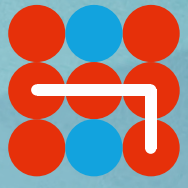
COI VULNERABILITIES AND RESILIENCE

Hybrid CoE Working Paper 8

JUNE 2020

Hybrid threats in the financial system

ALEKSI AHO, CATARINA MIDÕES, ARNIS ŠNORE

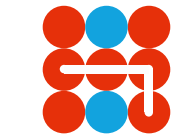


Hybrid CoE

Hybrid CoE Working Paper 8

Hybrid threats in the financial system

ALEKSI AHO, CATARINA MIDÕES, ARNIS ŠNORE



Hybrid CoE Working Papers are medium-length papers covering work in progress. The aim of these publications is to share ideas and thoughts, as well as to present an analysis of events that are important from the point of view of hybrid threats. Some papers issue recommendations. They cover a wide range of important topics relating to our constantly evolving security environment. Working papers are not peer reviewed.

The Vulnerabilities and Resilience COI focuses on understanding participating states' and institutions' vulnerabilities and improving their resilience by sharing best practices, developing new policy proposals and identifying topics to be studied further. The aim of the COI is also to improve public-private and civil-military partnership in countering hybrid threats.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-63-2
ISSN 2670-160X

June 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Preface

The Community of Interest on Vulnerabilities and Resilience launched its Finance and Markets work strand with a general kick-off meeting in Helsinki on 19 June 2019. During the meeting, hybrid threats were defined, and some questions formulated for the upcoming workshop, which took place in Brussels on 12 February 2020. These two events brought together approximately 120 participants from the public and private sectors.

The workshop on "Hybrid threats in the financial system" was organized in close cooperation with Bruegel, a European think tank that specializes in economics. The workshop examined hybrid threats in the context of the financial system by assessing vulnerabilities and solutions for effective protection measures and improved resilience. Particular attention was paid to potential systemic gaps that would open up possibilities for adversaries to use hybrid influence against economic and financial systems to create disturbances and prevent economic development and financial activities.

To address the issue of hybrid threats in the financial system, both economists and security policy experts came to the table, two groups which seldom overlap. There are clear differences between their world views, which translate into different perceptions of urgency and priorities.

For many economists, the economic expansion of a country is an opportunity for European businesses and citizens to access new markets and new products. Expansion is not a cause for concern per se, if it is not to the detriment of others. However, for security policy experts, economic expansion should not be perceived nor dealt with as separate from geopolitical ambitions. Economy and finance are elements in the confrontation of powers, and the EU is vulnerable to its surroundings. Geo-economics has been a part of the "great power competition" for decades.

It is for these reasons that the Community of Interest on Vulnerabilities and Resilience is aiming to map the vulnerabilities of the financial system in order to understand the methods of adversaries. In this endeavour, cooperation between the public and private sectors, as well as security practitioners and economists, is of paramount importance. This paper intends to capture the main findings from the above-mentioned events to understand how the financial system can be used as an enabler or target of disturbance, although the main focus is on the former aspect.

It is worth mentioning that the events were organized and the results compiled before the Covid-19 pandemic. However, issues raised during the events have become even more significant today, as the measures necessary to contain the virus have triggered an economic downturn. Vigilance is required as the pandemic can expose Western economies' vulnerabilities, and hostile actors could try to use the situation to inflict hybrid threats and achieve strategic gains within these economies and their financial systems.

Contents

Introduction

Like hybrid threats in general, hybrid threats emerging in the financial domain are always aimed at exerting a strategic impact. The financial domain may serve as an enabler for hybrid activities to have an effect on non-economic domains of the target. Yet the financial system may also be the main target for disturbance. While hybrid threats potentially make use of all strategic domains and sources of power, they can also occur in only one domain. However, the effects often cascade across many domains, creating social unrest, destabilization and cascading effects in all parts of society.

In the economic/financial domain, the financial system is often examined from the financial security and stability perspective, such as central banks' liquidity assistance to the financial system as a whole through market operations, as well as emergency lending to individual banks. In the hybrid threat context, the financial system should not only be looked at from the stability and financial security perspective, but should also include economic leverage-building, interference in internal markets, cyber threats and information influencing activities.

The financial system, given its centrality to day-to-day economic transactions, is an attractive target for adversarial action. Undermining its credibility, or otherwise disrupting its operations, can create havoc in an EU member state and in the EU generally due to financial, monetary, and single market interdependencies, as business activities are slowed down, distrusted, or even brought to a halt. In this case, one refers to the financial system as being a target of hybrid threats.

At the same time, the financial system is a channel for capital within the private sector, between the private and the public sectors, and for households. In the EU, banks in particular are responsible for a major share of corporate financing. The financial system is an intermediary of monetary policy, whose reactions can dampen or exacerbate macroeconomic shocks. The importance of the financial system as a link between different sectors makes it an enabler of hybrid threats, through which foreign actors can gain influence.

Both aspects pose great challenges to the EU, due to its governance architecture consisting of strong economic and financial integration but political and security policy in stronger member state leadership. This asymmetry can exacerbate vulnerabilities in the financial system, making them exploitable by outside actors and hindering resilience.

It can be argued that the ultimate long-sighted ambitions of actors responsible for hybrid threats are related to the market shares of the future global economy. Thus far, democratization and globalization have been presented in tandem by the Western world as the obvious road to social and economic prosperity. However, this presumption is seriously contested, with opening to outside markets clearly only benefitting a handful of countries, of which the most relevant, China, has reaped benefits without adopting democracy. Hence, the Western strategy is no longer seen as the only route to economic success.

In this narrative and geopolitical rivalry, hybrid campaigns are aiming to marginalize the Western liberal world, politically and culturally on the one hand, while gradually exerting an impact on the economy, on the other. The theory of external economies of scale has long indicated an important implication. External economies assign an important role to comparative advantage, history and accident in determining the pattern of international trade.

PART I: The financial system as an enabler of hybrid activities

The role of the financial system as an enabler, as opposed to a target, of hybrid threats implies the recognition of the existence of close links between capital movements, industrial developments, state interests and geopolitics, and of the centrality of the financial system as a mediator (intentionally or unintentionally) of these relationships.

Even if a cyber attack against a bank – preventing customers' access to online banking or disturbing the ATM network – is the most palpable hybrid threat involving the financial system, the biggest threat is arguably its instrumentalization to advance the strategic interests of other state actors.

The financial system ought to be resilient to attacks directed at it, but also to attacks that make use of it. The instrumentalization of the financial system to advance the strategic interests of state actors is not a new phenomenon. Using the economy as a tool for inflicting damage upon a target state cannot be considered a new tool for power projection, as geo-economics has been a part of states' toolkit for decades. However, the current hybrid threat environment requires us to improve our readiness for a community-level response. This section focuses on the financial system as an enabler of hybrid threat activities.

Risks/Vulnerabilities

The separation between economics/finance and national security

For many economists, the economic expansion of a country is an opportunity for European businesses and citizens to access new markets and products. Expansion is not a cause for concern per se, if it is not to the detriment of others. As an example, concerns about China often centre on 'levelling the playing field' or reciprocity, that is, ensuring that the expected economic benefits from Chinese expansion accrue to Europeans.

However, for security policy experts, economic expansion should not be perceived nor dealt with as separate from geopolitical ambitions. Economics and finance are elements in the power political struggle, and the EU is vulnerable to its surroundings. Such a separation in the risk perception can lead to economic policy mistakenly overlooking national security concerns. In the academic literature, the notion of geo-economics refers to this logic of using economic means for power projection (see e.g. Scholvin et al. 2018).

The construction of the EU, built originally around economic integration, not only lacks the ambitions but also the tools of a nation state. The EU has progressively centralized economic policy – on competition and trade – but geopolitical and security issues have remained mainly in the hands of member states.

The financial system is used as a tool around the world to further the strategic interests of states. Some of the most common elements are banks, which support and finance state activities, but more complex financial vehicles are also emerging. A telling example is the vision fund, which coupled tech investments with private actors and the Saudi Arabian regime.

While most states use the economy, foreign policy, security and technological tools in tandem, the EU has kept them separate for too long and should duly increase coordination between the economy and other strategic fields. Perhaps more worryingly, EU economic policy has often handled relations with other countries as if they too kept economic policy separate from other ambitions.

State subsidies and state-owned enterprises are examples of entities that place the strategic interests of a country first – before any con-

cerns of economic efficiency. If a concern about cyber attacks is that they are often untraceable and detected only years later, the same principle applies here. An investment or company which outwardly appears to be purely economically motivated can mask strategic interests, either pre-existing or developing further down the line.

EU fragmentation

The financial system is a weapon of soft power which the EU, without full nation-state competences, cannot wield and, institutionally fragmented, cannot fight against. The EU's lack of coordination is a significant challenge because if all countries fail to exercise the same level of care, security issues can arise. In the same vein, if certain countries are vulnerable to foreign influence because of less robust economic and financial systems, costs are bound to spill over. Buying dual-use technology from a European partner that relies on possibly compromised components is not a solution.

Chinese economic influence spills over into geopolitical matters in Europe, demonstrating simultaneously the blurred lines between geopolitics and economics, and the way in which EU fragmentation helps advance the strategic interests of other nations (see e.g. Leonard et al. 2019).

Overseas lending

Starting with China's "going global" strategy, China has become the world's largest official creditor, surpassing traditional official lenders such as the World Bank, the IMF, or all OECD creditor governments combined. China's official lending and investments amount to almost 10% of global GDP. However, China's overseas lending has always had a strategic element and some distinct features (see e.g. Horn et al. 2019).

Unlike the capital outflows from other major economies, which are largely privately driven, China's capital outflows are almost exclusively official lending and controlled by the Chinese government. The main creditors are state-owned banks, and a variety of state-owned enterprises. Official creditors such as the World Bank have typically lent at concessional, below-market interest rates and longer maturities, while China tends to lend on market terms and at shorter maturities, and the loans are often backed by collateral, meaning that debt repayments are secured by revenues, such as those coming from commodity exports or by giving the creditor the right to attach the profits of state-owned enterprises (see e.g. Horn et al. 2019).

The nature of Chinese lending is obscure since a major part of China's lending is "hidden" – meaning that neither the IMF, the World Bank, nor credit rating agencies have valid data coverage and a general overview. Moreover, the Chinese government does not release data on its lending activities abroad and is not a member of any prominent creditor organizations such as the Paris Club or the OECD (see e.g. Massa 2011).

The debtor countries also tend to have an inadequate grasp of how much they have borrowed from China and under which conditions, so the data coverage is patchy on both the creditor and the debtor side. This is the result of China's strategy to avoid lending credits bilaterally and directly to governments. The bulk of China's overseas lending takes place via and to Chinese state-owned enterprises, so the loans remain within the Chinese financial system, while debtor countries rarely collect data on debt owed by state-owned companies (see e.g. Hurley et al. 2018). The transparency problem is exacerbated by the fact that loans from China to other countries are often processed in tax havens and offshore financial centres such as Hong Kong or Macao.

China's overseas lending strategy is also tailored and differs depending on whether the recipient is a developing or an advanced and higher middle-income country. Instead of direct loans, advanced and higher middle-income countries often receive portfolio investments via sovereign bond purchases of the People's Bank of China. Another important feature of China's lending to advanced economies are short-term trade credits. These trade credits are extended by a large variety of state-owned and private corporations, mostly in the form of advances to foreign importers of Chinese goods (see e.g. Horn et al. 2019).

During the last Eurozone crisis, the capital via sovereign wealth funds (SWFs) became particularly attractive for EU countries. Italy, for instance, turned to cash-rich China, which made significant

purchases of Italian bonds and investments in strategic companies. Another, even more striking example is Portugal, where Chinese inflows turned the country into one of the EU's largest per capita recipients of Chinese capital (see e.g. Tavares da Silva et al. 2020).

The current Covid-19 crisis, and the economic crisis triggered by it, is another opportunity for adversaries to increase the economic dependence of European countries and to foster polarization within the Union, if the EU and its Central Bank are unable to respond to and mitigate the economic consequences of the pandemic.

The large amount of SWF investments in a particular country also increases the threat of disinvestment as a tool of influence. An announcement about the possible withdrawal of investments from a particular market is a viable instrument to apply pressure on other countries.

The obscure nature of Chinese overseas lending creates a significant hidden debt problem in many countries. Moreover, incomplete data on countries' overall debt poses challenges for debt management, surveillance work, asset pricing and financial risk assessments. These challenges undermine the role of international institutions and official creditors such as the IMF and the World Bank in the event of a financial crisis. Unlike Chinese lending, IMF lending is transparent, and it is usually conditioned on the aim to improve national policies. If a nation indebted to China turns to the IMF, officials should be aware that any funds the IMF disburses may be used to pay another official creditor, China, rather than used to blunt market strains (see e.g. Horn et al. 2019).

Foreign direct investment (FDI)

Foreign direct investment (FDI) has been one of the key drivers of globalization and is generally regarded as beneficial for the host countries to which FDI flows are directed, especially in developed countries and when physical and local human capital is created. However, FDI often comes with strategic aspects in order to bolster political and security interests. By acquiring strategic assets or merging with large European enterprises, especially with companies with government ties (such as so-called 'national champions', large companies often historically owned by the state, or providers of public goods such as electricity), actors not only gain wide access to European markets but also connections and relations to political power which, in turn, may ensure backing and protection from the government for supported projects.

In this context, taxation can play a serious role in gaining substantial economic leverage. By using weak regulations and an opaque business environment, foreign companies with close ties to the state can become major investors in the domestic economy, and great contributors to national budgets in terms of tax revenues. This kind of leverage incurs a considerable risk of external manipulation. Tax revenues can be withheld during moments of financial and political weakness to challenge the state's financial solidity and liquidity and accelerate a cash-flow crisis (see e.g. Conley et al. 2016).

It is widely held that the origin of financial flows and the ultimate beneficial ownership of companies operating in Europe are often complex. This has consequences for the accuracy and transparency of FDI data, as the presence of actors responsible for hybrid threats can be concealed – meaning that obscuring ownership chains and transferring profits out of the reach of tax authorities and financial intelligence may lead to a situation where these actors could bypass EU regulations and laws. This has been the case particularly in the energy sector, where Russian state-owned companies have striven to avoid ownership requirements by concealing the ownership chains (see e.g. The European Centre of Excellence for Countering Hybrid Threats 2019).

As many European companies have shifted their production to Russia and many foreign banks in Russia generate large profits, FDI can also function the other way around. Outbound investments from countries where FDI inflows are high may serve as an influence to confuse governments and private interests – meaning that large companies' long-term business relations with authoritarian regimes sometimes have a tendency to soften their governments' approach towards these regimes. Implications can be observed in Europe, where some countries have long called for a relaxation of EU sanctions imposed on Moscow over Russia's annexation of Crimea in 2014.

Sanctions

A better understanding of the FDI dynamics is important, as it also has political consequences. As mentioned above, sanctions have become an increasingly central element of the EU's and Western liberal democracies' security policy and deterrence toolkit.

However, the logic of FDI is twofold and large outbound investments from countries where FDI inflows are high can be counterproductive – meaning that sanctions will boomerang back and cut both ways, possibly provoking a domestic lobbying reaction against the sanctions by a country's own businesses.

This was demonstrated in 2019 when the US Treasury Department introduced its sanctions targeting oligarch Oleg Deripaska's aluminium giant Rusal and other Deripaska companies. As a result of the introduction of sanctions, it threw the international metals market into disarray and threatened to cause hundreds of millions of dollars in losses for leading US investment banks, since they had to mark their investments in Rusal's stocks and bonds down to zero. As the significance of the sanctions rapidly became clear, the US lifted them completely.

While not done purposefully, the sanctions imposed by the West in 2014 targeting Russia also exerted a powerful influence over the development of a more robust and durable state-directed capitalism model in Russia and reshaped the country's relationship with the global economy. As a result, it seems that Russia has built a system that is less vulnerable to external pressure, and the effectiveness of the sanctions remain questionable in this respect (see e.g. Connolly 2019).

Sanctions are also becoming increasingly personal. However, it is not only the EU or the US that have the ability to introduce sanctions. Authoritarian states may follow Western practice and target high-level individuals with extensive personal business networks and governmental connections in order to cause distress to Western businesses (see e.g. Borchert 2019).

Rivalling model: Authoritarian state capitalism

Democratization and globalization have been the two obvious roads to economic success in the Western world. Even though neoliberal capitalism has been a prevalent model for creating economic growth and increasing prosperity and the standard of living, its role is no longer considered self-evident. Authoritarian regimes, namely China and Russia, regard the liberal model as an obsolete system and state-directed capitalism along with state-owned companies as a new sustainable model – meaning that this redesigned, new concept of capitalism is considered to function more effectively. An increasing number of emerging powers are now taking steps to emulate this new form of state-directed capitalism (see e.g. Borchert 2019).

However, as authoritarian state capitalism is increasingly seen as a viable alternative, it creates an asymmetric situation in the West, and especially in the European Union, which leans on the principles of free market-based economies. The restrictions that European investors face in China, such as difficulties in moving capital back from the country, forced technology transfers and challenges to intellectual property rights, hamper EU companies' room for manoeuvre in Chinese markets, whereas China's entry into the EU market is effortless in accordance with the EU's principles and values (see e.g. Leonard et al. 2019).

There is evidence that political disintegration appears to follow economic integration in authoritarian regimes, since democratization and the opening up of international markets may lead to separatism and the dispersion of large states, as was the case with the collapse of the Soviet Union (see e.g. Alesina et al. 2003). However, this has not been the case in China, mainly due to the state-directed capitalism. In fact, vast economic gains have only legitimized the Chinese Communist Party, which President Xi Jinping believes is central to maintaining economic stability and enabling China to dominate technology-driven industries.

Trade openness and international economic integration are linked to the size of states. In a world characterized by trade barriers, the size of a country determines the size of its market – meaning that the market size is equal to its population and territory. On the other hand, with perfect economic integration and no trade barriers, market size and country size are not correlated, as every country is able to trade in a global market. Hence,

small countries can benefit from free trade more in relation to large countries (see e.g. Alesina et al. 2003). From the economic point of view and in accordance with the principle of comparative advantage, which is a foundational principle in the theory of international trade, it can be said that all actors, at all times, can derive mutual benefit from cooperation and voluntary trade. In other words, trade should be a win-win situation.

However, China is taking advantage of the WTO and Western free market-based economies. China promotes its exports while remaining comparatively more closed to foreign goods, making it more difficult for companies from other countries to do business in China. Nevertheless, the situation is even worse when it comes to inward FDI. As a result, the US is increasingly turning inwards and indicating signs of protectionism. Gains from trade will not accrue to all partners when one of the largest is engaged in such market-distorting behaviour.

State subsidies for enterprises/state-owned enterprises

The Western liberal model has leaned on free capital flows and minimal state intervention. The European Union Treaty on the Functioning of the European Union[1] generally prohibits state aid unless it is justified on the grounds of general economic development, although the economic downturn and severe liquidity problems experienced by large European enterprises as a result of the Covid-19 pandemic have led to a temporary relaxation of the state-aid rules.

Authoritarian regimes' custom of subsidizing their companies in order to enhance their access to credit and international markets distorts the level playing field (see e.g. Leonard et al. 2019). As a consequence, these state-owned companies, often with close ties to political power, can gain influence over the economy and technology in target areas.

By operating with lower prices due to a better cost base and owning factitious low cost of capital as a result of state support, it is possible to transform the supported enterprise or business cluster into a dominant actor in the target country's economy. The establishment of a state-supported dominant actor may entail both legal and illegal activities, such as long-term supply contracts conducted on general market terms, loans provided below market interest rates, corruption, or even being handed confidential market information by intelligence services (see e.g. Klus 2018).

Increased political and economic dependence can be used to advance geo-strategic objectives, as demonstrated in Ukraine prior to the annexation of Crimea, where Russian-supported companies managed to achieve almost monopolist positions in many Ukrainian economy sectors.

Flow control

Flow control rewrites globalization. It is a plan to take control of global logistic chains, namely being the owner of the main part of the global value-added chains from production to transport. Along with goods and commodities, flow components include capital, data and information, people and services that move in all five operational domains (see e.g. Borchert 2019).

Strongly associated with this is the regulation of data and information flows, fundamental inputs into the financial services industry and into strategic interests. China has developed a technological base where the state has control over the flow of information. An EU financial system reliant on foreign technology can result in sensitive data ending up in the hands of foreign actors.

European societies rely on traded goods and on tech systems, highly inter-linked with critical infrastructure. The EU has relied on the multilateral trading system, which has drastically reduced its effectiveness. The nature of globalization is changing. Flows across nations are fundamental to most economies, but even more so to smaller ones. If flows become conditional on political support, the current level of connectivity can become toxic, as trade increasingly becomes less free.

1 Treaty on the Functioning of the European Union - Part three: Union policies and internal actions - Title vii: Common rules on competition, taxation and approximation of laws - Chapter 1: Rules on competition - Section 2: Aids granted by States - Article 107 (ex Article 87 TEC) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:12008E107

The Communist Party of China has undertaken a mission to implement the "Chinese dream" and the "great revival of the Chinese nation". The fulfilment of this mission is a long-term ambition but the Communist Party has already stated that the power of the Party is not only an aspiration and a matter for the political system of China, but rather that the entire world will enter the "Chinese reign" (see e.g. Kallio 2018).

As empires expand, the management of a distant and heterogeneous population is challenging. However, annexations are no longer the only viable option for conquering the world. Along with globalization, flow control has become an essential instrument for marginalizing the Western liberal world.

In order to control the supply chains and in accordance with the Made in China 2025 ambitions, China's manufacturers are increasingly moving towards finished products instead of intermediate goods that other countries could use to assemble goods. This is made possible through taxes and quotas that have restricted other countries' access to Chinese minerals and other raw materials, giving Chinese companies an advantage (see e.g. Fung et al. 2013). Meanwhile, the Russian economy is still too heavily dependent on raw materials, and oil and gas are a major source of income for the federal government.

The Belt and Road Initiative (BRI)

In order to enable China's control of global supply chains and to expand the power and influence of the Communist Party, the Belt and Road Initiative (BRI) has become the largest infrastructure project in the modern world and will encompass an area comprising the majority of the world's population, energy resources and global GDP (see e.g. Greeven 2020).

However, China's ambitions are not only economic, and strategic geopolitical objectives are often brought to light when discussing the implications of BRI. There is growing concern about the increased economic ties to China in the Western world, and the consequences for traditional political alliances if business relations with China are prioritized over security and ideological ties.

In accordance with the mission, the involvement of European ports will be key in acquiring ownership of the bulk of the global value-added chains, including the BRI maritime component – the Maritime Silk Road. As Chinese investments in European seaports have increased rapidly in recent years, so have statements by European politicians and policymakers that regard Chinese economic activities in European ports as harmful. Port investments as a part of the general economic dependence of EU member states could influence their foreign policy and thus affect the overall ability of the EU to respond to geopolitical challenges.

However, it is not only the investments in European ports that are distracting. Shipping companies have a significant role as they can direct their own ships to terminals and ports of their interest. This is possible as several European container terminals are owned by shipping companies. Moreover, the capacity for deep-sea container shipping is somewhat concentrated and the rather small number of major shipping firms are increasingly able to direct cargo flows towards or away from individual ports. As a result, the power of the port authorities has decreased. In contrast, shipping companies can use the leverage to pressure ports to lower their fees or to invest in infrastructure upgrades (see e.g. Van der Putten 2019).

Global value chains

The ongoing Covid-19 crisis has already thrust the fragility of the modern financial system, markets, global manufacturing and supply chains into the spotlight. To date, the pandemic has highlighted the fact that, based on the just in time (JIT) delivery concept, inventories are already deliberately minimized. In the case of a major disruption of market-guided logistical systems such as the current pandemic, reserves near the user end are scarce. Globalization means longer delivery distances for many goods. Few countries are still self-sustaining in terms of supplying goods to ensure a basic standard of living.

Global value chain disruption resulting from the pandemic raises the question of how global value chains will be structured after the pandemic in a situation of increased geopolitical tensions.

During the pandemic, or even prior to it, attention was paid to the possibility of diversifying suppliers and relocating industrial activities from

China back to domestic areas. This has happened for two reasons in particular. The first is related to geopolitics as China's authoritarian capitalism and economic ambitions are increasingly connected to national security goals. The second concerns the question of the comparative advantage of the Chinese economy, which is evolving as China's manufacturers are increasingly moving towards finished products instead of intermediate goods that other countries could use to assemble goods. This is one of the reasons why China has been so successful. If its production processes were the same as they were 30 years ago, it would be a very backward economy.

The possible shift of supply chains away from China is unlikely, however, for several reasons. First, the options of where to move the supply chains are decidedly limited as the requisite technology, skills and a similar cost basis are needed. Some countries have taken actions to move manufacturing facilities away from China, but this has turned out to be difficult. Moreover, after the pandemic, many companies will be starved of cash and may not be able to move away from China to invest in other countries in an abrupt short-term manner.

Certainly, it would be possible to relocate some industrial activities back to domestic areas. Yet moving the entire supply chains, including skillsets, cost basis and technology would prove extremely challenging as the systems are based on the market economy and companies are constantly looking for lean solutions to cut costs. Furthermore, supply chains need to be examined from the perspective of where the market is. Over the coming decades, the largest and most dynamic consumer markets will be in China.

Although the discussion on the need to diversify supply chains and relocate industrial activities to avoid a situation where all one's eggs are in the same basket is welcomed, the current Covid-19 crisis has demonstrated that the place where the risks might be controlled most effectively and rapidly is China. Even if more regionalized and diversified supply chains reduced risks, China would retain considerable competitive advantages in many areas, such as electronics and machinery and equipment manufacturing. It cannot be replaced, at least not in the near term. Clearly, China's role in the global supply chains will shift. This is something that has been happening for a long time, with a large number of low value-added manufacturing jobs being transferred to neighbouring countries. The comparative advantage of the Chinese economy has always evolved and although some relocation might take place, the majority of global supply chains will remain in China since it is largely a matter of economies of scale (see e.g. Borchert 2020). However, a strategic assessment is needed to determine the sectors and industries that are critical for national emergency supplies.

FinTech / Dual-use technologies

Financial technology (FinTech), referring to an innovative information and automation technology in financial services, aims to compete with traditional financial methods in the delivery of financial services. The main developments in the application of digital technology have occurred thus far in lending, payment systems, financial advisory services, and insurance. FinTech companies include both start-ups and established financial institutions and technology companies trying to replace or enhance the usage of financial services. The FinTech sector is driven by technologies that are dual-use: blockchain, artificial intelligence, quantum computing and cloud computing.

By definition, FinTech is another field of potential hybrid activity and the connection between the financial sector and security challenges is clear. It is a new technology that opens up opportunities for new business, and it is a field that every government wants to protect and develop. However, new technology could also be used by adversaries if oversight and resilience are weak.

Currently, FinTech companies are relatively small compared to traditional banks, but nonetheless they are a part of the system and can have an influence if a national market is small or has poor oversight by regulatory bodies. Given the current circumstances in the EU economy, FinTech could provide outside actors with the means to exert an influence on the markets as many businesses would be looking for "quick and cheap" capital. Hence, there is the potential for disturbances and hybrid threats.

It remains to be seen whether the current crisis will change the way we handle our financial services, herald a move towards wholly digital solutions, and pave the way for new payment systems with completely digital currencies. Will the big technological companies lead the way and open up their virtual payment systems?

FinTech can also provide avenues for illegal activities such as terrorism financing and money laundering. Both can be used by adversaries to gain influence or to disrupt the financial services or economy of a target state. Hence, it is important to ensure that community-wide regulation is put in place and sufficient resilience built to prevent such activities. Financial regulatory bodies need to work closely with security services to detect such activities and provide the necessary advice for decision-makers in order to protect financial systems from such hostile activities. The challenge is to develop a regulatory framework that would allow FinTech companies to develop and to contribute to the economy, while preventing any illegal activity or hostile influence within the financial system.

Banks, as well as Visa and MasterCard, still dominate the market for transaction payments, but payment innovations often emerge from non-banks. New Chinese payment systems such as Alipay and WeChat and the Russian MIR are striving to gain a foothold in European markets. It must be kept in mind that trading with Russia and China might include preconditions regarding these new payment systems and adaptions to their standards.

The significance of the security implications of these new payment systems should not be underestimated due to the fact that the owner of the above-mentioned payment systems can exclusively track all the data and information moving in the system – meaning that no outsiders, such as Western intelligence services, can access their data and information.

Money laundering

Money laundering is the most blatant use of the financial system as an enabler of criminal activity, often involving an exchange of influences and the concealment of information involving political and private actors, namely through terrorism financing.

Although money laundering and corruption are criminal activities in and of themselves, they can also be used as a weapon against the financial system of a country, and hence there is a close link between money laundering and national security. Dirty money could be used to finance organized crime, destabilize governments, and erode the integrity of a country's financial institutions.

Money laundering can often be associated with proxy actors and seen as a way for foreign states to act through third parties in order to influence, interfere in or conceal its activities in another state, with the aim of producing negative results or advancing the ability to do so when desired.

Recommendations for building resilience

FDI regulation

In recent years, awareness of the blurring of the line between the strategic and economic interests of foreign actors has increased. Investments in individual EU member states have been identified as possible vehicles of political influence, carrying national security risks from which the FDI Screening Regulation resulted. Yet while it incentivizes information-sharing and coordination, it still ultimately falls to the member states to determine whether a transaction is approved or stopped.

While EU prohibition is not possible, fragmentation will remain and individual countries might be gateways to investments with negative security repercussions for other member states. A common approach is suggested whereby the European Commission could make a proposal on prohibition and the Council would decide by qualified majority (see e.g. Leonard et al. 2019).

Other regulatory tools to 'level the playing field'

The EU must develop tools to fight the unfair advantage that foreign enterprises have as a result of state support, and in that way curb the possible strategic interests of foreign states. Competition law can in some instances be adapted to address the issue, given state-owned enterprises possess a de facto level of market power, since they are neither profit maximizing nor resource-constrained. Market guidance and sanctions and remedies are part of this toolkit (see e.g. Heim 2019). Dual-use

technologies have been identified as a topic on which simple selection based on cost is not advisable in the context of public procurement.

Economic sovereignty

The FDI Regulation and other tools are a step in the right direction, but insufficient as such. Strategic sectors need to be economically sustainable otherwise they might be compelled to accept foreign investment even though it would come with malign interests.

Economies can rely on the open economy and on global value chains, while paying attention to incorporating security concerns into economic policy. The offensive angle is to make the economy stronger and more competitive, to the extent that it is never in a position where it must compromise strategic priorities for short-term economic gains.

However, achieving such a goal, particularly for countries with historical macroeconomic imbalances and structural problems, is not easy. Even though EU countries do not perceive budget constraints on other member states as a potential source of EU-wide security concerns, solutions are difficult to come up with. Nonetheless, it is worth noting the use of EU Structural Funds during the financial crisis to sustain public investment in those countries most affected. Although such funds were scarce and couldn't provide an alternative to Chinese capital in many strategic assets, it serves as an example of a community-level response where countries' vulnerabilities could be appropriately addressed.

An important sector-specific question concerns the extent of the resilience of the EU's technological base. The question refers not only to resilience to external actors that might have state support, but even under 'fair' market conditions, given the comparative EU disadvantages vis-à-vis other countries in terms of entrepreneurial base, research and innovation, and knowledge creation in high-tech sectors. The EU should not aim for technological independence in an open interconnected economy, but ought to make strides in some key generic technologies, particularly digital networks, cloud computing and artificial intelligence (see e.g. Leonard et al. 2019).

Data regulation

The EU might not be able to rely on internal players for fundamental network elements such as cloud computing, either due to the high costs for business and consumers, or to the absence of high-quality solutions as the technology base is strengthened. In the meantime, it must develop efficient, enforceable regulations on the use of data by companies operating dual-use technology, and on their independence from national political actors.

Anti-money laundering (AML)

Stricter oversight of financial transactions is necessary to tackle money laundering. In late 2019 and early 2020, the momentum existed for such policies, with proposals by member states for a centralized AML supervisor with EU-wide authority, and the European Commission signalling its commitment to achieving a comprehensive and effective framework to prevent criminals from laundering the proceeds of their illicit activities and from terrorism financing in a February 2020 roadmap (see e.g. European Commission 2020). Such avenues must be pursued in the quest for an effective mechanism, for example in the form of a new European AML Authority (see e.g. Kirschenbaum et al. 2018).

PART II: The financial system as a target of disturbance

A financial system, including financial institutions, markets, financial instruments and services, is essential for the minimum operations of a state. Hence, an attack against such a system can have enormous destabilizing effects and severely threaten the functioning of every industry. The interconnectedness of stocks, money, commodity markets and bonds means that when one suffers, other markets will react accordingly.

As a consequence, trust in financial markets is essential. Without trust, financial markets cannot function efficiently. However, with trust comes the possibility to exploit it in hybrid threat terms, whether through disinformation or a concrete attack on a banking system, increasing civic unrest, decreasing trust in the financial markets, precipitating bank runs and increasing the likelihood of an economic crisis.

An attack on a bank, investment fund, telecommunications/ATM network, SWIFT, or the central banks would represent a direct hit against the financial services system, and the ensuing damage could be substantial. Credit card and other payment systems could fail across nations, online banking could become inaccessible, and cash, payments and reliable information about bank accounts would be unavailable. Banks could lose the ability to transact with one another during a critical period of uncertainty and all parts of society would be affected.

Along with increased digitalization, cyber attacks against publicly listed financial services companies, as reported in the media, are on the rise. Cyber attacks affect all types of entities, with the year to July 2019 registering notable attacks on numerous public institutions – public agencies from Spain, Germany, the UK, Finland, Lithuania, Bulgaria, and Croatia – and on universities and international organizations (see e.g. Demertzis et al. 2019).

Large financial institutions are well aware of cyber risks and have built back-up systems and taken measures to reduce vulnerabilities. Yet there are a number of reasons why the current level of protection might be insufficient from an EU perspective (see e.g. Demertzis et al. 2019). However, unlike the anticipated man-made intrusions, a hybrid operation may be well prepared (with intelligence and intrusion completed before action) and sufficiently resourced to overwhelm the system's defences and cause devastation. The effect would be even more devastating if coordinated hybrid operations were simultaneously executed through many parts of the critical infrastructure and supply chains (see e.g. Savolainen 2019). After the crisis, recovery would take time, especially if the data were corrupted, manipulated or rendered inaccessible.

Risks/Vulnerabilities

Increased digitalization

In the modern world, almost all financial activities are conducted in a digital format and hard, real currency is losing its importance. The increased digitalization of the financial system has highlighted cyber vulnerabilities, where distant actors interfere with national systems, often anonymously. To the extent that digitalization increases efficiency by decreasing redundancies, it also makes systems more vulnerable. In a digitalized world, vulnerabilities can be dormant for long periods and be exploited at a distance, thwarting attribution and making it an excellent instrument in the hybrid toolkit.

Cybersecurity as a part of national security

The fundamental source of risk to the EU financial system in this context is that it is highly integrated,

while security policies remain more strongly national. Financial requirements fall to the ECB, yet security issues such as a cyber attack on a bank fall to the national security authorities. There is not enough alignment between the ECB and national authorities. Although the attacks are communicated to the ECB, there is little information flow from the ECB to the individual institutions. There is no official sharing of information among private players regarding attacks and defence mechanisms, despite the ECB having the information to act as a mediator.

Lack of coordination

The challenge is amplified by the lack of co-ordination. Although there are guidelines on the cyber protection of financial institutions, there is no uniformity in the regulation. The level of protection most likely differs substantially between different actors. Due to the extensive financial integration, an attack on a member state can have considerable cascading effects across the EU financial system.

Insufficient systemic perspective

Due to an insufficient systemic perspective, cyber attacks are largely considered in a typical operational risk framework – meaning that they are treated as actions by mostly private, criminal actors, not as a part of a widespread, co-ordinated hybrid operation against a nation or an institution, targeting either one or possibly all segments of the financial system and other domains. Even if private companies aim to be individually well-protected, there is systemic under-protection.

Externalities

Nor is the incentive structure conducive to protection. Companies have an incentive to hide attacks to avoid financial losses, which also jeopardizes the effectiveness of insurance markets, which might underestimate the cyber risk and reinforce under-protection. Society at large benefits from the increased protection of private players, in terms of data privacy and security, and companies are unwilling to bear the cost of additional protection if it outweighs their private benefits.

Recommendations for building resilience

The EU will not have nation-state capabilities, and hence it should concentrate on reducing vulnerabilities and building resilience as opposed to retaliation. Building back-up systems and cybersecurity and increasing awareness of hybrid threats are important but insufficient measures.

Information exchange

Within a jurisdiction, there is scope for increased information-sharing between economists and policy planners as well as private companies and national authorities. Yet, precisely because it remains a security issue, communication between regulators and security agencies of different states is often fragile.

The EU-level security agencies have made some progress in their mandate and competencies, but not nearly enough. A communication hub ought to be established. If successful, a Cyber Information and Intelligence Sharing Initiative (CIISI-EU) would be a step forward and improve the lack of information exchange between central banks and key financial institutions.

Conducting exercises/testing

A very powerful mechanism that can be explored without challenging the competency division of the EU and, if voluntary, without regulation, is the conducting of exercises/testing. G7 testing has considered cyberattacks specifically. The TIBER-EU testing framework, developed by the ECB and the national central banks, simulates real-life attacks on the core financial infrastructure. It can be made compulsory and can simulate EU-wide attacks. Moreover, it is not limited to the financial sector, and can include any industry considered critical. It is important that threat-led penetration testing is conducted in a harmonized way across the EU, avoiding the duplication of work for financial entities and authorities alike.

Macroprudential measures

From a macroprudential perspective, in the case of a crisis, swift actions by the ECB will be needed to ensure that there is liquidity, but also to make sure that it can be properly channelled

to businesses and citizens. Such provisions are yet to be designed, which creates a significant challenge for the EU and the ECB in dealing with the economic crisis resulting from the Covid-19 pandemic.

Data security as a competitive advantage

Another issue to be considered concerns data security as a competitive advantage. In order to incentivize business leaders to internalize externalities, that is, to invest more in cybersecurity for the benefit of national security, data security ought to be presented as a competitive advantage. Indeed, data leaks publicized in the press have substantial negative impacts on the financial returns of companies. The effectiveness of building a layer of awareness cannot be understated: presentations and programmes targeted at business leaders influence behaviour.

Ownership of the financial infrastructure

Ownership of the financial infrastructure is an essential element of national security. In order to be adequately protected, financial infrastructure should be considered critical infrastructure. Yet doing so would allocate control to the member states, overriding the essential progress achieved in economic integration. Ownership must at least be considered from a national security standpoint, as it should coincide with general strategic interests at the national level, which are considered when evaluating foreign investment.

References

Alesina, A. and Spolaore, E. (2003) *The size of Nations*. Cambridge, Mass: MIT Press.

Borchert, H. (2020) Looking Beyond the Abyss. Eight Scenarios on the Post-COVID-19 Business Landscape. HEDGE21 Strategic Assessments (Zolling/Freising: 21 strategies, 2020). Available at: https://www.borchert.ch/content/en/cmsfiles/publications/2004_Borchert_Covid-19_Scenarios.pdf.

Borchert, H. (2019) Flow Control Rewrites Globalization. Implications for Business and Investors. HEDGE21 Strategic Assessment (Dubai: HEDGE21/ALCAZAR Capital, 2019). Available at: https://www.borchert.ch/content/en/cmsfiles/publications/1901_Borchert_Flow_Control.pdf.

Conley, H., Mina, J., Stefanov, R. and Vladimirov, M. (2016) The Kremlin Playbook – Understanding Russian Influence in Central and Eastern Europe. Center for Strategic and International Studies. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf.

Connolly, R. (2019) Russia's Response to Sanctions: How Western Economic Statecraft is Reshaping Political Economy in Russia. University of Birmingham. Cambridge: Cambridge University Press.

Demertzis M. and Wolff, G. (2019) Hybrid and cybersecurity threats and the European Union's financial system. Policy Contribution Issue nº10, September 2019. Available at: https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf.

European Commission (2020) Money laundering & terrorism financing action plan. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering.

Fung, K. and Korinek, J. (2013) Economics of Export Restrictions as Applied to Industrial Raw Materials. OECD Trade Policy Papers, No. 155. Paris: OECD Publishing. Available at: http://dx.doi.org/10.1787/5k46j0r5xvhd-en.

Greeven, M. J. (2020) Globalizing Innovation Ecosystem, Entrepreneurs and the Digital Silk Road. In De Cremer, D., McKern, B. and McGuire, J. (Eds.). The Belt and Road Initiative – Opportunities and Challenges of a Chinese Economic Ambition (pp. 236-258). New Delhi: Sage Publications.

Heim, M. (2019) How can European competition law address market distortions caused by state-owned enterprises? Policy Contribution Issue nº18, December 2019. Available at: https://www.bruegel.org/wp-content/uploads/2019/12/PC-18_2019-181219.pdf.

Horn, S., Reinhart, C. and Trebesch, C. (2019) China's overseas lending, Kiel Institute for the World Economy, Kiel working papers 2132. Available at: https://www.ifw-kiel.de/publications/kiel-working-papers/chinas-overseas-lending-12820/.

Hurley, J., Morris, S. and Portelance, G. (2018) Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective. Center for Global Development, Policy Paper 121, March 2018. Available at: https://www.cgdev.org/sites/default/files/examining-debt-implications-belt-and-road-initiative-policy-perspective.pdf.

Kallio, J. (2018) Xi Jinping thought and China's future foreign policy: Multipolarity with Chinese characteristics. FIIA Briefing Paper August 2018. Available at: https://www.fiia.fi/julkaisu/xi-jinping-thought-and-chinas-future-foreign-policy-4?read.

Kirschenbaum, J. and Véron, N. (2018) A better European Union architecture to fight money laundering. Policy Contribution Issue nº19, October 2018. Available at: https://www.bruegel.org/wp-content/uploads/2018/10/PC-19_2018-241018_.pdf.

Klus, A. (2018) Adversary-Controlled Economic Assets as a Threat to National Security. *Small Wars Journal*. Available at: https://smallwarsjournal.com/jrnl/art/adversary-controlled-economic-assets-threat-national-security.

Leonard, M., Pisani-Ferry, J., Rebikova, E., Shapiro, J. and Wolff, G. (2019) Redefining Europe's economic sovereignty. Policy Contribution Issue nº9, June 2019. Available at: https://www.bruegel.org/wp-content/uploads/2019/06/PC-09_2019_final-1.pdf.

Massa, I. (2011) Export finance activities by the Chinese government. Directorate-General for external policies of the Union. Briefing Paper. Available at: https://www.europarl.europa.eu/RegData/etudes/note/join/2011/433862/EXPO-INTA_NT(2011)433862_EN.pdf.

Savolainen, J. (2019) Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)? Working Paper 2019. The European Centre of Excellence for Countering Hybrid Threats. Available at: https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Working-paper_WMDivers_2019_rgb.pdf.

Scholvin, S. and Wigell, M. (2018) Geo-economic Power Politics: An Introduction. In Wigell, M., Scholvin, S. and Aaltola, M. (Eds.). *Geo-economics and Power Politics in the 21st Century – The Revival of Economic Statecraft*. Routledge.

Tavares da Silva, J. and Pereira, R. (2020) China and the Portuguese Atlantic: The BRI's Last Puzzle Pieces. In Leandro, F. and Duarte, P. (Eds.). *The Belt and Road Initiative – An Old Archetype of a New Development Model*. Palgrave Macmillan.

The European Centre of Excellence for Countering Hybrid Threats (2019) Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats. Available at: https://www.hybridcoe.fi/wp-content/uploads/2019/10/Nuclear-Research-Report-2019_web.pdf.

Van der Putten, F.P. (2019) The relevance of the Maritime Silk Road for the Netherlands. Clingendael Report. Netherlands Institute of International Relations. Available at: https://www.clingendael.org/sites/default/files/2019-12/Report_European_ports_and_Chinese_influence_December_2019.pdf.


Hybrid CoE