The Algorithmic Sanction: Countering Artificial Intelligence (AI) Driven Economic Warfare

Key Takeaways for Policymakers

- **The Problem:** Artificial Intelligence (AI) poses a two-fold threat, allowing adversaries to possibly execute strategic economic sanctions, as well as evade ones imposed by India and its allies, thus posing the risk of making conventional defences irrelevant.
- **The Core Argument:** To counter this new threat, India needs its own sovereign, artificial, geo-economic intelligence system driven by artificial intelligence to protect its economic security and strategic independence.
- **Key Recommendation:** A public-private sandbox should be established in form of a National Geo-Economic Intelligence Centre (NGEIC) to develop indigenous tools, human capital, and international relationships.

Executive Summary

Economic interdependence has become a hallmark of modern geopolitics. This interdependence is now being weaponised by adversaries and this trend is evolving with the emergence of AI (Farrell and Newman 2019, p. 45). The risk of algorithmic sanctions, the application of AI to carry out hyper-precise offensive sanctions represents a qualitative breakthrough in the speed, scale, and precision of economic warfare (Tashji 2025). This policy brief argues that AI poses a two-sided threat to the economic security of India, as it gives both hostile actors the ability to impose hyper-precise offensive sanctions at a previously unimaginable rate and precision, and it provides sanctioned actors with the ability to engage in highly sophisticated, AI-driven evasion that breaks through the established compliance regimes. To counter this emerging threat, India faces an urgent requirement to build a sovereign, AI-enabled geo-economic intelligence capacity under purview of a new National Geo-Economic Intelligence Centre, a national mission of developing indigenous analytical engines, a programme of nurturing requisite human capital, and an outreach to shape international norms through diplomacy.

Introduction

The interdependence that used to be considered a stabilising element in the framework of benign globalisation has been replaced by the era of sharp geopolitical rivalry, whereby economic interdependence is no longer a stabilising factor but a source of weaponisation (Farrell and Newman 2019, p. 45). The current state of affairs is a U.SChina competition that no longer relies just on the presence of traditional armies, but rather is based on the systematic coercion of the global supply chains, financial networks, and technology ecosystems (Brown, Chewning, and Singh 2020, p. 1). This trade weaponisation has become a fundamental part of Chinese foreign policy towards its trading partners (Cha 2023, p. 1).

Since the embargo of major minerals like gallium and germanium, China has targeted individual companies to achieve political motivations; the idea of economic statecraft has become a fast-tracked tool of national power (Reuters 2023). India's External Affairs Minister noted that it is impossible to discuss foreign policy today without referring to 'de-globalisation, supply chain resilience, critical minerals, digital transformation, and Artificial Intelligence (AI)' (Bhatia 2024). While the principles of economic statecraft are not novel, the speed and scale with which AI can operate threaten to outclass traditional resilience approaches, which were created for a slower, less data-intensive era of competition (Solow-Niederman 2020, p. 653). This technological change highlights the immediate necessity of creating a sovereign, AI-based geo-economic intelligence facility.

The Dual Nature of AI in Economic Statecraft

The strategic implementation of AI is a symmetric problem, and it may dramatically increase the effects of sanctions and the ability to avoid them. This creates an "offencedefence battle" analogous to the one emerging in online crime, where AI is used by both criminals to perpetrate attacks and by law enforcement to counter them (Burton et al. 2025, p. 25).

Artificial Intelligence as an Offensive Technology allows states to go beyond blunt-force sectoral sanctions and make surgical strikes on the economy of an adversary (Tashji 2025). This strategy is analogous to sophisticated supply-chain analytics, where nodes are organisations, banks, or production facilities, and the edges are logistical or financial interrelations between them (Wasi et al. 2024, p. 11). There is however an important difference between a domestic economy and the economy of an adversary. A country's own economic network is a system of complete information. The problem of modelling the economy of an adversary, in its turn, is incomplete and asymmetric information, where an intelligence agency would have to infer the macro-structure based on a small and frequently noisy set of observations (Chaudhuri et al. 2024; Jackson and Pernoud 2021, p. 171) (equivalently, estimating the structure of a system based on its outputs a task that is always more difficult than describing an observed system). An intelligence agency can begin to predict the nature of these hidden dependencies using techniques such as Graph Neural Networks (GNNs) (Kosasih and Brintrup 2022, p. 5381). It is not aimed at generating a perfect “digital twin but a probabilistic (or fuzzy) network model where every economic link has a probability of existence based on the available intelligence (Raimondo and De Domenico 2021), and where critical but possibly nonobvious vulnerabilities (i.e., high-probability single-point failures that can trigger cascading failures to a strategic industry) can be detected (Huang et al. 2013, p. 1). This kind of network analysis is also supported by the ability of AI to absorb masses of nontraditional data in real-time (Clayton et al. 2025, p. 2). It has been shown that GNN based methods always achieve higher accuracy by 15-40 percent over traditional techniques in detecting anomalies, thus facilitating the prompt detection of suspicious activities (Wasi et al. 2024, p. 29).

AI as a Defence Mechanism, simultaneously the adversaries are using AI to fight them (Tashji 2025). State-sponsored vessel identity laundering and geospoofing systems employ generative AI to produce forged paperwork and synthetic identities on an unprecedented scale. These systems generate so much fake data that they overwhelm human-based monitoring systems. (United Nations Security Council 2024, p. 23). Academic literature already shows that it is feasible to develop AI-driven countermeasures, using deep learning to automatically detect suspicious vessel trajectories as indicators of a deception attempt using real-time tracking data (Maganaris et al. 2024). The challenge is no longer theoretical; recent academic research has shown that it is possible to produce benchmark datasets of over 800,000 synthetically generated identification documents explicitly for training defensive AI models (Guan et al. 2024). This capability contributes to threats creating more than $212 billion in suspicious activity in the US financial system in 2021, rendering manual, checklist-style compliance increasingly ineffective (Financial Crimes Enforcement Network (FinCEN) 2024). This concern is corroborated by broader financial industry evaluations, which identify the use of AI for document manipulation and social engineering as a substantial and growing threat (US Department of the Treasury 2024, p. 27). Identifying and associating synthetic identities to sanctioned entities is a critical task for which advanced, universal entity-resolution models are currently being developed. (Wang et al. 2024).

Guiding Framework

The creation of sovereign artificial-intelligence instruments is a requisite, but not a sufficient step. Such capabilities without a governing system create high risks (NIST 2023, p. 6). An initial framework is required to govern the application of these tools, the level of what may be regarded as an economic attack, and a framework of responding proportionately and strategically in the geo-economic domain. This framework is not just a technical guide; it is a strategic imperative that helps policymakers navigate the emergent digital fog of warfare that these algorithmic sanctions will produce. This phenomenon is analogous to the "algorithmic fog of war" in military contexts, where advanced AI, rather than providing perfect clarity, introduces new layers of complexity, uncertainty, and potential for error (Huelss 2025, p. 3). As Johnson put it, 'the AI age brings new possibilities for the unintended escalation by placing extreme cognitive burdens on the decision makers under time pressure' (Johnson 2022, p. 337). A strategic Indian framework is thus needed to manoeuvre through this uncertainty such that a strictly economically coercive act is not interpreted to be the start of a military confrontation (Jensen, Lin, and Ramos 2022). Notably, it should also institute strong ethical guardrails to govern data, define clear guidelines on how anonymized data of the private sector is used in the NGEIC, and that all automated analysis tools undergo intensive bias audits and human oversight to maintain public trust and democratic responsibility.

Principles for Human-AI Teaming

The creation of a sovereign AI capability is not enough; the success will be fully dependent on the efficiency of the human-machine team. Improperly implemented automation may trigger disastrous failures, such as skill atrophy, automation bias, and the poor understanding of the system's functioning**.** (National Academies of Sciences, Engineering, and Medicine 2021, pp. 9, 81). A strategic model should, thus, include clear guidelines on how to design the analyst-AI interface, the so-called analyst cockpit, and the cognitive processes that ensure that the human operator is the decisive element. The major tenets involve designing it in a transparent, explainable way (Patel et al. 2024), training analysts to anticipate AI failure modes (Warren et al. 2025, p. v), and workflow development to actively prevent both skill atrophy (Warren et al. 2025, p. vii) and cognitive bias (Stebbins et al. 2024, p. v).

Policy Recommendations

In order to overcome this challenge, India needs to take an agile adopter approach to AI to achieve economic security, as the Special Competitive Studies Project in the United States has promoted (Special Competitive Studies Project 2024, p. 18). It includes the shift of the traditional procurement model to the quick, iterative development strategy in the close collaboration with the private sector. India's response should be as sophisticated as the threat and be informed by an effective national strategy. The recommendations are aimed at developing this capability:

1. **Establish a National Geo-Economic Intelligence Centre (NGEIC) as a Public-Private Sandbox.** The major challenge faced to formulate a national geo-economic intelligence picture is that critical data are housed with the private sector. Legal liabilities and business sensibilities make companies unwilling to share such information (Nweke and Wolthusen 2020, p. 73). To overcome this, the NGEIC is to be designed as a public-private partnership that is established under a legal safe harbour. This framework would offer protection against liability to participating companies, which is based on other frameworks like the U.S. Cybersecurity Information Sharing Act (CISA) (Nweke and Wolthusen 2020, p. 73). The NGEIC would become a regulatory sandbox of geo-economic data, a successful precedent of innovation in data governance (Datasphere Initiative 2022, p. 20) and financial security (Financial Action Task Force (FATF) 2021, p. 30), which would offer a controlled setting in which private businesses would share anonymized data with government analysts to map aggregate offensive vulnerabilities and create defensive evasion countermeasures. This model is also in line with policy suggestions on how to deal with AI risks in other vital industries where a collective effort is considered necessary to share best practises and work on data standards (U.S. Department of the Treasury 2024, pp. 12, 34). The model directly compares with the recent suggestions of a non-profit public-private partnership to utilise open-source

data and technology to the benefit of the U.S. intelligence community (Special Competitive Studies Project 2024, pp. 40-41).

2. **Introduce an 'AI for Trade Resilience' National Mission.** The development of this sovereign capability is eminently feasible. India has an opportunity to leverage its world class digital public infrastructure, which was listed by the Financial Action Task Force as one of the most effective in the world (Financial Action Task Force (FATF) 2021, p. 30). The national mission must initiate the creation of indigenous AI and GNN-based tools to work in both predictive economic intelligence and defensive compliance monitoring. Current academic frameworks have already shown that it is possible to use large language models to autogenerate such knowledge graphs out of public data sources (AlMahri, Xu, and Brintrup 2024), use the resulting graphs to analyse predictive resilience (Karam et al. 2022, p. 117), and generate large-scale, privacy-preserving synthetics datasets required to train defensive compliance tools (Guan et al. 2024), providing a strong demonstration of the viability of this mission. This mission may begin with a pilot project that aims at securing India critical pharmaceutical supply chains. Drawing upon the previous methods of fraud detection, the pilot would create a supplier-customer knowledge graph to detect and mark suspicious transactions as signs of sanctions-evasion or intellectual-property theft, prototyping the defensive tools that will be validated within the NGEIC's data sandbox. (Xie et al. 2024, p. 2055).

3. **Build a Cadre of Geo-Economic Intelligence Analysts.** The development of tools is not enough without human capital to implement them effectively. The National Mission should thus incorporate a specialised curriculum to educate a new generation of analysts. Training based on the principles of human-AI teaming set out by the National Academies of Sciences must involve teaching to build accurate mental models of AI systems, training analysts to anticipate failure modes, to identify and mitigate automation bias, and emphasising stress-testing the tools they create against edge cases and off-normal conditions (National Academies of Sciences 2021, pp. 9, 81).

4. **Start a 'Quad Working Group on Algorithmic Economic Security.** India should propose a Quad Working Group to address this common threat but must do so with a realistic understanding of the members' divergent strategic interests. The project ought to first focus on a more foundational and less contentious goal: developing shared threat assessments and a common lexicon for AI-driven economic coercion. This practise is consistent with strategic proposals advocating for “collective resilience”, where like-minded allies form coalitions in order to deter economic coercion through credible, unified action (Cha 2023, p. 4). The long-term aim would be to explore models of defensive intelligence sharing and collective resilience, but this would have to be done with the express understanding that varying economic relationships with prospective

adversaries, and national policies regarding offensive capabilities, would require delicate and continuous diplomatic manoeuvring.

Confronting Core Implementation Challenges

The success of the NGEIC relies on overcoming a wave of political, business, technical, and strategic hurdles that go far beyond the initial setup. These challenges should be approached with advanced, realistic solutions from the outset.

1. **The Political Challenge: Overcoming Bureaucratic Resistance.** The Ministries of Finance, Commerce, and External Affairs will instinctively be averse to give up control over economic intelligence to a new NSCS-led body (Sinha 2018, p. 136). This resistance may take the form of passive resistance: a slow rate of sharing data, providing incomplete data, and starving the NGEIC of its best personnel**.** NGEIC. To address this, the NGEIC needs not just a high-level mandate, but it needs to be embedded within the fabric of ministerial self-interest. Its charter should provide it with the mandate to not just request but also task ministries to provide certain data streams necessary to national security evaluations, and that compliance will be reported to the Cabinet Committee on Security. The huband-spoke model should be empowered and embedded NGEIC analysts should co-author intelligence products that explicitly serve the host ministry agenda, thus making sure that ministries see the Centre as a force multiplier, and not as a competitor. Despite these efforts, this will be an ongoing political battle that requires high-level intervention to defeat institutional fortifications.

2. **The Commercial Challenge: The Private Sector Incentive Gap.** In the case of major companies, commercial and reputational risks of disclosing crown jewels of data to a state security project will probably exceed the advantages of generic government intelligence reports (Routh et al. 2025). The incentive model should be much more concrete. A coercive model, which associates participation with strategic government programmes like PLI schemes, would attract intense industry opposition and would most probably lead to malicious compliance, i.e. the submission of low-quality data in minimum quantities to meet a requirement. To overcome the private sector's reluctance to share sensitive data, government proposals often rely on providing concrete incentives, such as liability protection and relief from regulatory enforcement (Bejtlich 2015). The initial area of emphasis should be providing concrete custom intelligence products to a limited set of trusted private-sector partners, so as to demonstrate the value of the model and then seek wider inclusion. This redefines the incentive not as a vague promise of insight, but as a tangible

impact on access to markets and revenue, though doing so will be a huge political undertaking that requires long-term determination.

3. **The Technical Challenge:** The necessity to have granular, entity-specific data to determine vulnerabilities clashes with the legal requirement to anonymise data (Cairo 2023, p. 94). To address this, the NGEIC should implement a data-neverleaves architecture on its most sensitive private-sector collaborations, using privacy-enhancing solutions, including federated learning and confidential computing (The Royal Society 2023, p. 34). Instead of pulling raw data to a central repository, the NGEIC would actually train its analytical models within a partner firm's own environment. The Centre would only receive anonymised, aggregated insights and model updates, allowing potent analysis, and the firm to retain control over raw data. While this is the correct theoretical architecture, its practical implementation represents a monumental, multi-year national standardization effort across diverse and competing private sector IT systems, and must be treated as a core, long-term R&D challenge in itself.

4. **The Human Capital Challenge:** The NGEIC cannot compete with the private sector in terms of elite AI and data science talent salaries (Zugravu et al. 2024). The value offer should be unique, focusing on mission, access, and prestige. The NGEIC should be formed as a flagship institution for a "tour of duty," with a formal fellowship program that allows top private sector talent to serve for 2-3 years on specific national security concerns with unequalled data access before returning to respective industry. This creates a strong patriotic motivation and a long-term public-private alumni network. Although maintaining a full cadre on this model alone is optimistic, this model cannot be the only solution; rather, it must be viewed as an essential aspect of a hybrid talent strategy, supplemented by a strong internal training pipeline to create career analysts.

5. **The Strategic Challenge I: The Risk of Internal Misuse.** An effective instrument to visualise external risks can be redirected to domestic issues, posing a significant threat of political abuse or crony industrial policy. In a deeper sense, it creates a potent tool of state monitoring of the economy that has far-reaching effects on civil liberties. To address this, the governance structure of the NGEIC should be strengthened by an independent external oversight body that is permanent. This body, composed of respected jurists, technologists, and civil society leaders, should be a congressionally mandated body, with the power to audit the NGEIC in terms of its operations, and obliged to present its findings directly to a parliamentary committee, thus providing a strong degree of democratic accountability. Most importantly, the charter that establishes the NGEIC should include legally binding prohibitions, enforced by this body, against its use for monitoring domestic political dissent, or to analyse data on the basis of protected characteristics like religion or

political affiliation. Its empowerment and independence must be protected by statute to the greatest extent possible**,** recognising that its authority will always be the subject of recurrent political battles, and that it will need to be defended against defunding or capture over time.

6. **The Strategic Challenge II: The Dependency Paradox.** In the pursuit of such sovereign capability, a foreign-controlled technological stack (e.g. GPUs, cloud platforms) is substantially involved. This forms a vulnerability in the depths. The charter of the NGEIC should recognise this dependency and mandate a threepronged approach to mitigation: (1) intensive, continuous supply-chain security audits of all hardware and software; (2) a policy of radical transparency, favouring open-source tools to minimise black-box risks; and (3) an explicit role in ensuring the provision of analytical support to a long-term national mission to develop indigenous capability in such core technologies.
7. **The Data Access Challenge: The Walled Gardens.** Foreign-domiciled technology and financial platforms often have a strong incentive to withhold the most valuable geo-economic data. The main approach of the NGEIC should not be based on compulsion, as it is often not possible to gain direct access. It has to be preoccupied with the art of over-the-horizon analysis: learning how to infer activity in such walled gardens by examining second- and third-order information that is publicly available or otherwise accessible, not relying on the availability of the underlying data itself (Tecuci and Marcu 2021, p. 1.)
8. **The Economic Equity Challenge: Shielding Small and Medium Enterprises (SMEs).** The NGEIC is designed to accommodate complex data sharing and analysis, and this design is inherently biassed towards large corporations. This poses a huge risk of unintentionally introducing compliance or data-sharing overheads that SMEs cannot sustain, which may result in their marginalisation from strategic supply chains and consolidating the market in favour of large incumbents. To avoid this, the NGEIC should have a specific mandate to enable, rather than overburden, the SME sector. This involves the creation of a special SME interface, probably by industry associations, to concentrate on value delivery. The NGEIC should not be demanding data but must distribute anonymised sector-specific threat intelligence and resilience best practises to enable SMEs to safeguard the backbone of the economy against the very threats that the Centre is intended to counter.

Governance and Oversight: Insulating Capability from Political Capture

Beyond technical challenges, the greatest risk to the efficiency of the National Government Enterprise Intelligence Centre (NGEIC) might be internal: bureaucratic competition and political corruption. Such a tool is bound to be the centre of rivalry between ministries (Finance, External Affairs, Commerce) and security agencies. It is not the sophistication of its algorithms but rather a governance system that withstands these pressures while ensuring its outputs serve the national interest.

In order to accomplish this, the NGEIC must be formed under the direct purview of the National Security Advisor (NSA) and the National Security Council Secretariat (NSCS). This would position it as a truly cross-governmental asset, charged with the integration of the contributions of all concerned ministries instead of furthering the interests of one (IDSA Task Force 2012, p. 8). It should be governed by an oversight board, which should be chaired by the NSA, and with representation at the secretary level from the Ministries of Finance, Commerce, External Affairs, and Defence. This organisation would promote buy-in, reduce inter-agency tension, and make the analytical priorities of the NGEIC reflective of the overall strategic goals of India, as opposed to the parochial interests of one department (Munsing and Lamb 2011, p. 3).

One crucial role of this oversight board will be to manage the danger of defensive selfharm, the risk that the process of mitigating a vulnerability could cause more harm to the national economy than the potential damage from threat itself. To this end, the mandate of the NGEIC cannot be narrowed down to the vulnerability identification; a stringent cost-benefit analysis of any suggested mitigation must also be carried out. Every vulnerability report should be provided with an "Economic Resilience Impact Assessment" modelling possible costs, market impacts, and competitiveness impacts of any proposed policy measure. The oversight board will then turn into the essential forum in which the security imperatives stipulated by the NSCS will be weighed against the economic impacts advocated by the Ministries of Finance and Commerce. This will make the resilience strategy of India economically sustainable and does not inadvertently cause more harm than the threats it aims to mitigate.

However**,** such a centralised model should be complemented with a hub-and-spoke operation design to pre-empt bureaucratic resistance**.** While the NGEIC will serve as the central analytical hub, it must incorporate small, dedicated spoke units of its own analysts within the key partner ministries. The purpose of such embedded units is twofold: initially, to serve as trusted liaisons enabling the flow of high-quality data between the ministry and the hub; and second, to transform the intelligence of the NGEIC at the national level into action-oriented and specific insights that directly apply to the particular mission of the host ministry. This model makes ministries not merely data providers but active partners and direct beneficiaries of the intelligence, which forms a strong incentive to fully and enthusiastically cooperate and make the outputs of NGEIC highly integrated into the machine of economic and foreign policy of the government.

Risk Mitigation for the NGEIC

The development of a sovereign AI capability like the NGEIC automatically establishes it as a high-value target to adversaries. The defensive infrastructure is exposed to advanced second order attacks aimed at compromising its credibility. Such risks are data poisoning, where an attacker corrupts input data to deceive the Knowledge Graph; model evasion, where malicious actors design transactions to be misclassified by the defensive AI; and direct cyberattacks on the NGEIC's internal infrastructure (Vassilev et al. 2025, pp. 24, 32). The NGEIC should also be based foundation of robust AI security to be resilient. This involves the adoption of a zero-trust data architecture that constantly verifies the integrity of data entering the system. The analytical models should undergo a consistent algorithmic red teaming, which means that an internal team is actively trying to mislead AI to identify vulnerabilities proactively. Lastly, the centre needs to develop clear protocols that need to be followed by the analysts when the results of the AI is flagged as being low-confidence or possibly compromised and to ensure the human operator is trained to detect and override a manipulated system.

Conclusion

The introduction of algorithmic sanctions represents a qualitative change in the grammar of statecraft, moving from the analogue age of sectoral sanctions of broad scope to the digital age of hyper-precise network centric economic warfare. While the nature of this competition is an evolution of past practices, the overwhelming speed and complexity requires an equally evolved response, not an incremental one, and moving the centre of the geopolitical competition from the battlefield to the global economic network (Babić, Dixon, and Liu 2022, p. 2). Inaction is an option in this new space, which cedes decision advantage to adversaries and risks reducing India to the role of being a passive consumer of the security technologies from abroad and be vulnerable to coercion it cannot predict or defend against (Sanbad 2024, p. 151). The suggestions outlined in this brief are the first steps towards building this sovereign capability, representing an act of strategic self-determination in the digital era. This move will not only ensure the economic strength of India but also its ability to be an independent and influential player in the twenty first century.

A Note on Technical Complexity and Resource Implications

These suggestions are an important and requisite strategic investment. The development of sovereign geo-economic intelligence capacity is a multi-faceted, multiphase and continuous process. According to best practises, building a domain-specific Knowledge Graph (KG) requires a persistent KG construction pipeline, which incorporates variety of resource-intensive stages such as heterogeneous data acquisition, knowledge extraction, entity resolution, dynamic updates, quality assurance and development of predictive analytic models (Nweke and Wolthusen 2020, p. 73). More importantly, this technical challenge is not a static one. An intelligent adversary, aware of being monitored will actively adapt its economic networks, developing shell companies, diverting money trails, and corrupting data to evade detection. This triggers a continuous "adversarial arms race.". Thus, the Knowledge Graph cannot be perceived by the NGEIC as a one time construction project. It has to be viewed as a living, evolving system, which needs continuous, almost real-time updates and constant retraining of the model just to keep up with the adversarial adaptation (Nweke and Wolthusen 2020, p. 73). This inherently makes it a persistent, resource-intensive effort, necessitating a permanent investment in both talent and computing dedicated to stay ahead of the adversarial adaptation. While a precise budget requires more study, any cost evaluation must understand that the NGEIC is a continuous, operational intelligence organization rather than a time-bound R&D effort. The sustained operational expenditures (OPEX) would be the investments in high-end talent and dedicated computational resources. This level of investment is commensurate with the goal of building and sustaining a durable decision advantage in a contested global economic environment.

Technical Appendix: The System Architecture and Methodology of the National Geo-Economic Intelligence Centre (NGEIC).

1. Algorithmic Foundations

The fundamental analysis engine of the NGEIC is based on the modeling of economic networks as probabilistic graphs when faced with uncertainty. This strategy is needed since intelligence about economies of an adversary is always incomplete and noisy.

1.1 Graph Neural Networks (GNNs) to Vulnerability Analysis: We suggest applying Graph Neural Networks in order to derive macro-structure of economic networks. GNNs are particularly well suited to handle this type of work because they directly work with graph-structured data, learning representation of nodes (i.e. companies, banks) based on their local neighborhood. For vulnerability analysis, the primary tasks are:

Link Prediction: Predicting concealed or likely logistical and financial dependencies between entities. This plays a crucial role in revealing non-obvious supply chains that may be attacked, which has been empirically proven to using GNNs on actual automotive supply networks (Kosasih and Brintrup 2022).

Node Classification: The identification of critical nodes is through the classification of the nodes in terms of systemic risk i.e. their potential to cause a cascading failure to spread the risk across the network in case they default (Huang et al. 2013).

1.2 Integrated Defensive Signal Generation: The defensive posture needs a set of AI models, which serve as signal generators, offering rich features to the core GNN. Instead of being separate tools, their results are fed as attributes into the economic knowledge graph. This includes:

Detecting anomalies in time-series data: Deep learning models (e.g., RNNs, Transformers) are trained on real-time tracking data (e.g., maritime AIS) to produce anomaly scores on vessels or shipments, which are then added as risk attributes to the respective nodes or edges on the graph (Maganaris et al. 2024).

Synthetic Identity and Document Analysis: The system is conditioned on large-scale, synthetically generated sets of identity documents to develop powerful classifiers that can be used to identify forgeries and other types of document frauds. Each time when a new document or identity is processed, the confidence score of the model (i.e., the likelihood that it is a forgery) is added as a feature to the corresponding entity in the graph (Guan et al. 2024).

2. System Architecture and Data Governance

The technical architecture of the NGEIC will resolve the main dilemma of having granular and entity-specific data and the legal/commercial need to have data privacy and anonymization.

2.1 "Data-Never-Leaves" Architecture: NGEIC will not run on a central repository of sensitive information of the private-sector. Instead, it will apply a data-never-leaves design with Privacy-Enhancing Technologies (PETs).

Federated Learning (FL): The training of the analytical models occurs locally in the secure environment of partner firms. The updates to the model parameters are only sent to the NGEIC central hub anonymized and encrypted and are aggregated into a global model there. This means that raw proprietary data never leaves the owner's control.

Confidential Computing: Where feasible, computations will be performed in secure enclaves, where the computations will offer cryptographic assurances that the data under processing is inaccessible to the cloud provider or system administrator.

2.2 Knowledge Graph Construction Pipeline: This system involves a pipeline that is continuously resource-intensive and strives to maintain an evolving model of the global economic network. This is the technical response to the continuing "incessant arms competition" that is outlined in the brief. It includes:

Heterogeneous Data Acquisition: The ingestion of structured, unstructured data supplied by open-source and partners.

Knowledge Extraction: Parsing unstructured text through Large Language Models (LLMs) and extracting entities and relationships between them.

Entity Resolution: Resolving and linking entities in different data sources to create a consistent knowledge graph.

Dynamic Updates and Quality Assurance: It is necessary to continuously update the graph with new information and conduct validation tests to guarantee data integrity.

2.3 Algorithmic Red Teaming: To achieve resilience to adversarial attacks, the NGEIC will have an internal red team. The mandate of this team is to develop and actively attack the analytical models by corrupting the input data through data poisoning (corrupting input data) and by attacking the model through model evasion (designing transactions to be misclassified). Such an offensive, pre-emptive strategy is crucial in detecting vulnerabilities prior to its exploitation by third parties as stipulated in well-established adversarial machine learning frameworks (Vassilev et al. 2025).

Bibliography

AlMahri, Sara, Liming Xu, and Alexandra Brintrup. 2024. "Enhancing Supply Chain Visibility with Knowledge Graphs and Large Language Models." Preprint, submitted August 5, 2024. arXiv:2408.07705v1.

Babić, Milan, Adam D. Dixon, and Imogen T. Liu. 2022. “Geoeconomics in a Changing Global Order.” In The Political Economy of Geoeconomics: Europe in a Changing World, edited by M. Babić et al. International Political Economy Series. https://doi.org/10.1007/978-3-031-01968-5_1.

Bejtlich, R. (2015, January 20). Will sharing cyberthreat information help defend the United States? The Brookings Institution. https://www.brookings.edu/articles/willsharing-cyberthreat-information-help-defend-the-united-states/

Bhatia, Rajiv. 2024. "India's foreign policy priorities in 2025 and beyond." Hindustan Times, December 25, 2024. https://www.hindustantimes.com/ht-insight/internationalaffairs/indias-foreign-policy-priorities-in-2025-and-beyond-101735120104352.html.

Brown, Michael, Eric Chewning, and Pavneet Singh. 2020. Preparing the United States for the Superpower Marathon with China. Washington, D.C.: The Brookings Institution.

Burton, Joe, Ardi Janjeva, Simon Moseley, and Alice. 2025. “Al and Serious Online Crime." CETaS Research Reports. The Alan Turing Institute.

Cairo, Michael. 2023. “Synthetic Data and GDPR Compliance: How Artificial Intelligence Might Resolve the Privacy-Utility Tradeoff.” Journal of Technology Law & Policy 28 (1): Article 4.

Cha, Victor. 2023. "Statement before the House Committee on Rules: 'Examining China's Coercive Economic Tactics'." Washington, DC: Center for Strategic & International Studies, May 10, 2023. https://www.csis.org/analysis/examining-chinascoercive-economic-tactics

Chaudhuri, Promit K., Suraj Shekhar, and Colin Stewart. 2024. "Games Under Network Uncertainty." Preprint, submitted December 2, 2024. arXiv:2305.03124v5.

Clayton, Christopher, Antonio Coppola, Matteo Maggiori, and Jesse Schreger. 2025. "Geoeconomic Pressure." Working Paper, June.

Datasphere Initiative. 2022. "Sandboxes for data: creating spaces for agile solutions across borders."

Farrell, Henry, and Abraham L. Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." International Security 44 (1): 42–79.

Financial Action Task Force (FATF). 2021. Opportunities and Challenges of New Technologies for AML/CFT. Paris: FATF/OECD, July 2021.

Financial Crimes Enforcement Network (FinCEN). 2024. "FinCEN Issues Analysis of Identity-Related Suspicious Activity." News release, January 9, 2024. https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-relatedsuspicious-activity.

Guan, Hong, Fei-Yue Wang, Chen-Xu Wang, and Xiao Wang. 2024. "IDNet: A Novel Dataset for Identity Document Analysis and Fraud Detection." Preprint, submitted August 1, 2024. arXiv:2408.01690.

Huang, Xuqing, Irena Vodenska, Shlomo Havlin, and H. Eugene Stanley. 2013. "Cascading Failures in Bi-Partite Graphs: Model for Systemic Risk Propagation." Scientific Reports 3 (1): 1219. https://doi.org/10.1038/srep01219.

Huelss, Hendrik. 2025. "Transcending the Fog of War? US Military 'Al', Vision, and the Emergent Post-Scopic Regime." European Journal of International Security 10: 190–210.

IDSA Task Force. 2012. A Case for Intelligence Reforms in India. New Delhi: Institute for Defence Studies & Analyses.

Jackson, Matthew O., and Agathe Pernoud. 2021. "Systemic Risk in Financial Networks: A Survey." Annual Review of Economics 13: 171–202. https://dx.doi.org/10.1146/annurev-economics-083120-111540

Jensen, Benjamin, Bonny Lin, and Carolina G. Ramos. 2022. “Shadow Risk: What Crisis Simulations Reveal about the Dangers of Deferring U.S. Responses to China's Gray Zone Campaign against Taiwan.” CSIS Briefs. Center for Strategic and International Studies. February 16. https://www.csis.org/analysis/shadow-risk-what-crisissimulations-reveal-about-dangers-deferring-us-responses-chinas.

Johnson, James. 2022. "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age." European Journal of International Security 7: 337-56. https://doi.org/10.1017/eis.2021.23

Karam, Naouel, Fatiha Saïs, Nathalie Pernelle, and Mohamad J. Sahilia. 2022. "A Hybrid Knowledge Graph and Bayesian Network Approach for Analyzing Supply Chain Resilience." In The Semantic Web: ESWC 2022 Satellite Events, edited by Anna-Lisa Gentile, Ismail Ilkan Ceylan, and Ruben Verborgh, 117–31. Cham: Springer. https://doi.org/10.1007/978-3-031-43458-7_5

Kosasih, Edward Elson, and Alexandra Brintrup. 2022. “A Machine Learning Approach for Predicting Hidden Links in Supply Chain with Graph Neural Networks.” International Journal of Production Research 60 (17): 5380–93. https://doi.org/10.1080/00207543.2021.1956697.

Maganaris, Constantine, Athanasios Voulodimos, George Vouros, and Dimitrios D. Vergados. 2024. "Outlier detection in maritime environments using AIS data and deep recurrent architectures." In Proceedings of the 2024 PETRA Conference. New York: ACM. https://arxiv.org/abs/2406.09966

Munsing, Evan, and Christopher J. Lamb. 2011. Joint Interagency Task Force–South: The Best Known, Least Understood Interagency Success. Strategic Perspectives, No. 5. Washington, DC: National Defense University Press.

National Academies of Sciences, Engineering, and Medicine. 2021. Human-Al Teaming: State of the Art and Research Needs. Washington, DC: The National Academies Press. doi.org/10.17226/26355.

National Institute of Standards and Technology (NIST). 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1.

Nweke, Livinus Obiora, and Stephen Wolthusen. 2020. "Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection." In 2020 12th International Conference on Cyber Conflict, 73–92. https://doi.org/10.23919/CyCon49761.2020.9131721

Patel, Jitu, Saravana Kumar, and Gisela Van Kessel. 2024. "Give us a hand, mate! A holistic review of research on human-machine teaming." BMJ Military Health. Published online February 1, 2024. https://doi.org/10.1136/military-2023-002521.

Raimondo, Sebastian, and Manlio De Domenico. 2021. "Measuring topological descriptors of complex networks under uncertainty." Physical Review E 103 (2): 022311. https://arxiv.org/abs/2009.06326

Reuters. 2023. "China export curbs choke off shipments of gallium, germanium for second month." Reuters, October 20, 2023. https://www.reuters.com/world/china/china-export-curbs-choke-off-shipmentsgallium-germanium-second-month-2023-10-20/.

Routh, Adam, Roger Hill, Jennifer F. Cowley, William D. Eggers, Joe Mariani, and Kyle Nappi. 2025. “High-Stake Collaboration: The Private Sector's Influence on Great Power Competition.” Deloitte Center for Government Insights, February 12. https://www.deloitte.com/us/en/insights/industry/government-public-sectorservices/importance-of-private-public-partnership-in-great-power-competition.html.

The Royal Society. 2023. From Privacy to Partnership: The Role of Privacy Enhancing Technologies in Data Governance and Collaborative Analysis. London: The Royal Society.

Sanbad, Lipun Kumar. 2024. “From Dependency to Autonomy: Revamping the Defense Acquisition." Electronic Journal of Social and Strategic Studies 5 (Special Issue VI): 149– 60. https://doi.org/10.47362/EJSSS.2024.5608.

Sinha, Shakti. 2018. "Inter-ministerial and Inter-departmental Coordination." In Defence Reforms: A National Imperative, edited by Gurmeet Kanwal and Neha Kohli, 130–44. New Delhi: Pentagon Press.

Solow-Niederman, Alicia. 2020. “Administering Artificial Intelligence." Southern California Law Review 93: 633–95.

Special Competitive Studies Project. 2024. "Intelligence Innovation: Repositioning for Future Technology Competition." April 2024.

Stebbins, David, Jia Xu, Matthew Sargent, Christopher G. Pernin, and Danielle C. Tarraf. 2024. Exploring Artificial Intelligence Use to Mitigate Potential Human Bias Within U.S. Army Intelligence Preparation of the Battlefield Processes. Santa Monica, CA: RAND Corporation.

Tashji, David. 2025. "From Wall Street to the Pentagon | The Role of Finance in Modern Warfare." PWK International Advisers, February 1. https://pwkinternational.com/2025/02/01/from-wall-street-to-the-pentagon-the-roleof-finance-in-modern-warfare/.

Tecuci, Gheorghe, and Dorin Marcu. 2021. “A Framework for Deep Anticipatory Intelligence Analysis.” In Proceedings of the 2021 AAAI Fall Symposium on Cognitive Systems for Anticipatory Thinking, Arlington, VA.

U.S. Department of the Treasury. 2024. ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES: REPORT ON THE USES, OPPORTUNITIES, AND RISKS OF ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SERVICES SECTOR. Washington, DC, December 2024.

United Nations Security Council. 2024. "Note by the President of the Security Council." S/2024/215. March 7, 2024.

Vassilev, Apostol, Alina Oprea, Alie Fordyce, Hyrum Anderson, Xander Davies, and Maia Hamin. 2025. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2025.

Wang, Tianshu, Ralph Abboud, and Christos Faloutsos. 2024. "Towards Universal Dense Blocking for Entity Resolution." Preprint, submitted April 25, 2024. arXiv:2404.14831v2.

Warren, Kristin, Osonde A. Osoba, Jasmin Léveillé, James Ryseff, and Benjamin N. Harris. 2025. Improving Sense-Making with Artificial Intelligence. Santa Monica, CA: RAND Corporation.

Wasi, Azmine Toushik, Md. Mosaddek Khan, Jia Wu, Philip S. Yu, and Charu C. Aggarwal. 2024. "Graph Neural Networks in Supply Chain Analytics and Optimization: Concepts, Perspectives, Dataset and Benchmarks." Preprint, submitted November 11, 2024. arXiv:2411.08550.

Xie, Wenying, Jianing Zhai, and Yijun Liu. 2024. "Supply Chain Financial Fraud Detection Based on Graph Neural Network and Knowledge Graph." Tehnički vjesnik 31 (6): 2055–62. https://doi.org/10.17559/TV-20240606001759

Zugravu, Andreea, Tarek Mansour, Ary da Cunha, Ben Safran, and Aurélie Espérandieu. 2024. "Using Al in Economic Development: Challenges and Opportunities.” McKinsey & Company, May 22. https://www.mckinsey.com/industries/public-sector/ourinsights/using-ai-in-economic-development-challenges-and-opportunities.