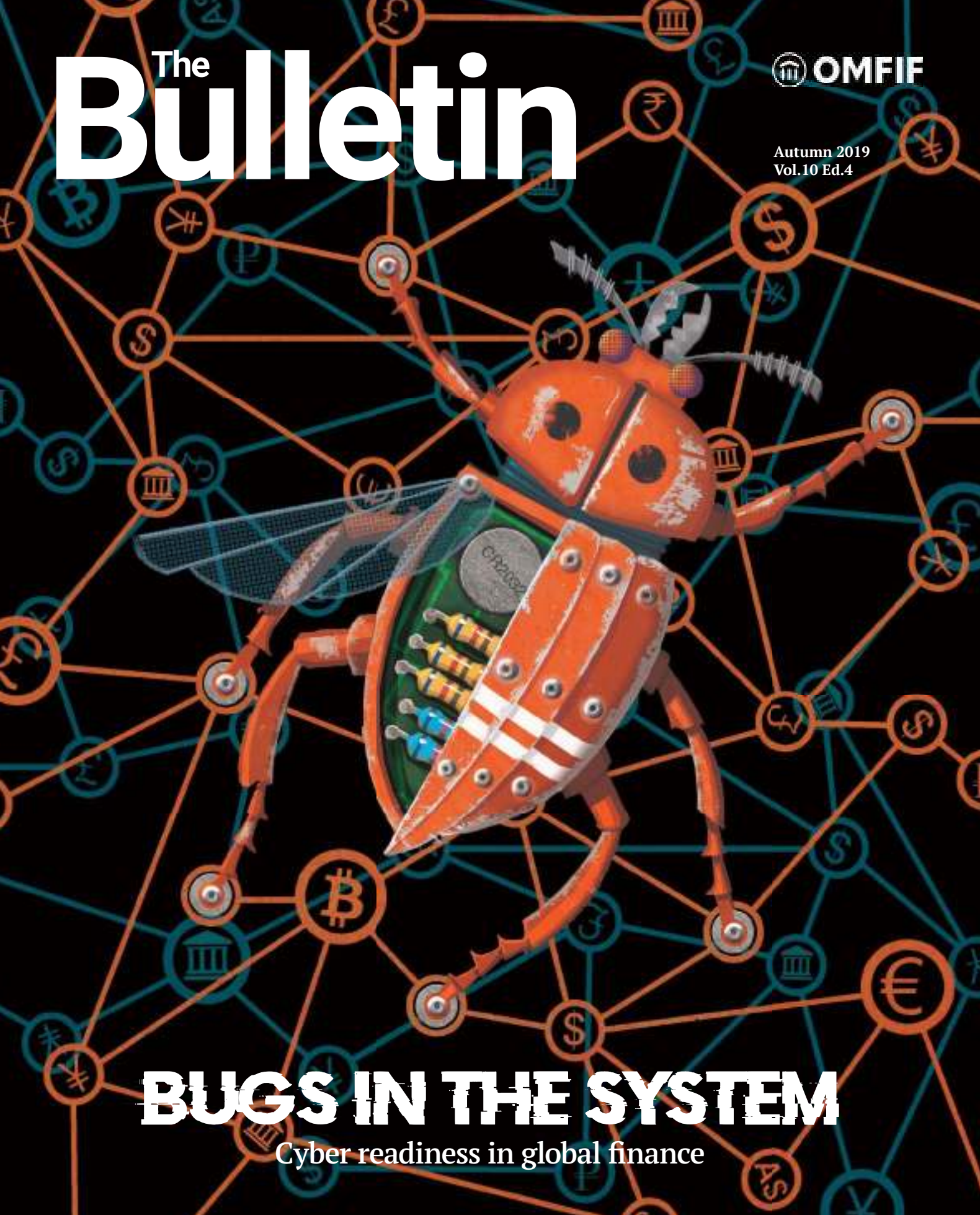
# The Bulletin

OMFIF

Autumn 2019
Vol.10 Ed.4



# BUGS IN THE SYSTEM

## Cyber readiness in global finance

# Invested in the future.

## You don't thrive for 230 years by standing still.

As one of the oldest, continuously operating financial institutions in the world, BNY Mellon has endured and prospered through every economic turn and market move since our founding over 230 years ago. Today, BNY Mellon remains strong and innovative, providing investment management and investment services that help our clients to invest, conduct business and transact in markets all over the world.

**To learn more, visit bnymellon.com**



BNY MELLON

The Bulletin
Autumn 2019 Vol.10 Ed.4

6



## Cover: Cybersecurity



## In conversation



## Money matters



## Worldview




*Cover illustration: Andy Bridge*

18



28



## Inquiry

# Dialogue on world finance and economic policy

THE Official Monetary and Financial Institutions Forum is an independent think tank for central banking, economic policy and public investment – a non-lobbying network for best practice in worldwide public-private sector exchanges. At its heart are Global Public Investors – central banks, sovereign funds and public pension funds – with investable assets of $36tn, equivalent to 45% of world GDP.

With offices in London and Singapore, OMFIF focuses on global policy and investment themes – particularly in asset management, capital markets and financial supervision/regulation – relating to central banks, sovereign funds, pension funds, regulators and treasuries. OMFIF promotes higher standards, performance-enhancing public-private sector exchanges and a better understanding of the world economy, in an atmosphere of mutual trust.

## Membership

Membership offers insight through two complementary channels – Analysis and Meetings – where members play a prominent role in shaping the agenda. For more information about OMFIF membership, advertising or subscriptions contact membership@omfif.org

## Analysis

OMFIF Analysis includes commentaries, charts, reports, summaries of meetings and The Bulletin. Contributors include in-house experts, advisers network members and representatives of member institutions and academic and official bodies. To submit an article for consideration contact the editorial team at analysis@omfif.org

## Meetings

OMFIF Meetings take place within central banks and other official institutions and are held under OMFIF Rules. A full list of past and forthcoming meetings is available on www.omfif.org/meetings. For more information contact meetings@omfif.org

## OMFIF Advisers Network

The 173-strong OMFIF advisers network, chaired by Meghnad Desai, is made up of experts from around the world representing a range of sectors: monetary policy; political economy; capital markets; and industry and investment. They support the work of OMFIF in a variety of ways, including contributions to the monthly Bulletin, regular Commentaries, seminars and other OMFIF activities. Membership changes annually owing to rotation.

OMFIF
Official Monetary and Financial Institutions Forum
30 Crown Place, London, EC2A 4EB
United Kingdom
T: +44 (0)20 3008 5262 F: +44 (0)20 7965 4489
www.omfif.org @OMFIF



**Company Number: 7032533. ISSN: 2398-4236**

# Bugs in the system

With rapid advances in interconnected digital technology have come increasingly frequent and sophisticated cyber attacks on those systems that govern our lives, not least the global economic and financial architecture.

For law-abiding people, digitalisation offers convenience, ease of access and cost efficiency. For the criminally minded, it presents countless openings for large-scale cyber attacks, a hazard that the World Economic Forum considers to be among the greatest global threats.

How policy-makers should respond when confronted with such risks – posed mostly by faceless adversaries and hacker groups – is a subject to which OMFIF pays much attention. Our latest technology-focused report, supported by Citi and written by OMFIF Chief Economist and Director of Research Danae Kyriakopoulou, deals with 'Driving cyber resilience in the financial system', focusing on the role of central banks.

We are pleased to feature in this edition of The Bulletin representatives from two institutions at the forefront of the discourse on cybersecurity. Sabine Lautenschläger, member of the executive board of the European Central Bank, spoke with Senior Editor Julian Frazer about collaborating with other policy-makers around the world, and Tommy Tan of the Monetary Authority of Singapore wrote about the importance of fostering a culture of information sharing. These articles are supplemented by in-house analysis examining the global cost of cybercrime and the culture of secrecy that inhibits deeper discussion about this threat.

The massive size, complexity and interconnectedness of the financial system makes a globally-disruptive cyber attack a matter of when, not if. Public policy-makers must move quickly to fill whatever cracks they can. As François Villeroy de Galhau, governor of the Banque de France, put it earlier this year, 'Our ambition must be as high as the risks to which our evolving and interconnected financial systems are exposed to.'

»1 July, London

## Investing in Indonesia

Perry Warjiyo, governor of Bank Indonesia, and Bambang Brodjonegoro, minister of national development planning, discussed Indonesia's economic outlook and responses to global tensions. They also addressed how best to boost infrastructure investment, overcome perceived regulatory challenges and incentivise public-private partnerships.

»1 July,London

## Brexit and the future of the Conservative party

Greg Hands, Conservative member of parliament for Chelsea and Fulham and former minister of state at the UK Department for International Trade (2016-18), discussed the UK's departure from the European Union and the future of the Conservative party. Topics included the Conservative leadership race, the impact of the party leadership on the different Brexit scenarios, and the long-term impact of parliamentary gridlock on UK politics.

»5 July, London

## Financial market manipulation

Oonagh McDonald, an international financial regulatory expert, author and former Labour party politician, discussed Libor, foreign exchange, gold and silver price fixing scandals. She outlined why the benchmarks should be reformed in the face of rapid technological changes. She also discussed recommendations for regulatory reforms to improve the security of the financial services industry.

»12 July, New York

## Brazilian economic outlook

The Brazilian economy faces a multitude of challenges due to political developments and demands for reform. João Manoel Pinho de Mello, deputy governor for competition, financial market structure and authorisation at the Banco Central do Brasil, discussed Brazil's economic outlook and threats to its financial system.

»15 July, London

## UK leadership race and Brexit

Bernard Jenkin, member of parliament for Harwich and North Essex, outlined why he backed his chosen candidate for the recent Conservative party leadership contest and the prospects for renegotiations with the European Union. He also discussed the likelihood of a vote of no confidence and long-run state of UK politics.

»25 July, London

## Economic and financial diplomacy

As the UK gears up to leave the European Union, Jakob von Weizsäcker, chief economist in the German finance ministry, and Veda Poon, director of international finance in the UK Treasury, outlined how the UK, Germany and EU can build on their economic and financial links.

# The OMFIF Foundation at St. Louis

**A wide-ranging three-day programme with the Federal Reserve Bank of St. Louis, the National Institute of Economic and Social Research and the Olin Business School at Washington University in St. Louis.**

»8 July, St. Louis

## Modelling the macroeconomy in risky times

Advances in macroeconomic modelling centring on interactions between agents in general equilibrium were examined in a preconference workshop organised by OMFIF and the National Institute of Economic and Social Research featuring its NiGEM econometric model.

»10 July, St. Louis

## US interest rate 'insurance' against slowdown

Jim Bullard, president of the Federal Reserve Bank of St. Louis, underlined the need for a cut in Fed interest rates as 'insurance against a sharper than expected slowdown', in a lunchtime interview. Presaging the 0.25 point fed funds rate cut decided on 31 July, Bullard said 'uncertainty about trade issues' was leading to a global growth slowdown.

»9 July, St. Louis

## Assessing priorities for society, politics and economics

A decade after the financial crisis, the Federal Reserve Bank of St Louis and the OMFIF Foundation organised an international gathering to examine themes such as household debt, financial inclusion, sustainable investment and the role of technology in employment and education.

»9 July, St. Louis

## Research and dialogue to strengthen economies

Central bankers should visit communities to better understand economic changes and promote research that can address local challenges, said Raphael Bostic, president of the Federal Reserve Bank of Atlanta, in an interview with his predecessor, Dennis Lockhart, OMFIF Foundation board member.

»28 August, Frankfurt

## Navigating the challenges low interest rates

OMFIF and DZ BANK convened a conference bringing together leading policy-makers, financial experts and industry representatives to discuss political and macroeconomic developments in Europe and beyond. Speakers included Frank Scheidig, global head of senior executive banking at DZ BANK, Wolgang Koehler, member of the board of managing directors at DZ BANK, and Joerg Kukies, state secretary in the German federal ministry of finance.

»4 September, New York

## Monetary policy implementation and reserves

In early 2019, the US Federal Reserve announced it would continue to operate in a framework of ample reserves as part of its normalisation strategy. Antoine Martin, senior vice-president at the Federal Reserve Bank of New York, François Haas, chief representative of the Banque de France for the Americas, and Giovanni Majnoni, chief representative of the Banca d'Italia for North America, discussed the monetary policy implementation frameworks, the Fed's current floor system and other related topics.

»18 September, London

## New European financial regulatory landscape after Brexit

In his opening remarks at an OMFIF roundtable on the new European financial regulatory landscape after Brexit, Otmar Issing, former member of the board of the European Central Bank, said the UK's decision to leave the European Union was evidence for some that EU integration had gone too far.

»11 September, London

## Brexit: Impact on Japan-UK trade and investment

The UK has remained of great importance to Tokyo as Japan's 'gateway to Europe'. In February this year, Japan and the EU signed what has been dubbed the world's largest free trade deal, the EU-Japan Economic Partnership agreement. This roundtable addresses the impact of Brexit on Japan-UK trade and investment and the future of London-Tokyo ties as key global financial centre.

»10 September, London

## Economic performance in Chile

In the face of instability in Latin America, the Chilean economy remains one of the strongest in the region, exhibiting solid growth and a healthy investment climate. Topics discussed at this roundtable included Chile's economic outlook, its monetary and macroeconomic policy, as well as regional challenges and opportunities.

»24 September, Oslo

## The future of reserve management

OMFIF and Norges Bank convened a joint meeting in Oslo comprising keynote speeches and panel discussions that addressed recent macroeconomic and financial developments, as well as challenges and opportunities for public sector investment management.

# Agenda

»Tuesday 15 October, New York

## *Global Public Investor* 2019 US launch

**A seminar for the US launch of *Global Public Investor* 2019, the publication devoted to public sector asset ownership and management around the world. The meeting in New York focuses on the key issue of sustainability and aims to share best practice among investors.**

»Tuesday 15 October, London

## City Lecture with Denis Beau

**A City Lecture with Denis Beau, first deputy governor of the Banque de France, on how regulation should help manage risks and capitalise on the opportunities that crypto-assets offer. Beau will outline how regulators can address concerns around data protection and cybersecurity.**

»Friday 18 October, Washington

## Retail central bank digital currencies

**A roundtable with OMFIF and G+D Currency Technology to discuss the implications of central bank digital currencies, how their design would impact monetary policy and financial markets, and some of the challenges facing financial actors.**

»Friday 18 October, Washington

## Absa Africa Financial Markets Index

**Now in its third year, the Absa Africa Financial Markets Index records the openness to foreign investment of countries across the continent. The index is the premier indicator of the attractiveness of Africa's capital markets, which can be used by investors and asset managers around the world.**

»Saturday 19 October, Washington

## Developing sustainable capital markets

**The eighth OMFIF and DZ BANK joint breakfast at the annual International Monetary Fund-World Bank Group meetings. This year's panel concentrates on priorities in the development of sustainable capital markets, green bond issuance and low carbon investments.**

»Sunday 27-Tuesday 29 October, Shanghai

## China Finance 40 Forum Bund Summit 2019

**Against the backdrop of accelerating financial opening by China, the Bund Summit has been created to promote open and candid dialogue between the Middle Kingdom and the rest of the world and to facilitate integration and co-operation.**

»Wednesday 6 November, London

## Roundtable with Andrew Bailey

**A roundtable with Andrew Bailey, chief executive officer of the Financial Conduct Authority, to discusss the future of UK regulation as the country prepares to leave the European Union. Topics will include the regulation of digital developments and enhancing transparency of FCA processes.**

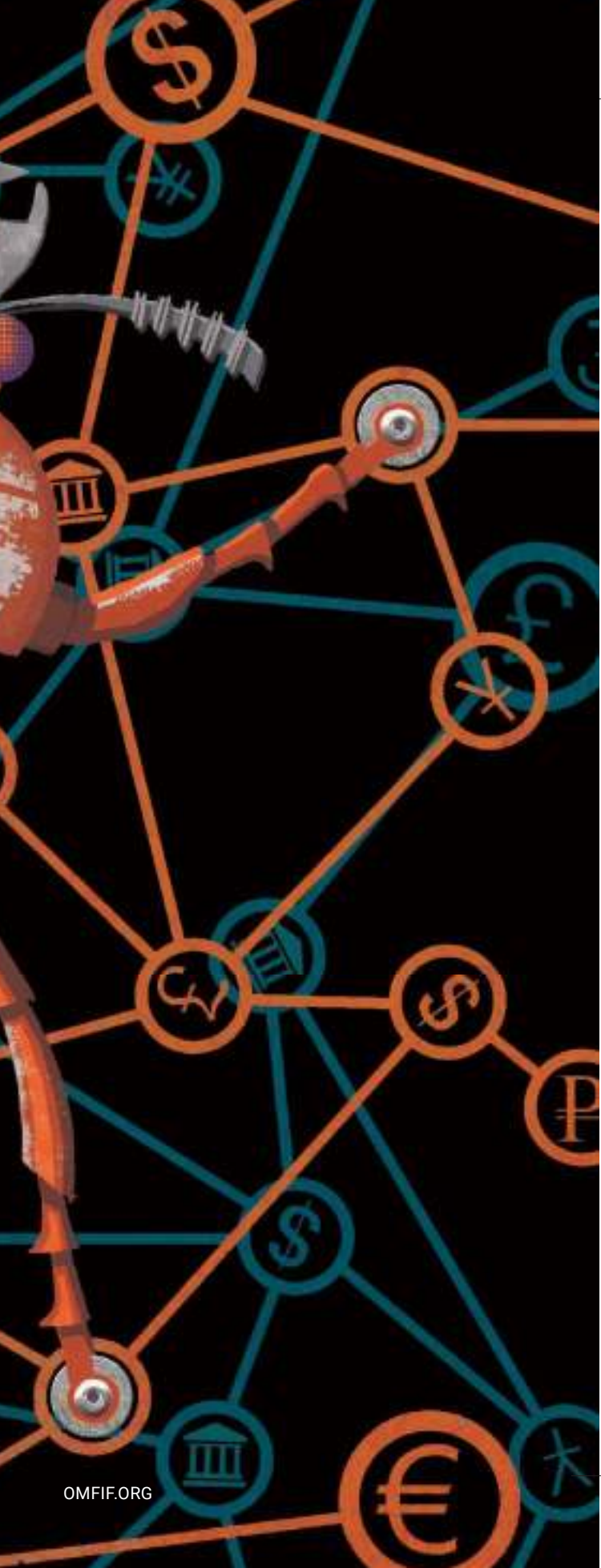
»Tuesday 19 November, Warsaw

## Asset and risk management forum

**A meeting of public sector reserves and asset managers to discuss challenges and opportunities for investment management. The forum focuses on recent developments in reserve management strategies in establishing a green investment agenda.**

For details visit omfif.org/meetings


CR2032



# BUGS IN THE SYSTEM

## Cybercrime could cost global economy trillions annually

**Bhavin Patel**
OMFIF

After extreme weather events, failure to mitigate climate change, natural disasters and massive incidents of data fraud, the World Economic Forum this year marked cyber attacks as the fifth biggest risk to society.

The WEF estimates the economic cost from an attack on a single cloud computing provider to be between $50bn-$120bn. To put that in context, 2012's hurricane Sandy inflicted around $70bn worth of damage, while hurricane Katrina wrought in 2005 more than $125bn in damage. The total economic cost of all natural disasters in 2017 is estimated at $300bn – the annual economic cost of cybercrime is thought to exceed $1tn.

Due to the increasing interconnectedness of digital devices and networks, both domestically and across borders, an attack on one or more institutions can have significant cascading effects, which can quickly become systemic. A single-point attack on an intermediary responsible for payments, clearing or settlement could spread to the entire system, leading to widespread outages among payments services.

In 2017 a series of cyber attacks using the WannaCry ransomware, a virus that encrypts user data that is then released following payment, affected manifold systems across the globe.

The total cost of these attacks is believed to have exceeded $1bn. The NotPetya virus followed, wiping data records of targeted systems of many organisations, which cost shipping operator Maersk almost $300m in revenue. Both attacks were suspected to be state sponsored.

Other cyber attacks on critical infrastructure include the disabling of an Iranian nuclear power plant in 2010 and power outages in Ukraine in 2015 following a supervisory control and data acquisition attack. Between 2015-16, a North Korean group hacked Swift payment systems and stole more than $100m from unauthorised payment messages.

The ability of governments to effectively confront these threats depends on robust collaboration in the international community. But to date the regulatory landscape has been fragmented, with limited guidance around response and recovery beyond basic principles. Firm-specific strategies to nullify cyber attacks have included custom detection, response and recovery methods. Individual government-led national strategies, without international collaboration, have increased the divergence of cybersecurity approaches.

## HARMONISING CYBER LAWS

The ideal would be to realise a cyberspace that is open, interoperable, secure and reliable – one that does not sacrifice functionality for security. One way of achieving this admittedly ambitious goal is to establish a set of core principles based on freedom, privacy, property rights and the right to self-defence.

The Budapest convention on cybercrime, drawn up by the Council of Europe at the start of the century, attempted to set global consensus and bring nations together in the development and implementation of cybersecurity programmes. It was the first international treaty seeking to address cybercrime by harmonising national laws, improving investigative techniques and boosting national co-operation.

**THE TOTAL ECONOMIC COST OF ALL NATURAL DISASTERS IN 2017 IS ESTIMATED AT $300BN – THE ANNUAL ECONOMIC COST OF CYBERCRIME IS THOUGHT TO EXCEED $1TN**

Despite having existed for almost two decades, the convention's effect has been limited. Asymmetry in values and differing geopolitical objectives has meant some major players – Russia, China, Brazil and India – have declined to participate. A key issue concerns the convention clause allowing transborder access to stored computer data during cybercrime investigations by the special services of various nations. Russian authorities believe this could undermine their national security and sovereignty. India, however, has said it will reconsider its position.

A regime can only be effective if all major powers participate and accept the relevant provisions. Either the current convention must be improved in a way that attracts more signatories, or a new unifying treaty must be created.

Thus far, bilateral co-operation and regional agencies, such as the European Union Agency for Cybersecurity, have been used by countries to address cybercrime matters internationally. The United Nations Group of Government Experts tried in 2015 to establish an international governmental code of conduct for cyber norms, but failed to reach consensus by June 2017. One way to generate more support for the group's agenda would be to grant it greater official status by adding it as a resolution in the UN General Assembly and allowing all permanent members of the Security Council to be involved in its construction. Despite a UN resolution being nonbinding, it would be a step towards institutionalising cybersecurity standards.

Another suggestion for improving international cyber strategy is for the US and Russia to restart a dialogue. Both countries are crucial to global cyber policy and diplomacy, but disagreements between the two have escalated, manifesting most plainly in the accusations of Russian interference in the 2016 US presidential election.

Cyber rules between the two nations differ. The US is aligned with a group of countries arguing that international law applies fully to cyberspace, whereas Russia is aligned with another group demanding a new treaty tailored to this domain. Washington and Moscow could sign a pact similar to the US-China cyber economic-espionage agreement, which led to a significant drop in the number of China-based attacks on the US, while keeping open the channel for future co-operation.

Another idea could be to be to punish nations that refuse to co-operate in combating cybercrime through different penalties such as travel bans, asset freezes, arms embargoes, capital restraints, foreign aid reductions and trade restrictions. Other proposals include creating a separate independent institution such as an international cyber court that could adjudicate government-level cyber conflicts.

The long-term strategy should be to incorporate cybersecurity legislation into international law. Building better and more inclusive international ties is essential. Doing so will help establish best practice, enable better information sharing on cyber threats, expand and enhance cybercrime legislation, improve law enforcement and judicial co-operation. If policy-makers fail to take concrete steps, the costs of cybercrime to the world economy will continue to spiral. ●

**Bhavin Patel is Senior Economist and Head of Fintech Research at OMFIF.**

# Uniting on the cyber frontier

## Regulators must collaborate to match attackers' speed

**Tommy Tan**
Monetary Authority of Singapore

Central banks have a long history of co-operation during financial crises. In 1930, the Bank for International Settlements was established to foster international monetary and financial collaboration in times of uncertainty. The Basel Committee on Banking Supervision was founded in 1974 by central banks to converge towards common standards, culminating in the Basel Accords.

Financial regulators are often sensitive to shifts in risks and act in concert to maintain the safety and soundness of the financial system they supervise. As the financial threat landscape evolves, cyber attacks have become a growing concern. While the risk is not new, its prominence has heightened considerably. As the internet becomes a ubiquitous and indispensable medium for business and individual interactions, the resultant interconnectedness has made the task of supervising and regulating cyber risks in jurisdictional isolation more difficult.

The impact of a major cyber attack is not very different from that of a physical one. The difference lies in the medium, that is the internet, which allows the attack to be carried out stealthily and at a frequency unparalleled in the physical world. The polymorphic, persistent nature and diversity of threat actors make countering cyber attacks an uphill task.

While every financial institution must establish good cyber hygiene to protect itself against threats, strengthening resilience in silo is not enough. Due to the interconnectedness between institutions' systems and business operations, an attack on a weak link in the financial system could have an adverse impact on other bodies, and bring about a domino effect in the entire system. The WannaCry malware outbreak in 2017 which caused severe service disruptions and financial losses globally illustrates the potential for cyber threats to spread rapidly across organisations, likened to a pandemic.

In August 2019 the Monetary Authority of Singapore issued a legally binding set of cybersecurity requirements for institutions to implement after consultation with the industry. MAS conducts regular exchanges with the banks' and insurers' associations through standing committees on cybersecurity to collaborate on sector-wide initiatives and exchange insights into cyber threats and countermeasures.

However, the fast-changing, borderless and disruptive nature of cyber threats makes it almost impossible for each jurisdiction to deal with them on their own. International standard-setting bodies play an important role in combating cyber threats through greater coordination and collaboration to promote effective regulatory and supervisory practices.

In recent years, different standard-setting bodies have begun to give form to non-financial expectations expounding on cyber resilience. For example, expectations to ensure that critical information technology systems can resume operations following disruptive events were included in the Principles for Financial Market Infrastructures published in 2012 by the Committee on Payments and Market Infrastructure of the International Organisation of Securities Commissions. In 2016, the CPMI-IOSCO published its 'Guidance on Cyber Resilience', the first such document on cybersecurity from by an international standard-setting body.

More efficient mechanisms are necessary to match the speed at which new cyber threats, techniques and vulnerabilities arise. The Central Banks, Regulators and Supervisory Entities Forum was established in July 2018 to address this challenge. Supported by the Financial Services Information Sharing and Analysis Centre, the forum facilitates timely sharing of cyber information between regulators and supervisors.

### THE CLOUD AND CONCENTRATION RISK

Many financial institutions have started exploring the use of cloud computing services, attracted by improved efficiency, security, scalability and cost savings. However, cloud services are not hazard-free. As more companies subscribe to major cloud service providers, concentration risk may emerge.

The use of shared pools of resources hosted in the cloud could expose multiple financial institutions to a common vulnerability that may result in widespread service outages or security breaches. As institutions' reliance on cloud service providers grows and the latter become systemically important, regulators will have to review their supervisory paradigm.

As financial regulators collaborate to establish common rules, build a culture of information sharing and develop strategies to deal with new and systemic risks, a united frontline will emerge on the cyber frontier. Together, they and the institutions they supervise will be able to face mounting cyber attacks and ensure the resilience of the global financial system. ●

**Tommy Tan is Director and Head of Technology Risk Supervision Division at the Monetary Authority of Singapore.**

# Cybersecurity's culture of secrecy

## Lack of reliable data weakening protection

**Julie Levy-Abegnoli**
OMFIF

It took US bank Capital One four months to discover that information about 106m of its customers had been stolen. The breach may never have come to light if not for a whistleblower who alerted the bank in July. The alleged culprit had boasted about her exploits online and posted a description of her loot on GitHub, a social networking platform for software developers. In September 2018, British Airways announced that hackers had stolen the data of 380,000 customers, only to reveal the following month that the number of victims was closer to 500,000.

These incidents illustrate companies' dearth of cybersecurity knowledge. They are also among the few that have been made public. For every cyber attack that is reported, three are not, says a cybersecurity expert from a major technology firm. Many companies fear reputational damage, which is why they are often reluctant to divulge the full extent of security breaches, if at all. As such, reliable data on the impact of cybercrime on the private sector is elusive. The figures that are available tend to come from firms trying to sell cybersecurity products.

**IN A WORLD WHERE DATA HAVE OVERTAKEN OIL AS THE MOST VALUABLE ASSET, IT IS REASONABLE TO EXPECT COMPANIES TO TAKE ROBUST PRECAUTIONS TO PROTECT CUSTOMER INFORMATION**

In a world where data have overtaken oil as the most valuable asset, it is reasonable to expect companies to take robust precautions to protect customer information. It can be hugely embarrassing, and therefore detrimental, for a firm to admit it lacks the necessary measures to safeguard effectively the data it stores, particularly if its business is built on trust, as is the case for banks. The secrecy surrounding security incidents is such that, according to one expert, those brought in to clean up breaches are often subject to confidentiality agreements.

### INTERNAL THREATS

According to insurance group Lloyd's, while companies usually have processes in place to deal with the aftermath of a cyber incident, they lack preventative measures. Most businesses do not invest sufficiently in 'security architecture', which includes firewalls or antivirus software, as well as standards and policies. This can be expensive, especially for small firms. Those that can afford protection struggle to attract workers with the right skills. According to research company Cybersecurity Ventures, by 2021 there will be 3.5m unfilled cyber protection jobs around the world. Because companies lack staff with expertise in cybersecurity, there is no one to train other workers, making these firms more vulnerable to attacks. That explains partly why email, one of the most widely used electronic services, remains attackers' preferred weapon, according to telecommunications giant Cisco.

Hackers are diversifying their methods, aided by the rise in popularity of cloud computing and the 'internet of things'. Cybersecurity threats will only continue to rise as technology develops. Encryption was designed to protect sensitive data online, such as credit card numbers. Ironically, it is also helping criminals conceal their activities, reports Cisco, making it even more difficult for companies to spot security breaches. This only worsens the data scarcity on cybersecurity.

Companies that fail to equip themselves with adequate cyber protections face a hefty cost – up to $5.2tn globally over the next five years, according to consultancy Accenture. This could stem from the price of fixing and managing a security breach, a fall in share price or the loss of customers.

Possible legal penalties for data leaks also entail significant costs. In July, the UK's Information Commissioner's Office handed British Airways a £183m fine, in line with the European Union's General Data Protection Regulation, which came into force last year and applies to all businesses servicing EU citizens. Under these rules, companies having suffered a security breach face fines of up €20m or 4% of their global turnover.

These requirements could perhaps fuel the expansion of the cybersecurity insurance sector. In the US, says professional services firm PwC, the cyber insurance market is worth between $2.5bn-$3.5bn annually, and is expected to grow by $2bn within three years, but still represents only a small portion of the total insurance sector. In Europe, the market remains relatively small. This is linked to the culture of secrecy surrounding security breaches. Because data on these incidents are scarce, it is difficult to quantify the risks and price policies accordingly.

Despite the lack of detailed information, companies agree that cybersecurity must be a top priority. As former Cisco Chief Executive John Chambers says, 'There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked.' ●

**Julie Levy-Abegnoli is Subeditor at OMFIF.**

# Cyber risks pose systemic threat

## Ensuring resilience integral to central banks' supervisory function

**Danae Kyriakopoulou**
OMFIF

True innovation is always disruptive. Financial technology is introducing important benefits for market participants and the wider economy, but it is also creating new risks and can make old ones take novel forms. Cyber risk is a critical example. While it is not a new phenomenon, the frequency, potential entry points, scale and complexity of cyber attacks grow as more financial services move online and collaboration among banks and technology companies becomes pervasive.

Central banks tasked with preserving trust in the financial system have an essential role in promoting cyber resilience. Their efforts must encompass ensuring individual entities are less prone to attacks through stronger defence systems, as well as prioritising mitigation of impacts and the likelihood of isolated events taking systemic dimensions.

### CENTRAL BANKS SUPERVISORY ROLE

In his May 2019 speech entitled 'Challenges for the financial sector in adapting to cyber threats', Banca d'Italia Governor Ignazio Visco described cyber risk as a market failure. Individual firm's strengthen their own defences, but there are additional, negative externalities not owned by any single firm or regulator, such as contagion and potential for systemic escalation, which are harder to take into account given the difficulties with assigning accountability or costs for 'public' good in competitive, market sectors. This necessitates market intervention.

Several central banks have initiated supervisory guidelines, cyber stress tests, behavioural training or reporting obligations for institutions they regulate, including those in important financial centres such as New York, London, Hong Kong, Singapore and the euro area. But the present picture faces numerous drawbacks. These include fragmentation, with Banque de France Governor François Villeroy de Galhau acknowledging that while 'regulators are paying attention to cyber risks, and while they share the same objectives, regulatory texts tend to differ and as a result add to firms' burden in terms of compliance, with little marginal gain.'

While firms have been able to adapt to the fragmentation of capital, they may not be able to withstand a potential balkanisation of technology, which would inhibit their ability to operate at scale. Financial institutions' increasing reliance on third parties that lie outside supervisors' regulatory perimeter is another important challenge. Getting the details right is key, particularly in terms of the time it can take to detect an attack and associated reporting requirements, as well as the design of fines in the case of non-compliance.

### RISK TO MACROECONOMY

Microprudential supervision of cyber risk in individual institutions is necessary but insufficient. Cyber stress tests, guidelines for third-party use and behavioural training can all help lower the probability of attacks. But these will continue to occur, and central banks have a responsibility to reduce the impact of cyber attacks on the financial system. As Banque de France Deputy Governor Denis Beau recognised, 'With greater interconnections between technologies and the financial system, and the opening up of information systems, cyber risk is moving from an idiosyncratic risk to a potential source of systemic risk that needs to be addressed.'

There are three main transmission channels through which an attack on an individual institution can become systemic.

First, interconnectedness in the financial system. If lost or interrupted, the services provided by a financial market participant cannot be replaced easily within the short window that well functioning financial markets require. An attack can thus directly impact others across the system.

Second, through loss of confidence. The financial system is based on the confidence placed in it by participants, and a cyber attack could lead to bank runs, liquidity freezes and stock value effects and defaults due to the simultaneous reputational and financial hits through fines.

Third, disruption and damage to data integrity. Reliable, real-time data are key to the performance of the financial system, and cyber attacks have the potential to disrupt market activity through the loss of data integrity.

More debate must be had on what specific actions individual regulators take and how to address barriers to progress, especially around information sharing and trust. But acknowledging that cyber risks can be a form of financial stability risk with the potential of taking on systemic dimensions is critical. It brings the regulation and oversight of such risks directly under the remit of central banks, whose mandates include financial stability. Cybersecurity is no longer an issue of legitimacy of action or inaction. ●

**Danae Kyriakopoulou is Chief Economist and Director of Research at OMFIF. For more on OMFIF's research into central banks and cybersecurity, download our latest report on 'Driving cyber resilience in the financial system' from the OMFIF website.**

# Emerging security threats

Malware, trojans, distributed denial of service; once highly technical terms that have gained notoriety as the names of malicious software that can cripple businesses. The number of cyber incidents occuring is increasing year-on-year. They threaten all sectors and each company must look to bolster their defensive arsenal to cope with these advanced attacks.

## Major cyber attacks in the 21st century

Spamhaus, a nonprofit web protection service that tracks and blacklists spammers and hackers, was targeted in 2013 by a DDos attack. It is the largest ever attack of its nature, slowing the entire internet across the planet.

In February 2016 Bangladesh Bank was targeted by cyber criminals, who stole nearly $1bn using a 'dridex' malware bot through a fraudulent email message.

The global 'WannaCry' ransomware attack in May 2017 crippled the UK National Health Service's technology systems and raised concerns that the NHS was unprepared for cyber threats. Hackers exploited outdated software, costing the NHS a total of £92m through services lost and IT costs in the aftermath.

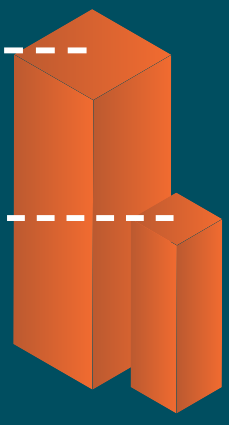
Unicredit, Italy's largest bank, was hacked in September and October 2016 and the summer of 2017, compromising the data of 400,000 customers.

NotPetya was part of a 2017 ransomware epidemic targeting businesses around the world. The malware infects a system's hard drive and demands that the user make a payment in bitcoin in order to regain access. The damage from the NotPetya incident is estimated at $10bn, making it the costliest ever global cyber attack.

## Cost of cybercrime

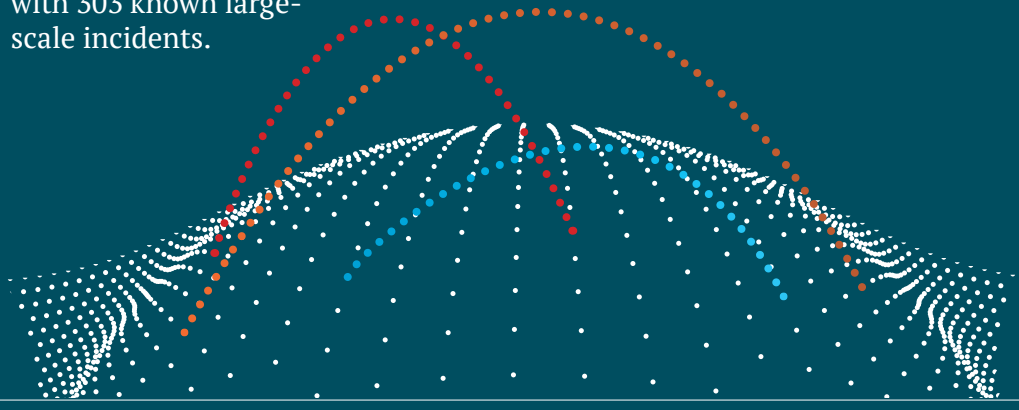
**$6tn**
by 2021

**$3tn**
in 2015



Between 2015-17, the US was the country most affected by targeted cyber attacks, with 303 known large-scale incidents.

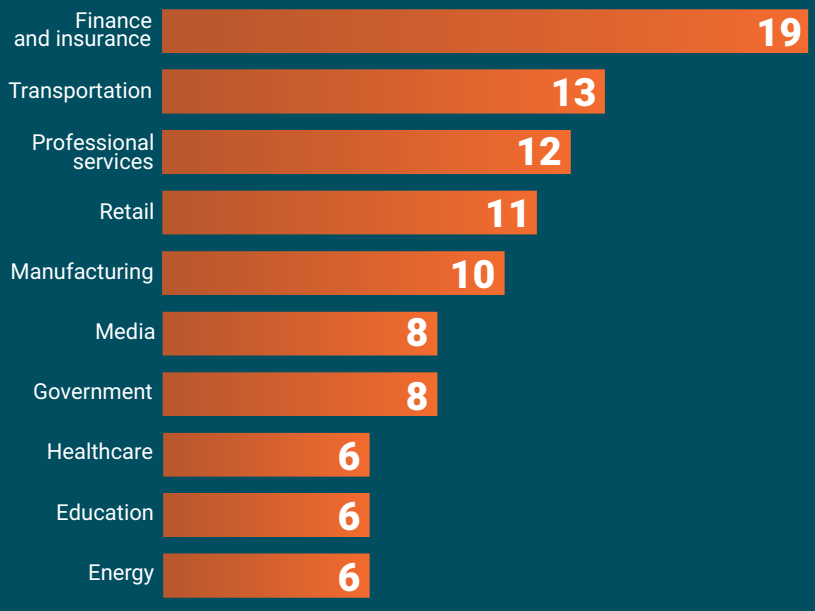
More than 20% of cyber attacks in 2017 emanated from China, 11% from the US and 6% from Russia.



## Financial industry hit hardest

The financial industry has been the most attacked industry for three years in a row, suffering 19% of total cyber attacks and incidents in 2018. In the light of the increasing value of customer data and the large digitial transanctions that hackers can intercept, threat actors and independent criminals alike see rich pickings in focusing on the sector. In response, financial firms are investing vast sums of money to make themselves more secure.

Most frequently targeted industries in 2018, %




*Source: IBM X-Force*

Trojan horse virus TrickBot was the most common method of attack on the financial sector, accounting for 13% of attacks in 2018.

The most damaging and costly risk for the sector is information loss, making up 43% of costs.

**$3,000**

Financial firms spend as much as $3,000 per employee to defend themselves from cyber criminals. Some of the largest banks tripled their cybersecurity budgets in the last four years amid a surge of attacks

# Pursuing cyber maturity

**Sabine Lautenschläger**, member of the executive board of the European Central Bank, speaks to OMFIF Senior Editor **Julian Frazer** about managing cyber risk in the euro area and collaborating with policy-makers the world over.

**Julian Frazer: How is the European Central Bank contending with cyber risks, and how do its approaches differ when preparing for or addressing attacks by nation states as opposed to non-state actors?**

**Sabine Lautenschläger:** The ECB contributes to ensuring the stability of the financial sector, and this includes enhancing cyber resilience. We implement a wide range of tools and approaches, including setting standards such as the Cyber Resilience Oversight Expectations, establishing cyber incident reporting protocols and developing testing frameworks (TIBER-EU) to set clear expectations and targets for the market. We conduct assessments, onsite inspections, crisis management drills and thematic reviews to validate whether entities meet appropriate levels of resilience. And we engage directly with the market to foster trust and collaboration.

Our approach is to ensure that the ECB and financial entities take a multidimensional perspective to achieve high levels of resilience. We do all this irrespective of the type of threat, its origin and motive.

The distinction between state and non-state actors is increasingly blurred and the gap in capability between the two is diminishing.

**JF: In the light of concerns around cross-border data sharing, to what extent has the ECB been able to collaborate with other regulators around the world in sharing best practice on cybersecurity?**

**SL:** Information sharing in cybersecurity is key. The ECB works with international regulators to share best practices and develop standards and tools to enhance global cyber resilience. We engage with the industry through panel discussions and conferences, and encourage market participants to share information and best practices with each other, to foster cross-fertilisation and collective action, for example within the Euro Cyber Resilience Board, comprised of pan-European financial infrastructures and regulators. In this board, we are working on a cyber information and intelligence sharing initiative, which will facilitate the multilateral sharing of information and data to prevent, detect and respond to cyber attacks and raise awareness of cybersecurity threats.

**JF: How receptive have businesses been in discussions with regulators on the need for increased spending on cybersecurity as part of risk management programmes?**

**SL:** Spending more is often not sufficient to increase cyber resilience. Many factors need serious consideration. The approach the ECB takes when engaging with financial entities is to ask them to understand the threats they face, to determine what problems they are trying to fix, and to set a clear vision and roadmap for their future target state of cyber maturity.

We place great emphasis on boards and senior management being involved in this process, as senior-level engagement is critical for effective decision-making and for ensuring a strong security culture. Once financial entities undertake this process of reflection, they should have a clear idea of their deficiencies and areas to prioritise, which will lead to the appropriate investment in the right areas.

**JF: Financial market institutions often struggle to find staff with the necessary skills and experience to fight cyber attacks. How best can policy-makers and private actors help close the cybersecurity talent gap?**

**SL:** As cyber threats continue to grow in sophistication, organisations from all sectors face a persistent challenge in recruiting skilled cybersecurity professionals. Some studies predict that by 2022 there will be upwards of 1.8m unfilled positions in the global cybersecurity workforce. We must organise workforce development to →

‘Organisations from all sectors face a persistent challenge in recruiting skilled cybersecurity professionals. Some studies predict that by 2022 there will be upwards of 1.8m unfilled positions in the global cybersecurity workforce.’

encompass a broad range of specialised skills and sector-specific knowledge desired by each employer. Hence all stakeholders should act already by building strategic partnerships, making appropriate investments, developing specialised education curriculums, facilitating apprenticeship programmes for hands-on experience, and building retraining academies to reskill workers.

All this can only be successful with a collective effort, with governments, educational institutions, academia and employers working in partnership. In the short term, private actors should cross-fertilise skills, resources and best practices to help each other, since cybersecurity is a non-competitive issue for us all.

**JF: Although more agile than incumbent institutions, new financial technology companies tend largely to possess fewer resources to set up robust cybersecurity systems. Have regulators been able to keep pace to protect customers of these nascent, data-driven businesses?**

**SL:** New financial technology companies are often more innovative, and such innovation is important for economic growth. But it is the case that such innovation, while welcome, may also bring risk. In general, we should apply the principle of same business, same risks, same rules. These companies must ensure that they build strong and safe systems.

With the technological development within the financial services industry, we must ask ourselves what kind of adaptation to the current regulatory framework can cater for the specific risks linked to these new technologies. Notwithstanding this, it is important that customers also take personal responsibility – simply downloading an app and accepting all terms and conditions, without being aware of the consequences, is suboptimal.

**JF: Much has been written about the possibility of a 'Digital Geneva Convention', but policy-makers in Europe have said in the past that existing international law is already applicable to the digital domain. Do new breeds of risk and conflict demand their own laws?**

**SL:** It is essential that we all have a common global understanding about how we should deal with digitalisation and the risk of a 'weaponisation' of technology. Today's conflicts encompass a hybrid of physical, digital and misinformation attacks. The scale and scope of cyber attacks have the potential of impacting the safety and security of civilian populations. For example, the attack on the Ukrainian power grid or the WannaCry attack, which destabilised healthcare and other civil infrastructures across the world. So, I think that policy-makers must take these factors into consideration as the basis for examining more deeply whether our existing international laws and treaties are adequate in this interconnected and digitalised world. ●

'The distinction between state and non-state actors that perpetrate cyber attacks is increasingly blurred and the gap in capability between the two is diminishing.'

## Profile

**Education:** Studied Law at the University of Bonn, sitting her first state examination in 1990 and her second in 1994.

**Career:** Lautenschläger held several high-ranking positions in German supervisory authorities before joining the European Central Bank in 2014. She became an official in the Federal Banking Supervisory Office (BAKred) in 1995, becoming its head of press and public relations in 1999. In 2002 BAKred was merged with the Federal Supervisory Offices for Securities Trading and Insurance to form the Federal Financial Supervisory Authority (BaFin). Lautenschläger was for two years BaFin's head of press and internal communication before becoming head of the department for the supervision of large, internationally active banks and qualitative supervisory standards. In 2008 she was appointed as a member of BaFin's executive board and the chief executive director of banking supervision. Between 2011-14 Lautenschläger served as vice-president of the Deutsche Bundesbank. As this edition of The Bulletin went to print, it was announced that Lautenschläger will resign her ECB position on 31 October.


Celebrate OMFIF's 10th anniversary
5 February 2020
Peter Praet, former chief economist of the European Central Bank, joins David Marsh and John Orchard for a reception to mark OMFIF's 10th anniversary.
Register your interest to attend on the website: www.omfif.org/10
The Gherkin
30 Saint Mary Axe
City of London
OMFIF
DZ BANK
Bank on Germany
10

# Largest economies dispel recession fears

## Money growth trends contradict forecasts of 2020 crisis

**Juan Castañeda and Tim Congdon**
Institute of International Monetary Research

Many experts agree that a recession is probable in 2020. Many also anticipated a recession in 2016, but it did not materialise. The world's leading central banks are fully aware of the current global slowdown. The Federal Reserve and European Central Bank have indicated they will respond flexibly to maintain demand and growth.

For a recession to occur in the next few months would require extreme policy-making incompetence. This column has stated previously that the world growth slowdown should not be expected to develop into something worse. At the time of writing (September 2019), the safest forecast for the world economy in 2020 is another year of roughly trend growth with little inflation.

Money growth data in the US and euro area remain positive about economic activity. In the three months to July, broad money growth (M3) in the US rose at an annualised rate of 9.3%.

With the exception of February 2015, this is the highest figure since before the 2008 financial crisis, signalling that a recession is unlikely to occur. In the euro area, M3 grew at an annualised rate of 5.6% in the three months to June, another indication that there will probably not be a recession. But there are caveats.

In recent months, US banks have increased their holdings of government securities, to pick up the expected capital gain from the Fed rate cut. In the euro area, money growth reflects currency inflows from abroad rather than domestic credit (this could include, for example, banks' acquisition of more claims on domestic public and private sectors). In China and India, money growth is stable, with an annual rate of almost 10%. Money growth is sluggish in the UK, Japan and Australia, probably due to asset price setbacks and poor business investment. However, these countries do not weigh as much in the global picture as the US, euro area and China.

All the same, the latest money trends in the two largest developed country jurisdictions contradict forecasts of a 2020 recession. ●

**Juan Castañeda is Director and Tim Congdon is Chairman of the Institute of International Monetary Research. For a more detailed analysis of the latest money trends, see the IIMR monthly report at https://www.mv-pt.org/monthly-monetary-update.**

# Worldview

## This month's expert analysis

# Data powering the new economy

## Open banking reshaping the financial landscape

**Linda Jeng**
Georgetown University Law Centre

After the 2008 financial crisis, former Federal Reserve Chair Paul Volcker said that automatic teller machines were 'the peak of financial innovation'. When cashpoints were introduced in the late 1960s, customers could for the first time view current account balances and withdraw cash without the assistance of human tellers. We are in the midst of an equally transformative wave of innovation in consumer banking. Customers no longer need to consult a cash machine for a snapshot of their accounts. They can pull out their smartphones and send payments instantaneously.

Customer data is powering these capabilities. Specifically, financial institutions are sharing customer-permissioned data with third parties. This is the defining and common feature of the various forms of open banking that exist across the world.

Some believe the global wave of open banking reforms gained impetus when the European Union adopted its revised Payment Services Directive in 2015. Under that directive, financial institutions must share payments-related data with authorised third parties when the customer has provided their consent. The UK had already anticipated these changes and developed a framework requiring the country's nine largest banks to share publicly-available information, such as branch locations, bank services and fees. Many other countries, including Japan, Mexico, Brazil, Australia, South Korea, India and South Africa, have adopted or are considering open banking frameworks. Others might argue that open banking is more advanced in China and the US, where there are larger data-sharing-based markets but no mandatory sharing framework.

### Privacy perils

Reassuringly, many of these countries are not considering open banking in a silo. They recognise that with the sharing of personal sensitive information come perils for individual consumer privacy and liability. These countries have adopted data privacy and protection rules. The most notable example is the EU's General Data Protection Regulation, which came into effect in 2018. Interestingly, during the development of some of these open banking and data privacy frameworks, many central banks and bank supervisors observed from the sidelines while competition authorities led the push for rule changes. The unfortunate result is that many central banks lack expertise on how financial services will change, particularly outside the traditional banking sector.

Although outside their conventional mandates of monetary and financial stability, central banks must urgently familiarise themselves with data privacy issues and how data-sharing practices are evolving. The customer service value chain is changing. Third parties are taking over from financial institutions to process personal customer data and fuelling the creation of innovative, increasingly popular services not provided by banks. These include aggregated financial snapshots, investment advice, person-to-person transfers, and accounting and tax preparation services.

Cybersecurity is a key concern. Even if data sharing transitioned fully to more secure channels such as application programming interfaces, breaches in sensitive personal data could still occur. Financial institutions, as well as third-party data processors and fourth-party storage service providers (cloud providers, for example) are all at risk. Such operational hazards pose significant reputation risks for those operating in the financial data-sharing sector. A significant data breach or misuse of data could destabilise the financial system.

### From banks to utilities

In the longer term, how third-party data processors and service providers change and add to the customer service value chain might transform banks into utilities. This could lead to a reduction in capital exposures, but also apply downward pressure to returns on equity.

The evolution of data sharing has the potential to impact the changing nature of banking and fuel the broader data-sharing economy. Every internet search and purchase, along with a person's location or photos, are stored online. These constitute valuable information that can be commoditised and leveraged into a service or product. In this rapidly growing sharing-based economy, ecommerce, service providers, manufacturers, distributors and financial institutions can partner to provide data-leveraged services and products.

According to a PwC study, the sharing economy is expected to grow to $335bn in 2025 from $15bn in 2014. In a future where data powers economies, central banks would be wise to become literate in data privacy and protection. ●

**Linda Jeng is Visiting Scholar on Financial Technology at Georgetown University Law Centre. She was Chair of the Basel Committee's working group on open banking, and previously served as Chief of Staff for Risk, Surveillance and Data at the Division of Supervision and Regulation of the Federal Reserve Board.**

# No need for investors to panic just yet

## Recession may only come to light following revisions to data

**Christopher Smart**
Barings Investment Institute

There's a moment that sends a chill down the spine of every sailor when a rock suddenly appears off the wrong side of the bow. Whether the chart was wrong, or the skipper missed a buoy, it's undeniably a sign of trouble.

That same cold jolt struck investors with the arrival of inverted yield curves, wilting inflation expectations and an array of other economic oddities. But it would be wrong to panic now.

The economic data have long indicated these were rough waters. Major economies are either already in recession or teetering on the brink. Growth continues to slow in China as authorities reined in credit last year and trade tensions hit.

On their own, these should be manageable challenges. The US is still growing at a reasonable rate, with strong consumer sentiment and low unemployment outweighing the effects of lagging industrial indicators and weak corporate earnings. There is room for fiscal support from countries like Germany and South Korea. China still has powerful tools to support credit growth and manage its deceleration. Dovish monetary policy at the world's largest central banks should help make the correction shorter and shallower than usual.

But the chart is only a chart and the rocks are still rocks. Regardless of the mixed economic data, bond yields keep drifting lower.

Unexpectedly, prices and returns have been muted by new and large global pools of cheap labour, by innovative technologies that seem to make everything cheaper, and by aging societies that don't spend as much as they once did. Against this backdrop, the legacy of unprecedented quantitative easing lingers in a world of high asset prices, rising debt and low rates.

Most investors have not updated their models to account for these oddities, and they are not sure how they should. The $17tn of debt that trades at negative yields is high on everyone's mind, but the phenomenon was never in anyone's economics textbooks.

The risk of recession has risen, and this confluence of so many weird and unpredictable currents helps explain the temptation to brace for disaster. It's possible this fragile sentiment will shatter altogether on the news of an unexpected bank failure, an uncontained cyber attack or a dramatic expansion of US trade tensions with Europe or Japan.

There may come fresh moments to panic, but short of large systemic shocks, the longstanding fundamentals still apply.

Economically, cheaper money should help extend the US consumer cycle and may even prop up corporate capital expenditures. Politically, investors are learning to adjust to a world of trade turmoil, where uncertainty has yet to spread significantly beyond bilateral flows between the US and China. Meanwhile, stocks, which only recently touched record highs, look relatively attractive on dividend yields.

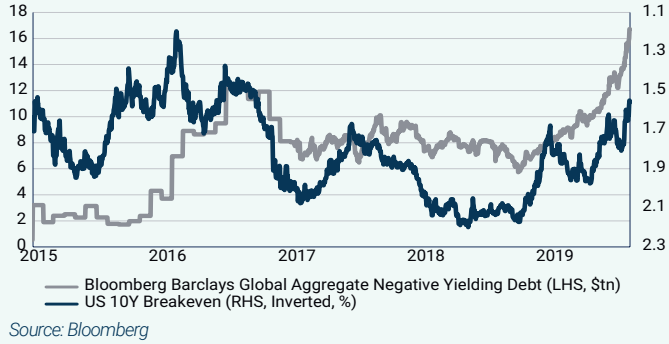
This means we may not actually notice the next recession when it hits, as it only appears in revisions to earlier and often confusing economic data. Markets may be volatile in the meantime as analysts make sense of economic forces and relationships that are different from those which shaped earlier cycles.

Still, just because a chart needs updating to account for some new shoals and currents, that doesn't mean we should jump ship just yet. ●

**Christopher Smart is Global Chief Strategist and Head of the Barings Investment Institute.**

**Negative yielding bonds traded rise**

Inflation expectations and negative yielding bonds




*Source: Bloomberg*

**Stocks attractive on dividend yields**

US 10-Year yield and S&P 500 dividend yield


*Source: Bloomberg*

# US trade deficit is homegrown

## Trump commits a 'fallacy of composition'

**Steve Hanke and Edward Li**
Johns Hopkins University

US President Donald Trump, alongside many business leaders, has a straightforward view on international trade, particularly the US external balance. He believes an external deficit is a malady caused by foreigners who manipulate exchange rates, impose tariff and non-tariff barriers, steal intellectual property and engage in unfair trade practices. The president and his followers feel the US is victimised by foreigners, as reflected in the country's negative external balance.

This wrongheaded mercantilist view of international trade and external accounts has its roots in how individual businesses operate. A healthy business generates positive free cash flows – revenues exceed outlays. If a business cannot generate positive free cash flows on a sustained basis, take on more debt or issue more equity to finance itself, then it will be forced to declare bankruptcy.

Business leaders employ this general free-cash-flow template when they think about the economy and its external balance. For them, a negative external balance for the nation is equivalent to a negative cash flow for a business. In both cases, more cash is going out than is coming in.

But this line of thinking represents a classic fallacy of composition. This is the belief that what is true of a part (a business) is true for the whole (the economy). Alas, economics is littered with fallacies. These cause businessmen to confuse their own arguments about international trade and external balances almost beyond reason.

### Savings-investment identity

The negative external balance in the US is not a 'problem', nor is it caused by foreigners engaging in nefarious activities. The US's negative external balance, which the country has registered every year since 1975, is 'made in the USA', a result of its savings deficiency.

To view the external balance correctly, the focus should be on the domestic economy. The external balance is homegrown; it is produced by the relationship between domestic savings and domestic investment. Foreigners only come into the picture 'through the backdoor'. Countries running external balance deficits must finance them by borrowing from countries running external balance surpluses.

It is the gap between a country's savings and domestic investment that drives and determines its external balance. This is demonstrated by the 'savings-investment identity'. In economics, identities play an important role. By definition, they are always true. Identities are derived generally by expressing an aggregate as a sum of parts, or by equating two different breakdowns of a single aggregate.

First, the national savings-investment gap determines the current account balance. Both the public and private sector contribute to the current account balance through their respective savings-investment gaps. The counterpart of the current account balance is the sum of the private savings-investment gap and public savings-investment gap or the public sector balance.

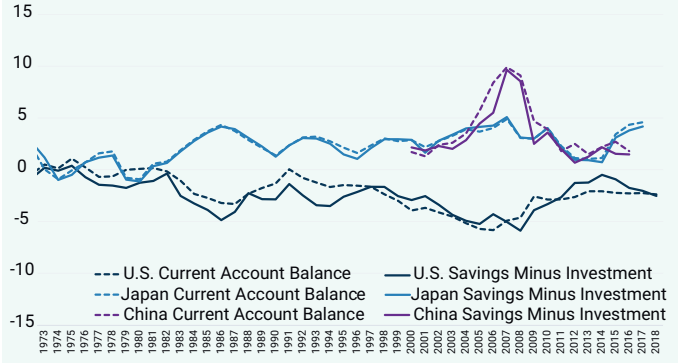
The US external deficit, therefore, mirrors what is happening in the US domestic economy. This holds true for any country, even those with significant external surpluses. The below figure, which comports with the savings-investment identity, makes this clear. The US displays a savings deficiency and a negative current account balance that reflects its negative savings-investment gap. Japan and China display savings surpluses, and both run current account surpluses that mirror their positive savings-investment gaps.

Given the stunning level of economic illiteracy that surrounds the strange world of international trade policy, it is time to use the irrefutable arguments and evidence to explain finally why a country's external balance is determined domestically, not by foreigners. ●

**Steve Hanke is a Professor of Applied Economics at Johns Hopkins University and a Member of the OMFIF Advisory Board. Edward Li is a Research Associate at the Institute for Applied Economics, Global Health, and the Study of Business Enterprise at Johns Hopkins University.**

**Savings and investment determine external balances**

Current account balance and savings-investment gap, % of GDP




*Sources: Economic and Social Research Institute of Japan, National Bureau of Statistics of China, and US Bureau of Economic Analysis. Calculations by Steve Hanke and Edward Li.*

# Fed rudderless in uncharted waters

## Powell's credibility has eroded as he pivots on policy

**Darrell Delamaide**
OMFIF

US Federal Reserve Chair Jerome Powell is having trouble keeping his troops in line. The September meeting of the Federal Open Market Committee brought an unusual three dissents among only 10 voting members.

The dissenters were themselves split. Two regional bank chiefs voted to keep the benchmark fed funds rate steady instead of lowering it a quarter-point, as decided by the majority. One wanted to lower it a quarter-point further.

Central bankers are having trouble figuring out what is going on, making policy decisions something of a wild guess. Stubbornly low inflation has become endemic, even though Powell and his counterparts keep saying the vaunted 2% target is just around the corner.

Unemployment is relatively low and staying low, even as more people are being drawn into the labour market. But even labour shortages are scarcely affecting inflation. It is a conundrum that even outgoing European Central Bank President Mario Draghi, the savviest of operators, has not been able to answer.

The world's most important central banker, meanwhile, can't seem to find his balance. Powell's press conferences verge occasionally on the inept, whipsawing markets as he pivots from one point of view to another. His authority and credibility have quietly eroded over his months as Fed chair. When first appointed to the board of governors in 2011, the lawyer turned investment banker and investor with little economic training seemed destined to occupy one of the six other seats on the board, dutifully following the chair's lead.

The monumental mistake made by President Donald Trump of not reappointing Janet Yellen to a second term was followed by the sloppiness of installing Powell as chief because somebody told him Powell was a low-interest guy.

But Powell is a follower, not a leader, in terms of interest rates or anything else. His press conferences are filled with references to 'our modelling', indicating that his beliefs are founded on what staff economists in Washington tell him. He is not capable of making his own determinations – unlike Yellen, or Ben Bernanke, or even Alan Greenspan before him.

### Limping along

There is a further leadership problem at the New York Fed. The money market turbulence in September came as New York, which is responsible for open market operations, underestimated how much funding would be needed for tax payments and bond settlements, even though both these events were known well in advance.

The excuses made by John Williams, who rose through the ranks of the research department at the San Francisco Fed before taking the top spot in New York, sounded flimsy. He claimed the Fed was ready because it was able to act quickly when all hell broke loose. One would have hoped that being ready would entail not letting that happen in the first place.

> 'Powell's press conferences verge occasionally on the inept, whipsawing markets as he pivots from one point of view to another.'

Powell has benefited from the set of policies put in place by his predecessors, and from a government that has no hesitation in providing fiscal stimulus. Draghi and his colleagues can only imagine getting that kind of support from fiscal authorities.

The fact remains that Fed policy-makers don't know whether to raise, lower or stand pat on interest rates. They claim to be 'data driven', but their backward-looking data don't seem to help them stay ahead of the curve. Criticism remains muted because no one wants to be seen agreeing with Trump as he tries to bully the central bank into a more accommodative stance.

National economies and central banks are in uncharted waters. If any further proof was needed, the latest trend for central banks to contemplate digital versions of their currencies provides it. Facing challenges from Facebook, JPMorgan and China to issue stablecoins and take global payments away from them, central banks have little choice but to counter with their own digital currencies.

The implications of global blockchain-based payments systems on the profit and functions of banks are profound. Caught in the pincer movement of financial technology providers and cryptocurrency payments systems, banks, which are ailing in most parts of the world, will be squeezed further.

In the meantime, the Fed will limp along without strong leadership to keep its truncated board in line. If Trump follows through with his intention of appointing goldbug Judy Shelton to the board, Powell may have even more dissent on his hands. ●

**Darrell Delamaide is US Editor of OMFIF.**

# Yellow metal thrives as China rises

## Membership of Beijing-led initiatives tied to rising gold purchases

**Pierre Ortlieb**
OMFIF

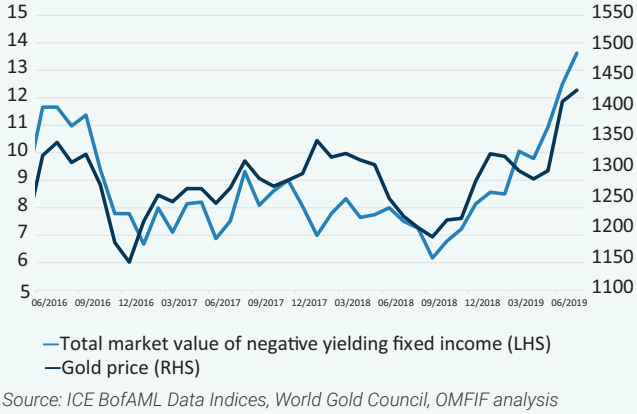
Gold has experienced a resurgence as a strategic asset for the official sector. In the first half of 2019, monetary authorities bought 374 tonnes of gold, a year-on-year rise of 57%. Since 2010, central banks across the globe have purchased more than 4,000 tonnes of gold. The value of their total gold holdings is around $1.4tn, or 10% of all foreign reserves. Unlike in previous decades, however, the current composition of gold buyers is surprisingly diverse, being spread across Asia, Europe and Latin America.

This surge in gold demand is often linked to common themes in geopolitics and western capital markets. Gold is as a popular hedge against equity weakness, both in the form of stretched valuations in the US, and weak performance, particularly among euro area financials. Additionally, the global surge in negative-yielding fixed income securities makes gold even more attractive, as the opportunity cost of holding the yellow metal declines. The total amount of bonds providing negative yields reached $15tn in August 2019, up from $6tn at the end of September 2018. The correlation between the amount of negative-yielding debt and the gold price is startling (see chart). The relative cost of incorporating gold into central bank portfolios has decreased, a point corroborated by gold market reactions to the Federal Reserve's interest rate cut in July 2019.

This comes in tandem with greater uncertainty over the future path of the dollar. A strong dollar has historically been bad for gold. Not only does it become more expensive to purchase gold in most markets, but it is also a sign that the US economy is doing comparatively well. Since the 2008 financial crisis and the election of President Donald Trump, there has been growing downward political pressure on the dollar, despite its realised strength so far this year. Trump has advocated the resumption of quantitative easing and bemoaned the dollar's strength, and other political figures have introduced legislation that would devalue the dollar. In addition to the ongoing US-China trade conflict, these factors exacerbate uncertainty in the reserve currency system, undermine faith in the dollar and fuel demand for the yellow metal.

**Comovement between gold and negative yielding debt**

Market value of negative yield debt, $tn (LHS), and gold price, $/troy ounce (RHS)




*Source: ICE BofAML Data Indices, World Gold Council, OMFIF analysis*

### Parallel networks

However, OMFIF's most recent report on gold and the international monetary system, sponsored by the World Gold Council, breaks new ground in this field by linking gold purchases to membership of China-led multilateral initiatives, such as the Belt and Road or the Asian Infrastructure Investment Bank.

Through these organisations, China is seeking to break away from the existing multilateral framework and establish an alternative, parallel network through which to leverage its growing power and internationalise the renminbi. As pointed out by Yin Yong, former vice-governor of the People's Bank of China, with 'more than 50 Belt and Road economies where the proportion of renminbi usage in cross-border transactions is lower than 5%, there is potential for huge improvement.'

The report suggests that, by participating in this alternative framework, countries indicate a willingness to diversify and regionalise their foreign exchange reserves. This in turn fuels gold demand, as uncertainty around the international currency system sparks a move towards safe haven assets such as the yellow metal.

Integration in China-led multilateral policy institutions may be an important factor influencing gold demand. This implies that countries with intimate institutional links to China who are currently not gold buyers or gold sellers could shift their stance; gold will continue to play an important role as Beijing-led institutions become increasingly prominent on the international stage. ●

**Pierre Ortlieb is Economist at OMFIF. Our report, 'Gold, global flows and the regionalisation of reserve assets,' sponsored by the World Gold Council, can be downloaded on the OMFIF website.**

# Beware dormant inflation

## Central banks must contend with stagnant prices

**Philippe Ithurbide**
Amundi Asset Management

Since the 1980s, most central banks have adopted and maintained an inflation target. It is generally around 2%, to ensure price stability. Since 2008, they have aimed to improve borrowers' solvency and extend the current expansion cycle as much as possible. Fearing deflation, central banks have adopted ultra-accommodative monetary policies, sometimes alongside unconventional measures, such as quantitative easing.

However, there is little to no inflation. This is due partly to the structure of the labour market (employees lack bargaining power) and competition. Because central banks have become deeply trustworthy institutions, inflation expectations are low. What is most striking, though, is certain countries' inability to stimulate inflation despite low rates, liquidity injections, a tight labour market and forward guidance policies.

This new situation implies profound changes in the perception of Organisation for Economic Co-operation and Development countries: low wage cost growth (a positive trade-off in favour of stakeholders and at the expense of workers so far), low underlying inflation and low interest rates, despite the advanced positioning in the economic cycle and tensions in the labour market. But inflation never disappears completely. It has been dormant in the past, with brutal consequences. All this affects directly the macroeconomic context, as well as central banks' and governments' objectives, instruments and mandates.

At the macroeconomic level, the absence of inflation and low interest rates imply that a debt crisis or recession is unlikely to materialise. These two factors are also associated with shorter inflation, credit and growth cycles. This is all due to a lower probability of interest rate increases, profit declines or solvency problems for borrowers.

### Central bank strategies

Despite doubts over inflation targeting, central banks are unlikely to change course, with the exception of the Federal Reserve. It has recently decided to review its objectives, tools, missions and communication policy. Some are debating central banks' strategy and whether interest rates should remain low in the long term. Regarding tools, unconventional monetary policy was initially severely criticised, but it now forms part of a central bank's 'classic' toolbox.

Central banks will probably face mounting pressure from governments regarding their mission. Their independence was adopted partly to help deal with high inflation, which some argue no longer exists. Others believe inflation targeting and independence would prevent central bankers from using more direct and effective solutions to solve current problems, such as deflationary pressures, over-indebtedness and potential financial crises.

One of the major concerns for governments is assessing properly tax and fiscal leeway that low interest rates and low inflation offer. The key question is whether this leeway is temporary or sustainable in the long term. They must also determine whether it is reasonable to grant any leeway considering the global context of continuous debt accumulation. Policy-makers must prevent the return of tax and fiscal complacency. They are also likely to debate in the coming months whether public spending represents the best way to support the economic cycle.

It would be risky to declare the end of inflation. It has changed in nature and remained low for years, but it is far from dead. Rather, it is dormant, and potentially on the rise. Whatever the next step, uncertainty persists. Central banks must continue navigating with little knowledge of what the post-financial crisis 'new normal' will be. ●

**Philippe Ithurbide is Global Head of Research, Analysis and Strategy at Amundi Asset Management. The full report on which this article is based, 'Is inflation definitely dead or simply dormant? Consequences for central banks', is available at research-center.amundi.com.**

'Despite doubts over inflation targeting, central banks are unlikely to change course, with the exception of the Federal Reserve.'

# Central banks' new digital mandate

## Policy-makers identifying common set of desired CBDC features

**Christian Jüttner**
Giesecke+Devrient Currency Technology

As life becomes increasingly digitalised, payments must follow suit. Accordingly, central banks' mandate to guarantee efficient and crisis-resilient means of payment must be transferred into the digital world.

Existing electronic payment schemes are not fulfilling this demand. Most require a subscription, bank account or impose high fees. Additionally, few solutions cover all relevant use cases: point-of-sale payment, online shopping and person-to-person payment, whether remote or face-to-face, with or without a network connection. As of today, no single universal digital means of payment exists. Payment instruments are rather to be matched with specific use cases, merchants and online shops – a friction demanding new digital solutions.

Big players like Amazon Pay, Google Pay, Alipay and Facebook recognise this and are challenging the financial system by investigating the development of comprehensive digital payment instruments. Global, fast-moving and featuring extensive user networks – and being rarely concerned with local legislation – these companies might have the potential to establish their chosen approach.

However, a working digital format of cash provided globally by a private institution could disrupt the financial system, posing additional risks by threatening the sovereign duty and position of central banks. Facebook's cryptocurrency project Libra, for example, must first pass regulators' assessments. In any case, the need for new means of payment will eventually give rise to some form of market-disrupting solution.

> 'A working digital format of cash provided globally by a private institution could disrupt the financial system, posing additional risks by threatening the sovereign duty and position of central banks. '

An increasing number of central banks are analysing whether they should provide a central bank digital currency – legal tender they issue and control, pegged to the local currency. They are investigating potential benefits, risks, regulatory constraints and approaches, with many national authorities moving towards presenting their possible solution. As yet, no decisions have been made. Giesecke+Devrient's discussions with various central banks have indicated that while motivations differ, a common set of desired CBDC features exists.

### Connected world

Central banks, as the only entities being able to issue and destroy digital cash, should maintain full control. As with attempts to counterfeit traditional banknotes, the risk of cyber attacks on CBDCs is high, necessitating robust security as part of their design requirements. It is currently almost impossible to pay digitally without disclosing personal data. A CBDC could serve as a digital means of payment that transports value and trust by providing a certain level of privacy that would support public acceptance. A means of payment that is capable of balancing security, privacy and transparency would offer substantial benefits.

Moreover, it must be easy to use, widely applicable and accessible. This should include not only the use of latest mobile devices, but also the availability to people without bank accounts. It should incur no or marginal transaction fees for the user.

Evidently, a digital currency should be treated as a complement to cash, offering additional features connected to the digital world. Giesecke+Devrient followed this vision with G+D Filia, the company's CBDC solution. In the G+D Filia approach, a data file minted by a central bank represents monetary value and is distributed according to the contemporary cash cycle, through commercial banks or other financial institutions. It can be utilised through smartphones, smartcards, smartwatches and other forms of electronic wallet. It precludes the need for an account, the disclosure of private data, system registration or consumer fees. Because it is open, it allows payment service providers to integrate it into their offerings as part of a larger payment system. This encourages new business models and fosters innovation and growth, filling the digital payment void while ensuring continuity in the financial system. ●

**Christian Jüttner is Global VP and Head of Corporate Development at Giesecke+Devrient Currency Technology.**

# Embracing digital disruption

## Companies pouring resources into new technologies

**Andy Budden**
Capital Group

Fund managers and analysts are constantly scouring the world for the next major technological disruption. Two innovations are already having a significant impact on the world.

Despite its futuristic-sounding moniker, artificial intelligence has been around since the 1950s, and may be best known as the brain behind digital assistants such as Siri and Alexa. But AI has never quite lived up to expectations.

That is rapidly changing thanks to the convergence of sophisticated algorithms, lightning-fast computer speeds and the sheer explosion of data across the digital terrain. As with major technological advances of the past, the maturation of AI is likely to usher in a wave of innovation that will have a profound impact across the business world.

AI and its close cousins, machine learning and neural networks, refer to computers designed to mimic human reasoning and logic. Initially, AI has helped companies boost efficiency by automating mundane tasks. Increasingly, machine learning is enabling in-depth pattern recognition and predictive analysis, with broad applicability in such sectors as healthcare, finance, transportation and manufacturing.

In medicine, for example, computers are becoming able to handle patient intake at hospitals, scan medical records for early detection of health problems and help design treatment plans. Beyond that, pharmaceutical companies could harness neural networks to identify the most promising areas of research with the greatest odds of clinical success. In finance, AI will help banks reduce loan losses by analysing credit risks more quickly and effectively. Unsurprisingly, big technology companies and a bevy of start-ups are all putting huge resources into AI.

### Rise of cloud computing

Cloud computing is also attracting considerable investor attention. It allows smartphones to perform countless functions seamlessly, from sending emails to storing photos and playing films. Phones often get little-noticed assists from large computers located hundreds or even thousands of miles away. These distant computers are known collectively as 'the cloud'.

One of the most visible trends over the past few decades is that digital devices have become progressively smaller. But although the devices themselves have slimmed down, the need for mammoth computers toiling behind the scenes is as great as ever. The swirl of data splashing around in today's digital vortex requires individuals and businesses to secure immense processing power, speed and storage. Those functions come from networks of servers located remotely and accessed over the internet.

> 'The swirl of data splashing around in today's digital vortex requires individuals and businesses to secure immense processing power, speed and storage.'

For companies that are switching from legacy systems, two of the cloud's biggest attractions are simplicity and cost savings. Businesses can essentially outsource technology — data storage, software purchases and processing muscle — just as they have many other functions. They avoid up-front outlays for hardware and software that quickly become obsolete. And there's no need for jumbo information technology departments to oversee every facet of an in-house system.

Companies also gain agility. They typically pay only for the storage capacity and computing power they use, allowing them to quickly scale up for projects or test new ideas. Cloud service providers also handle security, a critical issue in the wake of highly publicised hacking incidents at prominent companies.

Businesses are attracted by next-generation functions, such as data analytics and machine learning, that previously were impossible or prohibitively expensive. The cloud allows companies to undertake new tasks that can help their businesses grow. Increasingly, there is a shift towards creating value from the cloud rather than simply reducing information technology costs. A consumer brand, for example, could roll out precision-targeted marketing campaign and a medical provider could better decode health patterns to improve treatments.

Cloud computing is projected to surge as companies continue to migrate from legacy systems and individuals require lightning-fast speed for video and other bandwidth-heavy functions. This bodes well for the providers of cloud infrastructure services, with the market expected to balloon to almost $350bn in 2028 from less than $50bn in 2018, according to Capital Group estimates. ●

**Andy Budden is Investment Director at Capital Group.**

## COUNCIL


**Meghnad Desai**
House of Lords; chairman, OMFIF Advisers


**Otaviano Canuto**
World Bank Group


**Aslihan Gedik**
OYAK Anker Bank


**Robert Johnson**
Institute for New Economic Thinking


**Hani Kablawi**
Chairman EMEA and CEO Global Asset Servicing BNY Mellon


**William Keegan**
The Observer


**John Kornblum**
Noerr


**Norman Lamont**
House of Lords


**Kingsley Moghalu**
Tufts University


**Louis de Montpellier**
State Street Global Advisors


**Fabrizio Saccomanni**
LUISS University


**Frank Scheidig**
DZ BANK


**Ben Shenglin**
Zhejiang University Academy of Internet Finance


**Gary Smith**
Barings


**Xiang Songzuo**
International Monetary Institute


**Niels Thygesen**
University of Copenhagen


**Ted Truman**
Peterson Institute for International Economics


**Marsha Vande Berg**
Stanford University

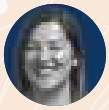
## NETWORK

Bahar Alsharif
David Badham
Franco Bassanini
Eduardo Borensztein
Consuelo Brooke
Colin Budd
Michael Burda
Shiyin Cai
David Cameron
Forrest Capie
Stefano Carcascio
Desmond Cecil
Efraim Chalamish
Moorad Choudhry
John Chown
Vladimir Dlouhy
Obindah Gershon
Jonathan Grant
Peter Gray
François Heisbourg
Frederick Hopson
Matthew Hurn
Korkmaz Ilkorur
Karl Kaiser
David Kihangire
Ben Knapen
Ludger Kühnhardt
Celeste Cecilia Lo Turco
Bo Lundgren
Mariela Mendez
Murade Miguigy Murargy
George Milling-Stanley
Winston Moore
Wilhelm Nölling
José Roberto Novaes de Almeida
Michael Oliver
Francesco Papadia
Robin Poynder
Poul Nyrup Rasmussen
Janusz Reiter
Anthony Robinson
Philippe Sachs
Nasser Saidi
Pedro Schwartz
Vilem Semerak
Song Shanshan
Marina Shargorodska
Paola Subacchi
David Suratgar
José Alberto Tavares Moreira
Jens Thomsen
David Tonge
Jorge Vasconcelos
Gottfried von Bismarck
Jack Wigglesworth
Paul Wilson

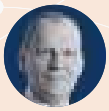
## CAPITAL MARKETS


**John Adams**
China Financial Services


**Yaseen Anwar**
Industrial & Commercial Bank of China


**Irena Asmundson**
California Department of Finance


**Georgina Baker**
International Finance Corporation


**Stefan Bielmeier**
DZ BANK


**Hans Blommestein**
Vivid Economics


**Mark Burgess**
Jamieson Coote Bonds


**Michael Cole-Fontayn**
Association for Financial Markets in Europe


**Thomas Finke**
Barings


**Gao Haihong**
Institute of World Economics and Politics

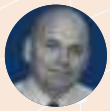

**Christian Gärtner**
DZ BANK


**Trevor Greetham**
Royal London Asset Management


**Daniel Hanna**
Standard Chartered Bank


**George Hoguet**
CFA Research Foundation


**Soh Kian Tiong**
DBS Bank


**Stuart Mackintosh**
Group of Thirty

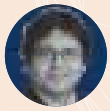

**Paul Newton**
London & Oxford Capital Markets


**Saker Nusseibeh**
Hermes Fund Managers


**Jukka Pihlman**
Standard Chartered Bank


**Colin Robertson**
SW1 Consulting


**Fabio Scacciavillani**
Oman Investment Fund


**Lutfey Siddiqi**
National University of Singapore


**Volker Wieland**
German Council of Economic Experts


**Katarzyna Zajdel-Kurowska**
World Bank Group

## MONETARY POL


**Iain Begg**
London School of Economics


**Marek Belka**
former prime minister of Poland


**Harald Benink**
Tilburg University


**Mario Blejer**
Banco Hipotecario


**Stewart Fleming**
St Antony's College, University of Oxford


**José Manuel González-Páramo**
BBVA


**Brigitte Granville**
Queen Mary, University of London


**Graham Hacche**
NIESR


**Akinari Horii**
The Canon Institute for Global Studies


**Harold James**
Princeton University


**Hemraz Jankee**
formerly Central Bank of Mauritius

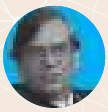

**Pawel Kowalewski**
Narodowy Bank Polski


**Philippe Lagayette**
formerly Banque de France

## ICY


**Andrew Large**
Hedge Fund Standards Board


**Gerard Lyons**
Bank of China (UK)


**Rakesh Mohan**
Yale University


**Athanasios Orphanides**
MIT Sloan School of Management


**Nagpurnanand Prabhala**
University of Maryland


**Edoardo Reviglio**
Cassa Depositi e Prestiti


**Olivier Rousseau**
Fonds de réserve pour les retraites


**Miroslav Singer**
Generali CEE Holding


**Shumpei Takemori**
Keio University


**Makoto Utsumi**
formerly Japan Finance Ministry


**Tarisa Watanagase**
formerly Bank of Thailand


**Ernst Welteke**
formerly Deutsche Bundesbank

## INDUSTRY & INVESTMENT


**Andrew Adonis**
House of Lords


**Robert Bischof**
German-British Forum


**Albert Bressand**
European Commission


**Caroline Butler**
Walcot Partners


**Nick Butler**
King's College London

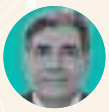

**John Campbell**
Campbell Lutyens


**Mark Crosby**
Monash University


**Hans Genberg**
The Seacen Centre


**Steve Hanke**
The Johns Hopkins University


**Hans-Olaf Henkel**
University of Mannheim


**Mumtaz Khan**
Middle East & Asia Capital Partners


**Joel Kibazo**
JK Associates


**Jürgen Krönig**
Die Zeit


**Oscar Lewisohn**
Soditic


**Boyd McCleary**
39 Essex Chambers


**Luiz Eduardo Melin**
International Economic Synergies


**Willem Middelkoop**
Commodity Discovery Fund


**Célestin Monga**
African Development Bank


**Danny Quah**
Lee Kuan Yew School of Public Policy


**Takuji Tanaka**
Japan Finance Ministry


**Daniel Titelman**
ECLAC


**Pasquale Urselli**
Mazars


**Paul van Seters**
Tilburg University

## POLITICAL ECONOMY


**Antonio Armellini**
former ambassador, OSCE


**Frits Bolkestein**
formerly European Commission


**Laurens Jan Brinkhorst**
University of Leiden


**Peter Bruce**
Business Day


**Jenny Corbett**
Australia National University


**Maria Antonieta Del Tedesco Lins**
University of São Paulo


**Hans Eichel**
former German minister of finance


**Jonathan Fenby**
TS Lombard


**Jeffry Frieden**
Harvard University


**Elliot Hentov**
State Street Global Advisors


**Roel Janssen**
NRC Handelsblad


**Yosuke Kawakami**
formerly Japanese Ministry of Finance


**Thomas Kielinger**
Die Welt


**Denis MacShane**
Avisa Partners


**Kishore Mahbubani**
National University of Singapore


**David Owen**
House of Lords


**Vicky Pryce**
Centre for Economics & Business Research


**Brian Reading**
independent economist


**Robert Skidelsky**
House of Lords


**Michael Stürmer**
WELT-Gruppe

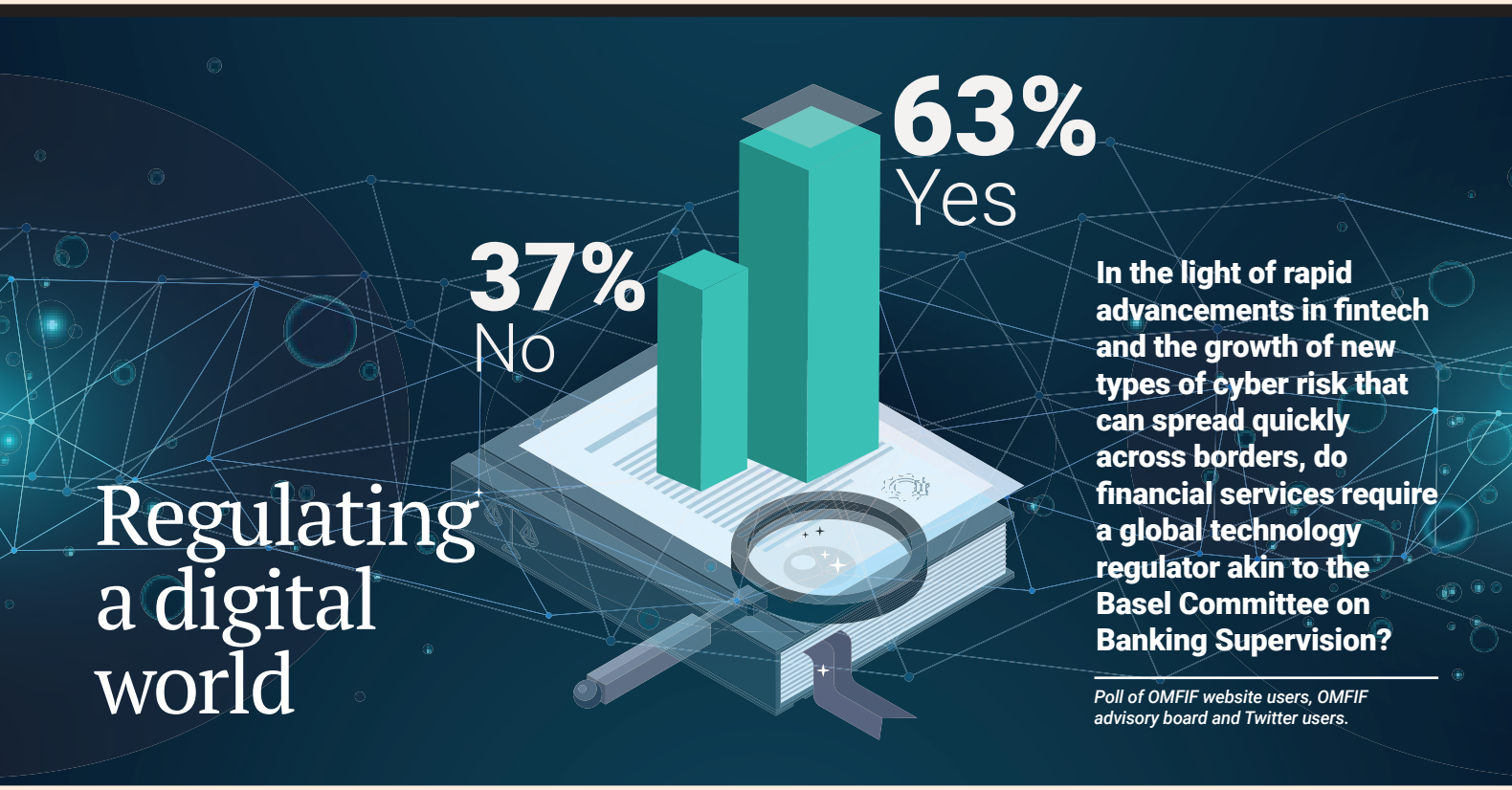

**Christopher Tugendhat**
House of Lords


**John West**
Asian Century Institute


**William White**
OECD


**Juliusz Jabłecki**
Nardowy Bank Polski

# Regulating a digital world




**In the light of rapid advancements in fintech and the growth of new types of cyber risk that can spread quickly across borders, do financial services require a global technology regulator akin to the Basel Committee on Banking Supervision?**

*Poll of OMFIF website users, OMFIF advisory board and Twitter users.*

'The economic and financial landscape is being transformed through rapid advances in financial technology. However, while fintech offers a wide range of opportunities, it raises potential risks to financial stability and integrity as well as to consumer and investor protection. My considered view is that it might be premature at this stage to call for a global technology regulator akin to the Basel Committee. The International Monetary Fund and World Bank can certainly help in enhancing collective surveillance of the international monetary and financial systems.'

**Hemraz Jankee, formerly Bank of Mauritius**

'Yes, but the issues may be inextricable from "regular banking", so rather than have a separate regulator, this could be a book of work within the Bank for International Settlements. It will also help elevate discussion and focus on cyber risk from just information technology and operations teams to executive committees and company boards. Cyber fluency should not just be for specialists.'

**Lutfey Siddiqi, National University of Singapore**

'There are two solutions, either the fragmentation of the internet, for example a European one, which would demand a regional regulator, or one internet globally. In the latter case, you need a global regulator. I would prefer the second solution.'

**Hans Eichel, formerly German Finance Ministry**

'No. New technology offers new means to undertake financial transactions, but it is not a separate system. Having a new regulator would increase the possibility of missing emerging issues in the financial system.'

**Irena Asmundson, California Department of Finance**

'The answer is absolutely no. Not that some sort of coherence wouldn't be good. But the points of view of many nations are so far apart that even a proposal for such a regulator would be impossible to formulate. Microsoft, for example, has tried to suggest negotiating binding agreements on various matters, but their proposals have been so far from reality that they haven't gotten very far. Better would be to begin examining general principles which could apply to all and to seek a means of propagating them globally, something akin to the Helsinki principles which helped end the cold war.'

**John Kornblum, Noerr**

'I would certainly suggest something like this under the leadership of the Bank for International Settlements. The Basel Committee was certainly the most efficient institution to approach necessary regulatory change during my time as head of supervision of financial markets. The Czech central bank, of which I was governor between 2005-16, acts also as an integrated supervisor of the financial market. I feel a unified approach might benefit all.'

**Miroslav Singer, Generali CEE Holding**


BARINGS

BARINGS.COM/ADAPTABILITY

18-571006