysis and risk assessment "* and a priority in this path is to *"continue refining and expanding its capacity to predict and respond to external shocks on global supply chains."*[1].

2.1 Risk management-based methodologies and tools

Risk management is crucial for safeguarding Defense supply chains. Risk management-based methodologies and tools allow for the effective identification, assessment and mitigation of risks. These tools include data analysis, risk modeling and scenario simulation. Collaboration with strategic partners, such as Moody's, helps with the integration of risk data into multi-level supply chains, increasing their visibility and resilience. Moody's provides tools to government departments for identifying existing supply chain risks and assisting in making informed decisions regarding future strategies.

This helps departments to respond in an effective way to these potential disruptions. This is achieved through various risk objectives:

- Financial risk;
- Foreign interference risk;
- Reputational risk, such as sanctions or adverse media;
- ESG risk;
- Intellectual property transfer risk.

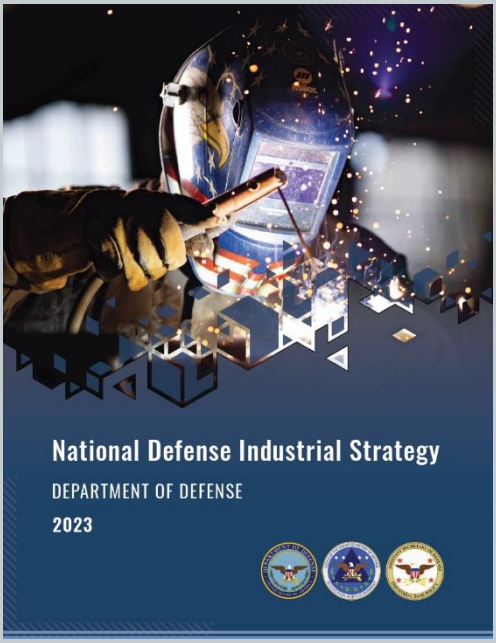
2.2 The importance of international collaboration in supply chain security

International collaboration is essential for supply chain security. Global threats require coordinated responses and information sharing among various actors. For example, the UK has developed the *Global Supply Chain Intelligence Programme* to improve global supply chain visibility and enhance resilience through strategic partnerships. Moody's is also well positioned to support this work through key strategic partnerships and the addition of our risk data to the multi-level supply chain. As recognized in the *Strategy for Critical*

1 Critical Imports and Supply Chains Strategy – UK Government – https://www.gov.uk/government/publications/uk-critical-imports-and-supply-chains-strategy

Imports and Supply Chains (January 2024), it is *"vital that the UK government and businesses continue to build... competence and expertise in supply chain analysis and risk assessment"*[2] and Moody's is proud to continue providing those tools to the British Government in this specific area.

3. THE U.S. DEFENSE INDUSTRIAL STRATEGY (NDIS 2023)



In January 2024, the Pentagon released the first of its kind National Defense Industrial Strategy (NDIS) – which is mainly designed to foster collaboration and partnerships with the private sector. According to the U.S. Department of Defense, this strategy will catalyze generational change from the existing Defense industrial base to a more robust, resilient, and dynamic modernized defense industrial ecosystem. Among other goals, the strategy encourages private enterprises to enter new markets, such as that of national security, while simultaneously strengthening the capabilities of the Defense sector.

Further, beyond identifying risks, the NDIS will develop public-private partnership solutions to help the United States keep pace with the increasingly complex and rapidly evolving global threat landscape. The strategy's core will guide U.S. engagement, policy development, and investment in the industrial base for the next five years. Building on the foundations laid by the National Defense Strategy, the NDIS aims to facilitate significant transformation from the current state of the Defense industrial base to a more advanced, resilient, and dynamic Defense industrial environment. *"The current and future strategic environment demands immediate, comprehensive, and decisive actions to strengthen and modernize our defense industrial base ecosystem, enabling it to operate with speed and scale for our warfighters"* said Deputy Secretary of Defense Kathleen Hicks during the strategy's release. *"The DoD's first National Defense Industrial Strategy will help ensure that we build the modern defense and innovation ecosystem necessary to defend America, our allies, partners, and our interests in the 21st century"*[3]. Fundamentally, the strategy links the nation's economy and its national security. It reinforces this balance and asserts that the U.S. military's strength is inextricably tied to the overall health, security, and stability of the country's industrial base. Its objective is to strengthen and maximize the capacity to produce with speed and scale to enable the armed forces to succeed in conflicts with peer adversaries worldwide. It enumerates potential threats, solutions, and specific outcomes in case of failure.

2 Ibidem
3 https://www.defense.gov/News/Releases/Release/Article/3643326/

Key pillars of the NDIS strategy include:

3.1 Supply chain resiliency

Recent global disruptions like the COVID-19 pandemic, geopolitical tensions such as Houthi drone attacks on shippings in the Red Sea, or minor events like the collapse of the Francis Scott Key Bridge in Baltimore have highlighted the vulnerability stemming from heavy reliance on foreign components and materials in the U.S. industrial base. The NDIS calls for diversification, enhancement of manufacturing capabilities, and implementation of stringent supply chain security measures. It includes investments in critical technologies and raw materials domestically and with trusted and selected international producers to shield the Defense industrial base from global shocks.

3.2 Workforce development

The core of the NDIS recognizes that technological superiority depends on the skills and ingenuity of the workforce. To keep pace with technological changes, a skilled workforce is required not only in current technologies but also adaptable to future advanced innovations. To achieve this, the strategy promotes comprehensive education and training programs, industry-academic partnerships, and incentives to attract and retain talent in critical STEM fields for Defense.

3.3 Rapid innovation and acquisition

Acknowledging significant gaps between the development of critical technology and its implementation through a labyrinthine federal procurement process, the strategy calls for speed in the acquisition process. Through streamlined regulations and requirements, the NDIS promotes agile procurement processes, public-private partnerships, and regulatory reforms to accelerate the timeline from research and development to operational use. This approach not only supports faster integration of cutting-edge technologies but also stimulates the innovation ecosystem, encouraging both startups and traditional companies to contribute to Defense capabilities.

3.4 Economic deterrence and international cooperation

Finally, the NDIS emphasizes the interconnection between security and the global economy, leveraging economic strength and international alliances to deter adversaries and competitors. Economic sanctions, export controls, and investment screening are tools to protect technological advancements and counter espionage. Similarly, the strategy calls for enhanced cooperation with allies and partners to ensure a unified front in confronting security threats, sharing the defense burden, and promoting global peace and stability. Through this strategy and its implementation, the Pentagon is embracing a "*public-private partnership*" like never before in history. Through a comprehensive framework aimed at ensuring that the United States and its allies not only defend but anticipate risks from competitors and adversaries.

4. MOODY'S APPROACH TO EXPONENTIAL RISK

In the era of polycrisis, the interconnection of risks poses challenges to national security agencies and businesses worldwide, requiring them to implement effective risk management based on reliable data and analysis. The Public Health Emergency of COVID-19 in 2020, Russia's invasion of Ukraine in February 2022, Houthi attacks on marine vessels in the Red Sea, Hamas' attack on Israel in October 2023, and widespread IT disruptions due to CrowdStrike's upgrade in July 2024 have created a series of cascading risks and effects that national security agencies and businesses have had to address.

> *"It is clear: we are now living in a new era. The Era of Risk^N - Exponential Risk".*
> (Rob Fauber, Moody's President & CEO)

This new era means that the old way of managing risks – as isolated and siloed events – is no longer sufficient. Moody's brings structure to a world of unstructured data, curating and standardizing data on key risk types that could threaten the National Security.

4.1 360° Risk assessment: financial, environmental, reputational, cyber, technological risks

Moody's offers a 360° risk assessment framework that covers multiple dimensions of risk across various sectors and domains. This framework leverages Moody's extensive data assets, innovative analytical models, and sector-specific experience to provide government clients with insights on the sources, drivers, and potential impacts of diverse types of risk. The framework includes the following components:

- **Risk assessment process**
  Mapping key risks by their probable impact is crucial. Moody's solution delineates a risk tolerance line that helps differentiate between risks that require mitigation and those that can be accepted. It is appropriate to have a menu of mitigation strategies tailored to the risk level of suppliers and resources in general.

- **Financial risk**
  A supplier's financial instability is the most reliable predictor of performance risk. Moody's provides public and private sector customers with credit and market risk solutions that help them assess the financial health and stability of entities and market, identify potential vulnerabilities and contagion effects, and respond to financial shocks and crisis.

- **Ultimate ownership & control**
  Understanding the ultimate owners of key suppliers, service providers, and consultants is vital, given their considerable influence on the Defense field and access to strategic assets. Moody's provides comprehensive risk intelligence solutions, offering legal entity, ownership, and control data crucial for thorough third-party and supplier due diligence. Moody's delivers curated intelligence on sanctions, enforcement actions, political exposure, state ownership, and adverse media, helping clients to mitigate compliance risks effectively. Additionally, Moody's provides robust software tools for onboarding, risk assessment, and ongoing management, helping with a seamless end-to-end compliance in an ever-evolving regulatory landscape

- **Reputational risk**
  Reputational risk can threaten every organization's standing through associations with suppliers. Moody's provides comprehensive risk intelligence, encompassing sanctions, enforcement, political exposure, state ownership, and adverse media. Its robust onboarding, risk assessment, and in-life management software assists with end-to-end compliance. It analyzes and identifies reputational risks by monitoring supplier developments and flagging significant concerns. Additionally, Moody's provides tools to help the understanding of supply chain networks, including third-party, fourth-party, and subsequent suppliers that may pose potential reputational harm.

- **Geopolitical risk**
  Geopolitical events can limit supplies, increase supply chain costs, and drive up global and regional prices. Moody's provides risk assessments for 188 countries, with the ability to assign the weight or importance of each and integrate them into the suppliers' overall risk score.

- **Natural disaster risk**
  Natural disasters can significantly disrupt supplier business activities through employee evacuations and/or damage to facilities and infrastructure. Moody's provides tools to help to predict the risk of natural disasters in locations significant to suppliers, helping determine which suppliers may require mitigation steps based on natural disaster risk levels. Moody's assists in identifying and diversifying the supplier base by finding alternative suppliers in different regions or countries, reducing the impact of potential disruptions from natural disasters.

- **Cyber risk**
  Cyber supply chain risks involve the loss of company data by suppliers, breaches of company systems by hackers through supplier access, and suppliers going offline due to ransomware attacks. Moody's provides cyber risk ratings that assess the probability of a company experiencing a cyber incident, exposing cyber risk within an organization's third and fourth-party supply chain ecosystems.

- **Operational risk**
  Operational risks can undermine the resiliency of supply chains, disrupt operations or processes, and affect the quality, production, and delivery of products and services. Moody's can help uncover operational risks by identifying significant financial risk trends likely to deteriorate supplier performance and highlight extended supply chains (multi-tiered suppliers, facility locations) for various products. This helps quantifying the resiliency risk on the supply chain, assisting customers in planning mitigations for operational risks.

CONCLUSIONS

The defense landscape in the era of advanced technology is characterized by increasing complexity and threats that go beyond traditional conflicts, including cyberattacks and disinformation. The ability to quickly produce, maintain, and update military equipment is essential to ensure the operational readiness of the armed forces. Public-private partnerships are fundamental in this context, allowing the expertise and resources of the private sector to be leveraged to improve the effectiveness of military operations. The National Defense Industrial Strategy (NDIS) 2023[4] emphasizes the need for a robust and resilient Defense industrial base to address these challenges.

Furthermore, international collaboration is crucial for the security of supply chains. Global threats require coordinated responses and information sharing among various actors. Programs like the UK's *Global Supply Chain Intelligence Programme* aim to enhance the visibility of global supply chains and strengthen resilience through strategic partnerships.

Moody's, with its experience in risk assessment and supply chain intelligence, is well-positioned to assist with these efforts by providing valuable insights and data to help mitigate risks and the stability of supply chains.

4 The National Defense Industrial Strategy (NDIS) - U.S. Department of Defence

BIBLIOGRAPHICAL REFERENCES

National Defense Industrial Strategy - U.S. Department of Defense - 2023

National Defense Strategy - U.S. Department of Defense - 2022

Critical Imports and Supply Chains Strategy - UK Government - 2024

C. Todaro/V. Iavarone - Sicurezza economica e conflitti internazionali: nuovi scenari di minaccia per il Sistema Industriale Strategico - CISINT/OSSISNa - 2024

Web site: https://www.moodys.com/

AUTHORS:

Domenico Piscitelli
Director, Government & National Security, Europe & Africa
Moody's

Dominik Kampmann
Director, Government & National Security, Europe & Africa
Moody's

David Snepp
Sr. Director, Government & National Security, North America
Moody's

O.S.S.I.S.Na.

The Italian Observatory for the Security of the National Strategic Industrial System (**O.S.S.I.S.Na.**), established within CISINT – Centro Italiano di Strategia e Intelligence, is a project oriented toward the indepth study of issues concerning the security of national strategic industrial assets (companies and supply chains), which are fundamental to the Nation and social welfare.

The Observatory consists of national-level experts from the institutional, industrial and academic fields with the shared aim of focusing on the study of the following macro-areas: Methods & Best Practice, Technology, Regulatory and Geopolitics.

This initiative is aimed at promoting educational (in the academic, institutional and business areas) and dissemination paths (through seminars, webinars and contributions in the national mass-media) to raise awareness of issues related to the protection of the National Strategic Industrial System, while also developing its own proposal capacity for institutional decision-makers.

C I S I N T
Centro Italiano di Strategia e Intelligence

Viale delle Milizie 34, 00192 - Roma
E-mail: info@cisint.org
www.cisint.org