

EGMONT PAPER 132

– MAY 2025 –

Financial Influence Operations in the Hybrid Threats Spectrum

Bernard Siman



ABOUT THE EGMONT PAPERS

The Egmont Papers are published by Egmont – The Royal Institute for International Relations. Founded in 1947 by eminent Belgian political leaders, Egmont is an independent think-tank based in Brussels. Its interdisciplinary research is conducted in a spirit of total academic freedom. A platform of quality information, a forum for debate and analysis, a melting pot of ideas in the field of international politics, Egmont’s ambition – through its publications, seminars and recommendations – is to make a useful contribution to the decision-making process. The opinions expressed in this paper are those of the author(s) alone, and they do not necessarily reflect the views of the Egmont Institute.

ABOUT THE AUTHOR

Bernard Siman, O.B.E. is a Senior Associate Fellow at the Egmont Institute covering Hybrid Threats and Warfare. He is also Head of Cyber and Financial Diplomacy at the Brussels Diplomatic Academy of the Vrije Universiteit Brussel (VUB). He teaches graduates and diplomats “The International Monetary Policy & Financial Architecture” and “Cyber Diplomacy & Statecraft”. He also teaches regularly at the Belgian Royal Military Academy. He was one of the authors of one of the first applied research reports on Hybrid Warfare in the Middle East, published by LSEIdeas, the foreign policy and security think tank of his alma mater, the London School of Economics and Political Science. In addition to financial services and security, he specialises in Hybrid Warfare and Mediterranean, Black Sea and Maritime and Middle East geopolitics, advising both governments and corporates. He has written extensively on these topics. He is a Member of both Chatham House and the Royal United Services Institute (RUSI).



Table of Contents

| | |
|---|-----------|
| Abstract | 4 |
| 1/ Threats to the components of the financial system and “Trojan-Horse” Operations | 6 |
| Targets are hard and soft | 6 |
| Economic security and financial security: Linked but distinct security spheres | 6 |
| Trojan horse operations 1: Financial hybrid threat examples and scenarios | 7 |
| Trojan horse 2: Misuse of Environmental, Social and Governance (ESG) requirements | 9 |
| The anatomy of an ESG hybrid operation: The lynchpin is an activist investor | 9 |
| Anatomy of an ESG hybrid operation: Misuse of ESG | 10 |
| EU’s ambiguous position on ESG hinders financing for defence innovation | 11 |
| Trojan horse 3: Convertible loans | 12 |
| “Threat finance” will continue to play a subversive role, especially for terrorists | 12 |
| Deepfakes: Hybrid threat to identification of financially transacting parties | 12 |
| FDI screening insufficient | 12 |
| 2/ Hybrid financial influence operations targeting global financial stability | 13 |
| Where FEIOPS sit in the hybrid spectrum | 14 |
| International monetary system vulnerable to hybrid threats | 15 |
| FEIOPS target the fiat system, as it is closely linked to geopolitics through the US dollar | 16 |
| Policy Recommendations | 17 |
| Conclusion | 18 |



This paper examines the Hybrid Threats, posed by perfectly legal and legitimate financial markets' operations, to national security through a variety of legal routes including acquisitions of intellectual property (IPs), Environmental, Social, Governance (E.S.G.) regulations, Activist Investors and others. Focus has hitherto been on macro-measures, such as Foreign Direct Investments (FDI) Screening, sanctions compliance, Anti-Money Laundering ("AML"), Counter-Terrorism financing ("C-TF"), supply chain security, raw materials and the like. However, very little attention has been paid to micro-level financial and economic security threats through legal and legitimate financial markets operations. In other words, Why spy when you can buy. To achieve economic and financial security in the interest of national security and maintaining military capability superiority, such micro-financial markets operations in the Hybrid Threats spectrum, i.e., in the financial markets, must be tackled to prevent, inter alia, critical technology leak; as well as to enable greater investments in military capabilities, which have become a key defence, security and Strategic Autonomy priority. The focus on macro-measure, in other words, is insufficient to achieve the objectives of economic and national security and must be urgently augmented by microlevel financial markets measures and awareness beyond AML and C-TF.

Threats to the financial system have evolved from being a primarily regulatory concern for governments, which enforce the rules of the global financial regulatory architecture (including for money laundering and terrorism financing), to increasingly becoming a national security threat for individual states and the EU, conducted mainly by hostile-actor-backed individuals and entities, largely through non-illegal and legitimate financial markets operations aimed principally at acquiring dual use and critical technologies, at undermining strategic companies, and at impairing lending to and investments in military capacity building.

These threats, that have existed for a long time but have not been recognised as being threats in a globalised world economy of open liberalised markets based on the international rules-based order, have in effect become an integral part of the broader hybrid threats spectrum that includes e.g. disinformation, cyber and A.I., corruption, fraud etc.

Recognition of their specific subversive and pernicious role in undermining national security and military capability (beyond general concerns about economic security) remains weak, however. The open and globalized markets paradigm that has prevailed in the last three decades in both the public and private sectors has created a doctrinal refusal to acknowledge that the free flow of capital in the absence of adherence by all states to the "Rules of the Game" (as enshrined by the World Trade Organisation (WTO) and other global standards setting institutions) has created a security threat ruthlessly exploited by adversary and hostile states. Moreover, the technical and specialised nature of financial markets did not entice politicians, bureaucrats and academics to delve into the subject, focusing instead on the general macro theme of "Economic Security", forgetting that finance is the blood that flows in the economic corpus to keep it alive. This gap between the adherence to the Rules of the Game by, inter alia, the EU and its member states on the one hand, and adversary and hostile states not adhering to the rules on the other, has created the perfect strategic weakness for the latter group to exploit in its pursuit of strategic advantage through the acquisition of critical and dual use technologies, and undermining funding for defence. Both the public and private sectors in the EU member states resisted and indeed continue to resent interference in what is seen as financial transactions in the normal course of business with little regard for national security threats.

Hybrid operations using the financial markets are effective in their own right but become still more potent when combined with other hybrid tools such as disinformation, digital manipulation, "active measures" (corruption, money laundering, physical threats, and so on), influence operations (including those incorporating disruptive

technologies such as Artificial Intelligence), “lawfare”, cognitive influence tools, the cyber and digital spheres, information warfare, and attacks on critical infrastructure.

The conduct of hybrid operations against the financial system targets its constituent components. These are the banks, funds, stock exchanges, other financial institutions such as insurance companies, payment systems, clearing systems, and their underlying hard and soft infrastructures. Such hybrid operations involve the use of integrated, coordinated, targeted and dynamically composed tools. This entails the continuous adjustment of the hybrid tools mix to achieve the objective of a hybrid operation and its specific aim against a specific target operating either within the financial sector, or the target being a non-financial company owning a dual-use or critical use intellectual property (IP), with the aim of acquiring that IP through legal and legitimate financial market operations. Again: why spy when you can buy?

This latter theatre of hybrid operations – that is, acquiring dual-use IP through non-illegal and legitimate financial markets operations – has emerged as a key threat to national and economic security, as well as military superiority. The three are interlinked more than ever through innovation as represented by IPs. Small startups and medium-sized innovators frequently face cash flow problems. The typical financial funding model across Europe is inadequate for these entities and individuals. It is an outdated model because it struggles to provide risk capital (e.g. uncollateralized loans) to innovators who lack assets to be pledged as security against debt funding. Meanwhile, equity financing is often too expensive for startups, requiring founders/innovators to cede substantial equity, and indeed in many cases cede control as well. This is typically when investors backed, owned or controlled by hostile or adversary actors move on their prey through legitimate financial markets operations by providing access to funds. This interest may occasionally be combined with other hybrid threats and instruments such as disinformation and intimidation, including burying the target company and management under a pile of spurious law suits, a form of micro-“Lawfare” aimed at wearing the target down financially and psychologically.

As innovation has become essential to maintaining military capability and superiority, so the protection of IP should become a national security matter of the first order, including considering finance as another instrument in the hybrid threats toolbox. In other words, the acquisition of critical and dual-use technologies through financial market operations has become a key tool in strategic power competition among states and is no longer a straightforward regulatory concern. The state’s interest in the financial sector must therefore evolve from a mainly regulatory interest to a national security interest, with the necessary institutional adjustments giving national security agencies a role in the markets where vital national interests like defence are at stake.

This paper deals with two distinct if closely related types of financial threats in the hybrid threats spectrum. The first is the financial system’s constituent entities. The second is the hybrid threats to the global financial system itself.



1/ THREATS TO THE COMPONENTS OF THE FINANCIAL SYSTEM AND “TROJAN-HORSE” OPERATIONS

Targets are hard and soft

Hybrid threats to the financial system cover both “soft” and “hard” targets, spanning all or a combination of the hybrid threats’ tools mentioned above.

In the “hard” threats spectrum the protection of the integrity of the infrastructure of the financial system has become paramount. This includes the security of sub-sea data cables, which transmit 95 per cent of global internet data and are thus key to cross-border financial transactions, whether it is a consumer transferring \$500 or a multinational corporation transferring \$50 million. The protection of satellite infrastructure and communications functions, including against electronic warfare jamming aimed at disabling satellite signals, is also key to the global financial system’s functioning. The space and cyber domains and their security therefore overlap in their vulnerability and in complementing each other to ensure the continuity of operations in the global financial system and its regulatory architecture.

Hybrid threats to the integrity of A.I. data are also to a large degree a function of the cybersecurity measures taken to ensure that integrity. The threat to that integrity is a key emerging hybrid threat vulnerability in the financial system’s functioning and business continuity.

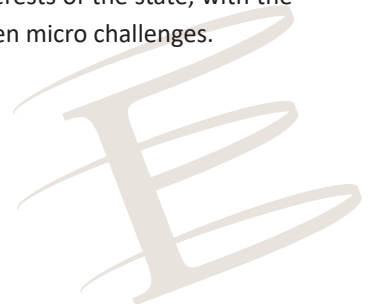
Hybrid threats also target the integrity of two key enablers (i.e. critical infrastructure) of the financial system’s healthy functioning: the payment system; and the clearing system.

The payment system enables the smooth execution of purchases and transfers. The clearing system enables the global financial system to transact seamlessly. In particular, the US dollar clearing process grants the US global extraterritorial judicial powers as soon as a dollar is cleared through its system. This is a key tool in combating terrorism, threat financing and money laundering. Hybrid threats aimed at disrupting or disabling these two systems can employ combinations of hybrid tools, ranging from the technical (cyberattacks) to the non-technical (disinformation). Integrated, coordinated and targeted hybrid attacks combining several tools (e.g., financial market operations by hostile actors with hostile intent, social and digital media, cyberattacks, disinformation, deepfakes) can thus also be deployed to cause civil disorder (such as spreading disinformation about bank insolvencies leading to domestic unrest), hamper stock market operations, undermine the normal functioning of strategic companies and target retail bank operations to undermine customers’ confidence in the banking system.

If the economy is the body of society, finance is the blood that keeps it alive. Hybrid threats do not confine their operations to targeting economic and financial security through undermining supply chains, raw materials sourcing and the like. They also target the blood that flows through the veins of the economic body: finance. It is therefore essential to consider threats to the financial system separately from economic security and to deal with them not as general regulatory or legal challenges but as national security threats over and above the traditional areas of AML and C-TF.

Economic security and financial security: Linked but distinct security spheres

Whereas economic security concerns itself with macro challenges directly linked to the interests of the state, with the public sector playing a key role in its affairs, financial security focuses on private-sector-driven micro challenges.



As mentioned above, the focus in countering hybrid threats has thus far focused largely on economic security macro challenges, e.g. supply chains, raw materials sourcing, securing markets, sanctions regimes and trade issues.

This is insufficient from a national security perspective, as financial security means that transactions take place mainly in the private sector through financial market operations that are not always covered by foreign direct investment screening regimes (FDI screening). Moreover, financial market operations require technical knowledge that is not widely available in state institutions. Moreover, the well-established regulatory functions within the rules of the global financial architecture have been the institutional preserve of central banks and market regulators, rather than national security agencies. National security has had very little involvement beyond law enforcement tasks concerning money laundering and terrorism financing. Complex and sophisticated hybrid threat operations within legal financial markets operations have attracted little national security or political attention, especially as they require a specialist intelligence capability connected to the financial markets, including non-listed company transactions. The latter are the most likely scenario for startups and small innovators, where many of the Ips for dual use technologies are to be found. The focus on the state's regulatory functions must be urgently augmented by a national security focus on specific and identifiable areas such as dual-use and critical-use technologies. Quantum technologies, A.I., semi-conductor chips, bio-technologies and new materials are excellent examples of where this national security focus can complement traditional regulators' regulatory functions. The chief risk in these areas is technology leakage through non-illegal financial market operations.

Trojan horse operations 1: Financial hybrid threat examples and scenarios

The following example is a fictitious case study based on an actual case. All names and details have been altered. All details here are for illustrative purposes only and do not reflect the original case's actual situation in any way.

Company X, a Dutch company, owned an ITU licence for two satellite broadband constellations. The licences were granted by Luxembourg – a major authority in this area of licences and Company X's main Regulator. Company X required further funding for its cash flow purposes to continue its systems' development and eventual deployment. No EEA-based financial institution, fund or financial backer, debt or equity was willing to further fund the company. It sought other investors.

Company Y, a non-EU-, non-US-backed company, with ultimate beneficiaries from an adversary state, became aware of this funding and IP acquisition opportunity and started gradually to build a substantial equity holding in Company X. It was subsequently suspected that it had strong links with a foreign military outfit.

Suspicious arose because Company Y said it intended to use the Dutch-built communications terminals (the founders had invented and developed the IP) for a non-EU- non-US-owned constellation, despite the fact that the Dutch Ministry of Economic Affairs had barred another communications manufacturer with a similar adversary backer from exporting terminals to certain markets, including the latter's home market.

Company Y tried to wrest total ownership, licence and management control from Company X and thus to own both the IP and the licences.

The Luxembourg regulator said that the two interests (i.e. those of X and Y) that had co-owned rights to the constellations' frequency filings had proved unable to meet the terms of their licence. The Luxembourg regulator subsequently approved Company X's stake but not Company Y's.



Both the Dutch government and the ITU then supported the Luxembourg regulator’s decision.

This was when another hybrid threats tool was deployed intensely: “micro-lawfare”. This is the launch of mass court cases against a company, management and personnel to make it financially, personally, psychologically, operationally and practically extremely difficult for them to continue operating the target company. The financial and personal costs of such lawfare tactics are extremely high, aiming to force surrender. Seventy court cases were launched by Company Y and its shareholders against Company X and its management.

In a lengthy ruling, advised by the Ministry of Economic Affairs, the Dutch cabinet declared two key resolutions:

1. It endorsed the earlier ruling of Company X’s home regulator, Luxembourg
2. It went beyond this legal affirmation, declaring that Company X’s constellation was a dual-use asset of strategic interest in the global geopolitical context (Company X also had US operations).

The decision followed an 18-month investigation launched by the Ministry of Economic Affairs involving the following ministries: Economic Affairs; the Interior; Foreign Affairs; Defence; Justice; Digital Affairs; and Transport (as well as other organs).

So, what are the lessons for counter-hybrid operations?

1. FDI screening is insufficient as a tool of economic and financial security. It urgently needs to be augmented by systematic counter-hostile investments tools. Financial market operations intelligence is essential to establish both what is and what is not a hybrid operation by an adversary or hostile actor. A hostile-actor-backed fund is not going to announce its actual identity or ownership; rather, it will utilize the single market through the weakest point of entry to appear to be an EEA entity that might not automatically attract FDI screening. This is where adequate and timely intelligence, as well as the existence of administrative and judicial instruments, is most important.
2. The EU and its member states lack administrative or judicial systemic instruments to counter such operations, ultimately leading to technology leakage, the most serious threat to national security and military superiority. In this case study the matter had ultimately to be decided at the political level, and only after 18 months. If the political level had not responded then, the technology would have flown out of the EU’s (and NATO’s) nest through a financial hybrid operation. Again, there is an urgent need to introduce administrative and judicial instruments that will automatically be triggered when national security breaches are suspected in investment and funding cases.
3. Courts should be enabled to cancel and annul share sale and purchase agreements retrospectively based on a negative statutory national security advice. Judges are currently unable to do this if a sale and purchase agreement’s modalities and formalities are in line with the legal and procedural requirements should the company and its management and shareholders become aware, after they have sold their shares, that the investor or lender is ultimately backed or owned by a hostile or adversary actor. Such a measure will strengthen deterrence against vexatious and frivolous micro-lawfare claims made by hostile financial investors and funders against companies and their management with the sole aim of defeating them through high legal, psychological and personal costs. If such a measure is introduced, it will render such micro-lawfare much less effective – and may indeed successfully put an end to it.
4. With so many ministries and state institutions involved it is no surprise that it took 18 months to reach a conclusion, and then only by the political leadership. Cross-silo coordination and cooperation among state institutions is key to countering financial hybrid operations, otherwise it will be very difficult to catch the ball every time.
5. The creation of a specialist financial intelligence capability with a national security remit that fundamentally differs from central banks’ and regulators’ financial intelligence units will be essential. Its task will be to assemble the jigsaw pieces from commercial and financial markets intelligence sources to assess if there is a particular ongoing hybrid

operation in narrowly defined areas of the corporate world. It will also function as a trusted specialist conduit, with the private sector enabling it to report activities of concern in national security sectors and corporate situations.

Trojan horse 2: Misuse of Environmental, Social and Governance (ESG) requirements

ESG has increasingly been included in the risk-return analysis when many leading funds make investment plans. Governments and the EU have also introduced ESG requirements, which can be summarized as follows:

- **Environment:** company exposure to economic consequences of climate change, including the impact of government climate change regulations and policies (benefits or adversely impacts the company)
- **Social:** HR practice, e.g. diversity, inclusivity, training, equal opportunities, labour relations, employee retention, etc.
- **Governance:** compliance with laws and regulations on tax, labour, the environment, board composition, management compensation, transparency, etc.

The corporate sector's current transition to net zero and the green economy, as well as the other two areas, social and governance, makes it most vulnerable to the abuse and misuse of ESG for hybrid threats. The greatest vulnerability is always manifested in periods of transition.

As a hybrid threat, ESG misuse is manifested in two distinct forms:

1. Direct impact, which includes:
 - a change of Board and management control
 - a change of company policies
 - who controls and has access to IPs – friend or foe – matters enormously to the threat of technology leakage and therefore to national security.
2. Strategic impact, which is manifested most clearly in the following:
 - the undermining of trust in financial markets, including how they operate. This is critical, as a great deal of financial stability, including currency stability, depends on trust in how financial markets function
 - the undermining of trust in the system – for example, by deploying misinformation on non-compliance to create the perception that some parts of society and the economy are favoured above others
 - the undermining of social cohesion, especially in the environment and social aspects of the ESG requirements, to create the impression that some parts of the financial system operate outside ESG requirements, undermining minorities or flouting gender balance requirements, for example.

The anatomy of an ESG hybrid operation: The lynchpin is an activist investor

Activist investors are a specific and well-defined equity investor category in the shares of companies. They are individuals or groups who buy a modest equity stake in a publicly listed company to influence how the company is run and benefit from the achievement of better financial returns. In the great majority of cases activist investors do so legitimately to achieve higher financial returns by identifying a particular weakness that the current price of shares influences management and the board to rectify, leading to a higher share price as the target company's financial performance improves. By doing this, they make a profit on the increase in the share price. They can demand seats on the board and reviews of business plans and audits, and they will typically have done their own research. They can be private equity funds, hedge funds, wealthy individuals and other forms of specialist funds. They identify a "problem" that the activist investor thinks they can "fix", and they try to get seats on the board. They often seek to change management, blaming it for the weakness. In many cases they also enlist the media to pressurize the company. The warning lights for the target company's management and

its board that an activist investor is stalking the company can be that they make a filing with the financial regulator stating that they have acquired a certain percentage typically defined by the regulator as requiring statutory disclosure. The activist investor can also sometimes remain below the regulatory disclosure threshold and will thus only be known to the management and the board when they start to make statements about the company's management and future direction.

An ESG-driven hybrid threat emerges when an activist investor is directly controlled, backed or influenced by a hostile or adversary actor, or when an opportunistic alliance has been concluded between a legitimate financially motivated activist investor on the one hand and an investor backed or controlled by a hostile or adversary actor on the other. Such a hybrid operation in effect starts either way by finding an activist investor to execute a coordinated and tailored operation against a specific target – typically, a company whose shares are listed on a stock exchange.

Anatomy of an ESG hybrid operation: Misuse of ESG

A case study may be useful here. All details and names have been completely changed, and all details used are only for illustrative purposes, except for the anatomy of how such operations are conducted.

We will call the target company “Vital Materials Inc”. It is a multinational company, producing dual-use innovative materials, with its global headquarters based in the EEA. Its main market listing is on the main Frankfurt stock exchange.

It owns multiple production sites globally, both inside and outside the EEA. It must also comply with the regulatory requirements and laws of each jurisdiction and has pledged to comply with net zero and green economy requirements. Because the transition is a gradual process over many years, the quality of some of its production sites falls short of EU requirements. It has also fallen behind with its own timetable for achieving the required environmental standards.

It has an excellent R&D capability. It owns both critical and dual-use patents, with some of the best engineers and scientists working at its facilities. It also funds university researchers.

The main shareholder, also the founder, has a significant minority stake. The remaining equity is listed and is held by a variety of market investors, including funds and individuals. The shares are traded freely on the stock exchange.

Vital Materials Inc. has published a clear policy to transition to the Green Deal across its global operations and locations. It has been implementing the policy gradually given the complexity of transitioning, especially adjusting supply chains, and bearing the cost of retooling facilities. The capital expenditure programme therefore requires the combining of both internal cash and fresh capital from new investors.

The reality of transitioning means the retooling of one of the EU sites will take significantly longer than planned and announced.

It is in this context that an activist investor, spotting a weakness in the company's implementation of its plan, has discreetly accumulated 4 per cent of the shares. The activist investor does not need to declare their holding because it is below the statutory disclosure threshold of 5 per cent.

Having accumulated 4 per cent of the shares, the activist investor sends a string of letters to the company's CEO and board, making the case that the company has failed in its plans on ESG grounds and demanding quick action at that production site.



The activist investor has simultaneously been building a relationship with the local mayor, with the aim of gaining support for the complaint. This leads the local authority to start threatening to suspend some of the licences for the site it had granted to the company years ago.

With social and other media activity and campaigns bolstered by disinformation and deepfake reports of accidents at the site due to the weakness of the ESG requirements, the local and national media now take an interest and zoom in on the story.

The activist investor also enables an NGO to buy a very small number of shares. The NGO thus becomes a shareholder with bragging rights, including at the general meeting, magnifying media interest and coverage.

The combination of these negative factors and pressure on the company and its management results in the share price beginning to fall, seriously weakening the hand of the current management and board with their main shareholders and other stakeholders, as they are perceived to have handled the whole situation badly, affecting earnings growth.

Backed by hostile investors and actors, the activist investor moves to acquire more shares at lower prices, increasing their ability to exert pressure on the company as the size of their holding increases.

Ultimately, the activist investor is invited to join the board – Open Sesame! They henceforth have access to IPs, and how they are controlled, sold, licensed and otherwise treated. They are also in a position to influence the company's future business plans.

In worst-case scenarios, new investors have driven companies to bankruptcy while retaining the IP and any licences.

EU's ambiguous position on ESG hinders financing for defence innovation

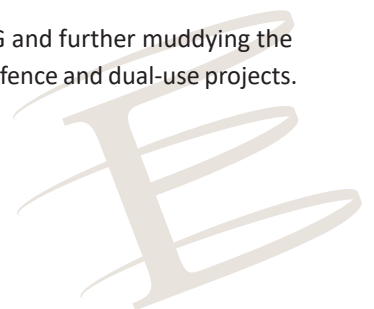
A strategic own goal has emerged because of the ambiguity of the EU's position on how defence and dual-use funding is regarded for ESG purposes. The messaging has been mixed at best. This needs to change urgently.

Banks and funds are reluctant to fund defence or dual-use investments because of the perception that EU ESG regulations do not support such investments and funding.

This is crucially important as we move towards not only higher levels of defence procurement but also to support and innovation across the board, from typical legacy defence vendors to innovative startups.

This matters to both NATO's efforts and the EU's. The NATO Innovation Fund (NIF), an innovation-driven equity-funding mechanism, is likely to be hampered by ESG regulations from a purely compliance perspective if the EU does not make a clear statement exempting all defence and dual-use investments and funding from ESG regulations. It is therefore critical for defence innovation to remain in the EU instead of migrating, and that the EU acts urgently. Such action will unleash a wave of private innovation funding, especially given that the purpose of the NIF in backing a particular company is to give confidence to private investors to co-invest with the NIF. Such a model may unleash a wave of much-needed investments in innovation, with all its defence and national security advantages.

Disinformation about ESG therefore has the strategic aim of obscuring EU messaging on ESG and further muddying the water to prevent private capital investment and co-investment in innovation, particularly in defence and dual-use projects.



This is another strategic reason for the EU to make a clean break with current messaging and make it unambiguous that such investments fall outside the remit of ESG regulations.

Trojan horse 3: Convertible loans

A key distinction must be made between “ownership” and “control” in how funding affects a particular company. Most research on the subject of how much foreign financial influence is exerted in a particular economy focuses on examining companies’ shareholder registers. Such an ownership-driven approach misses the complexity of the issue of control without ownership, primarily through convertible debt instruments such as bonds. In other words, a company’s shareholding can appear completely free of any indications of hostile foreign influence because all the shareholders are bona fide nationals. In reality, however, if the company has taken on convertible debt (i.e. debt that can be converted into equity at the lender’s option at a pre-agreed price), this potential new shareholding, should the lender choose to exercise their right to convert it to equity, may in fact control the company’s affairs. They are in effect not only shareholders in waiting but have the power to call in their loans, which may drive the company into bankruptcy. Moreover, they have the power to influence the company when it needs cash flow to seek a capital increase. This may mean that all other shareholders can be diluted, as they lack the necessary funds to participate pro rata in the capital increase. Such a step puts the hostile investor firmly in control of the company and its IP, licences and business.

Intelligence here is key. From a national security perspective, it is essential that control is exposed, and equity ownerships are examined – that is, beyond who the current shareholders are.

“Threat finance” will continue to play a subversive role, especially for terrorists

Threat finance includes a combination of money laundering, trade, criminal activity, fraud, digital operations and arms purchases, as well as corruption, to achieve not only economic gain to fund operational activities but also to undermine the governance structure and cohesion of target states and actors. It has acquired increasing importance for terrorists, and increasingly organized crimes groups, since the rise of Al Qaeda and Daesh/ISIS/ISIL. These players have developed hybrid tools in the financial sphere to varying degrees of sophistication, some of which are highly effective threat finance operations. Threat finance also covers trade in goods, and how they are financed for terrorist purposes, the misuse of development aid, organized crime finance, and money laundering, fraud and corruption.

Deepfakes: Hybrid threat to identification of financially transacting parties

A growing hybrid threat in the financial sector is the role of deepfakes in undermining the verification of the identity of one party to a transaction, as well as that of the ultimate beneficiary during a live virtual meeting. Malign actors can steal the identity of a legitimate bank client in real time, undermining the due diligence process of who the ultimate beneficiary actually is, or taking on the character of the recipient of funds. From a security perspective determining who the ultimate beneficiary is (e.g. when opening an account with a bank or fund) lies at the heart of identifying good and malign actors.

FDI screening insufficient

There seems to be a consensus in the EU, as well as in individual member states, that FDI screening will itself be sufficient as a counter measure.



Some EU member states like Germany and Denmark have become increasingly concerned about and aware of financial and economic operations by non-EU entities, particularly from China and Russia, aiming to acquire controlling stakes in companies that have developed or own critical and dual-use technologies and IPs. They have therefore developed and legislated FDI screening laws giving the state significant powers to call in proposed acquisitions and subject them and their backers to a highly intrusive screening process. The process not only includes due diligence on the acquiring entities and their shareholders but also on how the financing structures work, as in some cases (such as convertible loans or mezzanine financing) the actual ultimate equity beneficiaries may have the option to acquire the equity in the target company later or to influence how the management acts. Moreover, in the cases of Germany and Denmark there is a five-year post-acquisition period during which the state retains the power to call in the acquisition if it deems it necessary. The German and Danish models may become templates for other member states.

Although this development recognizing the critical link between financial, economic and corporate activity on the one hand and national security on the other is welcome, it is far from sufficient on its own. This is the case for three main reasons:

1. FDI screening covers only non-EU based entities. For EU-based acquiring entities no such screening is required under the current legislation. Clearly, hybrid operations will aim to obfuscate the issue, hiding the ultimate beneficiary (i.e. the acquirer) behind screens such as investing in multi-investor funds that will then execute the acquisition or use EU-based companies with ultimate beneficiaries that are hostile or adversarial. It will be more effective to call in all critical and dual-use technology acquisitions.
2. FDI screening does not cover vexatious claims by the acquiring entity made before making an acquisition proposal against the target company or its management. For example, they may have been subject to an influence operation aiming to weaken the company and the individual involved financially and to intimidate them in the law courts or the court of public opinion by falsely claiming that they do not adhere to ESG standards.
3. FDI screening, perhaps for domestic bureaucratic and political reasons, completely ignores the issue of ill-intended research funding to universities in critical and dual-use technology areas, whether to professors or graduate students.

2/ HYBRID FINANCIAL INFLUENCE OPERATIONS TARGETING GLOBAL FINANCIAL STABILITY

These threats are chiefly aimed at undermining trust in the financial system and its stability. Open democratic systems will have to develop both awareness of and effective tools to deal with influence operations deployed by adversary states (as part of their hybrid warfare) targeting the trust factor, the workings of various financial activities, and the stability of the global financial system and its regulatory architecture.

The very basis of a globalized rules-based economic and financial order, with all its geopolitical dimensions, not least because of the centrality of the US dollar, relies mainly on the pillar of the free flow of capital and its attendant rules. When trust in these rules wanes, the international monetary system (IMS) and its institutional architecture weaken. Global financial, economic and trade stability therefore suffers, leading to various disconnects. Such disconnects – for example, serious trade imbalances – can have equally serious geopolitical consequences. This is one of the most serious ways in which financial and economic influence operations (FEIOPS) can undermine stability. Russia and China have been deploying hybrid tools in the financial and economic sectors not only in areas specific to finance but mainly to achieve broader strategic objectives. This section aims to place them in the broader FEIOPS context.



Democracies used to the orthodoxy of the free flow of capital and trade and to free markets within agreed regulatory frameworks have been slow to comprehend and respond to this new set of threats. Governments and the European Union (EU) have been equally reluctant to interfere in market activity on national security grounds as part of their regulatory functions. Over the last decade or so, however, the economic and financial sectors have become key tools, as well as targets, in the conduct of hybrid operations.

In this respect it is important to note that the financial tools democracies deploy can play a key role in geopolitical deterrence. The importance of the financial sector in statecraft has been demonstrated in the West's response to Russia's illegal war on Ukraine, as it has met a kinetic military invasion not only with military means but with financial sanctions that do not simply target trade but are based largely on Russia's position in the international monetary system and its global architecture. In other words, it is also a case of tanks versus banks. Democracies' response must therefore be qualitatively upgraded from building resilience and crisis management (i.e. reactive) to effective deterrence (i.e. preventive) by making the cost of launching hybrid attacks in the financial sphere very high for attacker states.

Where FEIOPS sit in the hybrid spectrum

It is both useful and important to situate FEIOPS in the spectrum of hybrid warfare tools, as they not only complement other tools when used in combinations but are also potentially mutually enhancing. There are three specific areas in the spectrum within which FEIOPS are most effective.

The first is related to adversaries' hybrid use of diplomacy and public outreach. This includes divide-and-conquer along ethnic, religious, linguistic, class, regionalist and other lines exploiting differences; building and cultivating "friends" in target states; recruiting and developing "useful idiots"; and building up general support, including the provision of financial support for politicians, associations and causes. Financial incentives and FEIOPS play a key role in delivering the aims of this aspect of hybrid threats for a state launching hybrid warfare offensives.

The second is related to information and narrative warfare. This concerns the creation of a negative narrative in the target state and exploiting political events (e.g. referenda and elections) to help achieve the attacker state's desired outcomes. These operations could extend to undermining trust and confidence in either the whole or parts of a particular financial system (e.g. undermining trust in the solvency of banks and stock markets) or in the international monetary system and its architecture, including the effectiveness of regulatory regimes or the fairness of the management and conduct of a particular global institution.

The third can generally be termed "command and control". This encompasses a broad set of directions issued by the attacking state, leaving the implementation and details to its proxies and supporters, including money laundering, corruption and fraud, and cyberattacks on banks and individuals' accounts.

The strategic aim of the attacking state or non-state actor is to launch influence operations that target the use of corruption and create financial panic. Influence operations in the financial and economic sectors are therefore both an enabler and an essential integral and integrated part of the hybrid warfare toolbox.

Developing both business and government awareness of FEIOPS will be a step change in the regulatory environment and the state's role in how markets function on the one hand, and how business views its position in the national security equation on the other. Such a development will effectively alter the role of regulation and the regulatory authorities in the

economy and the financial services sector. There is therefore an acute need for a specialist and expert corps of financial diplomats to help guide this strategic shift as they combine the equation's two elements: geopolitics and international relations; and the requisite financial and economic expertise.

International monetary system vulnerable to hybrid threats

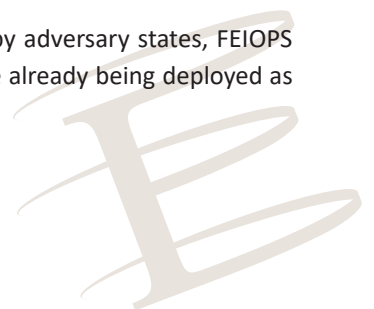
The international monetary system (IMS) constitutes the arrangements, both formal and informal, that drive relations and links between currencies. It is thus the glue that binds the world's individual national and supra-national economies together to enable them to interact according to agreed rules. These rules of the game are a key component of the rules-based international order. This is because they are crucial for global financial stability and the flow of trade leading to economic prosperity. Critically, they are also a key geopolitical stabilizer, ensuring that balance of payments (BOP) tensions and stresses between trading states are dealt with before they boil over into domestic political shocks affecting employment and living standards. These shocks are the point at which BOP tensions and their domestic consequences are more likely to become international and geopolitical conflicts, leading in most cases to retaliatory measures and a worsening international relations environment, and in some cases to armed conflict.

The IMS is closely related to another key component of global stability and prosperity, that of the rules-based world trading system. These two systems, the IMS and world trade, are closely linked through currency exchange rates, for example. A key purpose of the largely voluntarily agreed rules of the IMS is thus to create stability in the foreign exchange markets to enable growth in world trade, support the elimination/resolution of BOP problems, and provide orderly access to international credits when crises or shocks occur that disrupt stability at both national and international levels, thus restoring overall stability. Global regulatory and policy coordination are critical to the workings of the IMS, which can be achieved either through explicit agreements or through one country voluntarily following the same rules as the others (the "network externalities"). In other words, the rules of the game are what each country must follow so that the IMS keeps working to deliver global financial and trade stability and growth.

Throughout history the IMS has had a main centre or core such as gold, which was adopted to enable the gold standard to operate the rules in the nineteenth century. Today's IMS is largely the result of the United States ending the post-WW2 Bretton Woods system of fixed exchange rates in 1973, which had been agreed in the dying days of WW2 in 1944. In its place the system of fiat currencies was introduced, in which the value of the currency does not depend on any underlying metal value such as gold but instead largely relies on trust in the governments that issue currencies.

This is where the vulnerability of the IMS to hybrid influence operations lies: undermining trust in the democratic system, its institutions and decision-making processes through mis/disinformation and financial activities may result, if not countered, in the undermining of the IMS and global stability, potentially leading to the existing rules of the game being challenged, with all sorts of geopolitical and stability consequences. The international free flow of capital since the fiat currency system was introduced enabled a massive growth in global capital markets (nearing the historic heights of 1913). Both periods witnessed a massive growth in technological innovation, leading to very high new levels of complexity and interlinkages. This necessitated the development and adoption of the current sophisticated global regulatory system, and international multilateral cooperation and coordination through multilayered international institutional arrangements, arrangements and architecture.

As this elaborate set of delicately balanced arrangements and architecture is challenged by adversary states, FEIOPS will increasingly be deployed in targeting its fault lines. Moreover, financial instruments are already being deployed as



geopolitical instruments of conflict. The West's agreed response to Russia's illegal invasion of Ukraine included removing Russia from the Brussels-based SWIFT system (Society for Worldwide International Financial Transfers), and freezing the assets of the Russian central and private banks. In effect the measures disable the Russian rouble's convertibility, crippling trade with Russia. These are pure financial instruments deployed in the context of a hot geostrategic conflict. Indeed, the first set of US sanctions against Russia after the latter's recognition of the two breakaway Ukrainian regions of Donetsk and Luhansk already included the effective cutting off of any debt funding for and trading in Russian state bonds. Financial activity in its broader geopolitical context will necessitate a new appreciation of its role in determining how strategic challenges, interests and responses are handled, as well as the decisive role it can play in statecraft, including as tools of hybrid influence, in undermining the current currency system, for example.

FEIOPS target the fiat system, as it is closely linked to geopolitics through the US dollar

The reality of the fiat currency-based IMS is that the US dollar sits at its centre because it remains essentially the dominant fully convertible global reserve currency. It is thus a fact that dominance of US military power underpins the global US dollar-based fiat system and the position of the US dollar as the world's reserve currency.

There are three key observations in this regard:

1. Maintaining trust in the US dollar, so crucial to preserving global financial and economic stability, is related not only to maintaining trust in how the US government backs the US dollar but also to *perceptions* of the US's global military superiority. Mis/disinformation influence operations target perception forming and cognitive resilience, not least in how *confidence in the currency is related to perceptions of military capability* and domestic stability (for a deeper treatment of this subject by the same author: <https://www.egmontinstitute.be/trump-takes-on-the-fed-and-weakens-the-geopolitical-position-of-the-us/>).
2. The current US dollar-centred fiat currency system and its central position as the world's reserve currency mean the US can in principle print US dollars to the extent required and can thus fund domestic US spending such as the domestically critical welfare budget. This is the link between the IMS and US domestic politics. Targeting cognitive perception formation through hostile hybrid influence operations in the financial and economic sectors, or in weakening perceptions of the US's military superiority, may therefore pose challenges not only for US domestic politics but also for global financial stability, and how the rules of the game are upheld or otherwise.
3. It is important to note that the IMS is not an architecture agreed by all countries in one meeting, unlike the World Trade Organization (WTO). It is mainly constructed by voluntary commitments made by states which see both the systemic value of adhering to the rules of the game on the one hand and the specific benefits derived in bilateral and regional contexts (such as trade and capital markets) on the other. Moreover, states sign up to the IMS because they want to utilize their trading and foreign gains efficiently. Some have already experienced existential crises (e.g. war, the collapse of their banking systems) and been well served by IMS support mechanisms. They also sign up because maintaining order and stability leads to security, prosperity and the alleviation of poverty. In addition, many countries join the system because their trading partners and neighbours have already joined, simply because joining maximizes benefits and minimizes costs. In some cases, geopolitics drives the desire of some states to join – for example, the Gulf states, which choose to peg their currencies to the US dollar because oil is dollar-denominated – and to solidify the geopolitical alliance with the US.

The IMS and geopolitics are thus very closely linked, making the IMS another key target in the Great Power Competition. A key observation that seems little understood by a democratic world accustomed to seeking stability through its multilateral

efforts is that maintaining the status quo is no longer necessarily the aim of all major players. Indeed, Russia, China and Iran see no benefit in maintaining the current rules or in preserving stability, regarding the changing of the status quo as beneficial to their interests. This is reflected in the attempts within the BRICS grouping to de-dollarize the trading system. Moreover, they see the existing system as perpetuating the West's power, and they therefore deploy hybrid influence operations in pursuit of both the narrow objectives of weakening a particular state's financial and economic systems and globally challenging and altering the rules of the game.

POLICY RECOMMENDATIONS

The following are practical policy recommendations to augment the current regime of financial regulations and transactions control with the urgently needed national security character and authority:

1. Establish a specialist Financial Security Intelligence Capability with the aims of gathering information on actual ongoing and proposed transactions, particularly in the non-listed companies segment that are owners or developers of dual use IP; to issue national security advice on certain transactions where there are suspicions about the intent of the investor/funder, and to create a trusted and legally mandated conduit between the public and private sectors (e.g. providing the proverbial phone number to call by the CEO of a company under siege by an investor backed by a hostile or adversary state). This capability does not need to be a new agency. Rather it can be a cross-silo platform for the exchange of information, deciding on what is and is not a Hybrid operation, and agreeing on action.
2. Enable courts and judges to retrospectively annul sale and purchase for shares, or loan agreements, based on a negative national security advice. This step will have the added advantage of significantly raising the threshold against the success of hostile financial markets operations.
3. Create a cross-silo financial security platform across state institutions to be able to identify, and subsequently react, in a timely manner to Hybrid Threats in the financial sector.
4. Create a systemic capability to intervene (both having the duty and the right) by the admirative or judicial organs in cases of suspected nationals security breaches in the investment and lending sectors, rather than being powerless awaiting political level decisions to intervene, which is time-consuming in situations where time is of the essence.
5. Mandate the teaching of Hybrid Threats, as part of Business Continuity and Crisis and Reputational Management, in graduate courses in business schools, and instituting awareness programmes for the private sector that this is not just a national security threat, but is a Business Continuity and Crisis and Reputational management necessity.
6. Complete the Capital Markets Union to provide innovators with deep sources of risk capital thus treating the key root cause of vulnerability, i.e. the lack of availability of risk capital that opens up the opportunity for Hybrid operations in the financial markets leading to technology leak.



CONCLUSION

A bureaucratic and business culture shift is required to make state institutions take a serious interest in FEIOPs similar to other (more visible) threats, while business needs to acknowledge and comprehend that not all market activity is benign and to trust the state in what it is facing. The timing of such a shift in culture and institutional frameworks is opportune, as citizens, business and the state share the common interest of defending democracies' prosperity, security and way of life. All three are materially and directly threatened by FEIOPs much more than by cyber per se. Business as usual will have dire consequences for democratic societies accustomed to symmetric rather than asymmetric hostile operations. This will be a key and necessary cultural shift for both state institutions and the business and academic worlds.

Russia's invasion of Ukraine signals that the liberal economic order of free markets and global free flows of capital, goods and services has reached its security limit. The West's open markets can no longer be abused to attack the liberal democratic order from within using the latter's own tools.

The only way to defeat hostile influence operations is to develop and adopt a new *modus operandi* that relies on the cross-silo collaboration of the various state institutions on the one hand, and between the state and the private sector on the other. Threat finance is now an integral part of hybrid warfare operations. Trade finance is a critical component of threat finance, as it can raise funds through a variety of mechanisms to buy arms and finance terrorist and other hostile operations. Financial and state institutions must therefore implement qualitative assessment measures of trade finance facilities rather than simply rely on box-ticking regulatory exercises.

The strategic conclusion is that the future of democracies will be uncertain in the newly emerging authoritarian, cyberized, digitalized and anti-status-quo-ante world, in which stability is not a common aim, non-state actors and ungovernable spaces proliferate, and influence operations affecting public life, the economy and financial stability, trust, and the control of data are as strategically potent in the long term as arms. Democracies and their allies must band together to develop collective and integrated operational, legal, technical and conceptual resilience to withstand and defeat largescale, systemic and sustained threats, or this future will itself be threatened.





The opinions expressed in this Publication are those of the author(s) alone, and they do not necessarily reflect the views of the Egmont Institute. Founded in 1947, EGMONT – Royal Institute for International Relations is an independent and non-profit Brussels-based think tank dedicated to interdisciplinary research.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the permission of the publishers.

www.egmontinstitute.be

© Egmont Institute, May 2025

© Author(s), May 2025