Do you remember the recent WannaCry ransomware attacks? Well, attackers have better options.

State-sponsored hackers, criminals, and others, now prefer WannaMine and other malware variants, that hijack processing power to mine a cryptocurrency called Monero.

A good lawyer and friend has told me: "I want to have the Internet, the whole Internet, and nothing but the Internet." Everything that stands between him and the Internet is a curse. A few days ago, his computers were very slow, and he wondered why.

WannaMine infects computers, uses them to run complex decryption routines that create Monero, and adds the cryptocurrency produced to a digital wallet belonging to the puppet masters that designed the process.

Attackers usually trick victims into loading crypto mining code onto their computers through phishing. If you receive a legitimate-looking email, you may click on a link, no matter how many times you have been advised not to do so.

To make things worse, attackers can inject scripts on legitimate websites. Once victims visit the websites, the script automatically executes.
Can it become worse? Absolutely. **What if they persuade you** that you save money if you let them mine crypto currencies using your computer? For example, you receive a service for free, if you let them use your processing power *while* you are browsing a web page. Deal?

There is software available, designed to offer websites an alternative to advertising. Instead of requiring users to tolerate ads, sites offer an ad-free experience, in exchange for some CPU power to mine cryptocurrency. And users opt in. Are you surprised to hear that the mining doesn't end when a user leaves the website?

How can you avoid that? Awareness, training, countermeasures are all required. For example, you can prevent JavaScript or other website scripts from executing, and you must use adblockers. No, you cannot have the Internet, the whole Internet, and nothing but the Internet.

What about other devices and cell phones? As an example, an Android malware called Loapi can lead to all kinds of problems, including cryptocurrency mining.

Trojan.AndroidOS.Loapi is a hidden part of apps, distributed through third-party markets, browser ads, and SMS-based spam. Mobile antivirus apps and, of course, adult-related apps, may hide the Loapi module.

After the installation of the app, Loapi asks for administrator rights. *Again, and again, and again, until you give up and do it.* You can change it later, right?

If you try to deprive the app of administrator rights, Loapi locks the screen and closes the settings window. And they you try to solve the problem, and
you download other apps (antivirus, for example). In this case Loapi alerts you that these apps are malware, and it demands their removal. *Again, and again, and again, until you give up and do it.*

And what is Loapi doing on the device? *You gave it administrative rights, remember?*

- Loads banner and video ads.
- Downloads and installs other apps.
- Visits links, opens web pages, opens Facebook and Instagram to drive up ratings.
- Signs up users to paid services. Even when such subscriptions must be confirmed by SMS, Loapi sends the text message secretly. Then these messages are deleted.
- It turns the phone into a zombie and takes part in DDoS attacks.
- It mines cryptocurrencies (Monero tokens). This activity can overheat the device.
- It downloads new modules to adapt to any new strategy, development, or objective.

I will tell it again. Install apps only from official stores. Disable the installation of apps from unknown sources. (Settings, Security, the Unknown sources check box is not selected). And this is just the first line of defense, based on awareness, training and countermeasures.

Welcome to the Top 10 list.

*Best Regards,*

George Lekatis
President of the IARCP
General Manager, Compliance LLC
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828
Virtual or virtueless? The evolution of money in the digital age

Yves Mersch, Member of the Executive Board of the European Central Bank, at the Official Monetary and Financial Institutions Forum, London.

European folklore warns of the will-o'-the-wisp, a malignant creature that dwelt in marshes. It would appear as a light in the distance, which a traveller would mistake for houses.

As they reached the place where they thought the light was, it would move further ahead, drawing them deeper into the marsh to their untimely death and a watery grave. In some areas, will-o'-the-wisps were said to mark buried treasure. Investigation of the phenomenon found it was related to dissipating bubbles of marsh gas.

SEC Office of Compliance Inspections and Examinations Announces 2018 Examination Priorities

The Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) announced its 2018 examination priorities.

OCIE publishes its exam priorities annually to improve compliance, prevent fraud, monitor risk, and inform policy. Of particular interest this year will be matters involving critical market infrastructure, duties to retail...
investors, and developments in cryptocurrency, initial coin offerings, and secondary market trading.

"I appreciate OCIE's dedication to maximizing the effectiveness of their resources with a keen eye toward asset verification, market infrastructure, and duties owed to retail investors," said SEC Chairman Jay Clayton.

**Number 3 (Page 1)**

**At the crossroads - innovation and inclusive growth**

Carolyn Wilkins, Senior Deputy Governor of the Bank of Canada, at the G7 Symposium on Innovation and Inclusive Growth, Montebello, Quebec.

```
“We know that technological advances are key to improving an economy's potential to grow. They have raised living standards in G7 countries and across the globe, and have helped lift more than one billion people around the world out of extreme poverty since the Second World War.

The current wave of innovation—digitalization and automation—promises to raise trend growth in the economy even more.”
```

**Number 4 (Page 1)**

**European Cyber Security Month 2017**

Deployment Report, February 2018
For the fifth consecutive year, last October the European Cyber Security Month (ECSM) campaign was successfully executed across Europe.

The campaign was coordinated and supported by ENISA, the European Commission, Europol’s Cyber Crime Centre (EC3), European Banking Federation, the Estonian Information Systems Authority and cyber security organisations from the Member States.

Number 5 (Page 1)

Cryptomining trends

News articles have focused recently on the value and volatility of cryptocurrencies, over the past year, most notably Bitcoin which had a peak value of $20,089.00 in December 2017.

Cryptocurrencies can be earned, or ‘mined’, by performing computationally intensive operations to support the running of the currency. Malware intended to mine cryptocurrencies on victim computers has been available since at least 2013 and surged in popularity in late 2017 as the currencies’ value increased.

Number 6 (Page 1)

IT security: BaFin specifies requirements for the banking industry

Bundesanstalt für Finanzdienstleistungsaufsicht

BaFin has published the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT).

The BAIT have now become the cornerstone of IT supervision for all credit and financial services institutions in Germany. The requirements are directed at the management boards of such companies.
The future relationship between Germany and the UK in finance after Brexit

Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at UK Finance, London.

“And this great country and this wonderful city are where the future is made: a place of rare art and cultural diversity and of economic dynamism and innovation. So I am more than happy to be here with you today.

When I read the news of the Brexit vote, I was shocked. As I looked at the news, I simply couldn’t believe it. I imagine I was not the only one among us.”

The Solvency II Review: What happens next?

Gabriel Bernardino, Chairman of the European Insurance and Occupational Pensions Authority (EIOPA)

“Ten years after the emergence of the financial crisis, we are now in a different phase of the regulatory cycle naturally influenced by the new political priorities of increasing investment and economic growth.”
Meltdown and Spectre – Updated Advice

Malware making use of Meltdown and Spectre, the two CPU vulnerabilities highlighted back in January, is now being seen in the wild. Security researchers are reporting they have seen over 140 malware samples based on the proof of concept code.

Whilst there have not been instances of Meltdown and Spectre actually being leveraged to compromise a system, it is a timely reminder that miscreants will take published security vulnerabilities and weaponise them into malware quickly, making it all the more important to patch.

Playing 20 Questions with Bacteria to Distinguish Harmless Organisms from Pathogens

New biosurveillance technology would quickly identify potentially harmful traits in unfamiliar bacterial strains

Bacteria underpins much of our world, acting behind the scenes to affect the health and behavior of animals and plants. They help produce food, provide oxygen, and even reshape the environment through a vast array of biological processes.

They come in a phenomenal number of strains—many still unknown—and thrive in different ecological and environmental niches all over the world. But while their diverse behaviors makes them essential to life, bacteria can also be deadly.
Virtual or virtueless? The evolution of money in the digital age

Yves Mersch, Member of the Executive Board of the European Central Bank, at the Official Monetary and Financial Institutions Forum, London.

European folklore warns of the will-o’-the-wisp, a malignant creature that dwelt in marshes. It would appear as a light in the distance, which a traveller would mistake for houses.

As they reached the place where they thought the light was, it would move further ahead, drawing them deeper into the marsh to their untimely death and a watery grave.

In some areas, will-o’-the-wisps were said to mark buried treasure. Investigation of the phenomenon found it was related to dissipating bubbles of marsh gas.

With the draining of marshes to make way for agricultural land, will-o’-the-wisps are rarely sighted nowadays. But there remain plenty of distant flashing lights to distract travellers with promises of riches.

As with the previous incarnation, these flashing lights often turn out to be just like bubbles of marsh gas - insubstantial and foul-smelling, but also flammable and sometimes able to burn things around them.

The most recent beguiling wisps are named variously "cryptocurrencies" - to denote the use of cryptographic methods and technology - or "virtual currencies" (VCs) - to denote their lack of legal recognition.

There are, at present, more than 1,500 VCs in circulation, with dozens of new schemes being launched monthly, including initial coin offerings (ICOs).
Most have failed to attract users, in particular in the major currency areas. The total value outstanding has fluctuated sharply, largely from speculative activity.

The global value of all VCs is currently around a fifth of the value of all euro banknotes in circulation and around 3% of the narrow monetary aggregate M1. Of course, these figures are probably already out of date, such is the volatility of the market.

Having a million dollars' worth of Bitcoin today would have required the simple investment of three million dollars in mid-December.

Because holders can hide their identity and location, it is impossible to accurately analyse VC circulation in the euro area. But euro-related activity on exchanges represents a small share of global activity, and is concentrated on a small number of users.

While VCs remained an esoteric interest, it seemed sufficient for authorities to mostly observe and issue warnings here and there. But it is the dose that makes the poison. Now that VCs may grow to be economically significant, we need to reduce the risk of negative impacts on the economy.

In my remarks today, I wish to explain what it takes for something to be considered "money" - and how VCs measure up. I will then set out what I believe are some of the key regulatory questions that need addressing, and actions that need to be taken to mitigate the potential blowback from VCs to the rest of the financial system.

What is money?

Money has formed an integral part of human economic interaction for millennia. It has appeared in many forms - metallic currency, paper notes, cowry shells, cigarettes and even the great Rai stones of Yap.

Are VCs the latest incarnation of money?

The answer for now, and indeed for the foreseeable future, is no. Economists generally define money as being a verifiable asset that fulfils three basic functions: a medium of exchange, a unit of account and a store of value.

How well do VCs carry out those functions?
Medium of exchange

Some VCs have attained patchy acceptance as a medium of exchange. The current largest, Bitcoin, is accepted by some retail outlets, but on a global scale these outlets remain small in number, and hardly any actual transactions have taken place.

On a daily basis, there are around 284,000 Bitcoin transactions globally, compared with 330 million retail payments in the euro area. Indeed, a recent Bitcoin conference stopped receiving payment in Bitcoin because of the cost and time involved in processing the payments.

Bitcoin is far inferior to existing payment options. Bitcoin transactions generally require confirmation from six miners. With each block taking around ten minutes to mine, you would expect transactions to take an hour to process. But with recent network congestion, the average time for one confirmation can easily exceed several hours.

At these speeds, if you bought a bunch of tulips with Bitcoin they may well have wilted by the time the transaction was confirmed.

Bitcoin payments are also expensive. The recent cost of a Bitcoin transaction is €25, the same cost as carrying out 12,500 transactions on the incoming TARGET Instant Payment Settlement (TIPS).

Bitcoin is heavily resource intensive, and certainly not a green technology. Bitcoin mining is estimated to currently consume energy at an annual rate of 46 TWh, approximately 35 times the electricity consumption of all Tesla cars in the world.

In comparison, traditional payment services have made large strides in innovation. The instant payments scheme SCT-Inst was launched in November 2017 and the Eurosystem will implement the TIPS service in November 2018.

A key characteristic of the instant payments scheme is that funds are made available to the beneficiary in, at most, 10 seconds for 0.2 euro cents.

In TIPS, we aim to settle those transactions within a fraction of a second, in central bank money, with Europe-wide reach and interoperability. So it is with conventional technology, not with VCs, that genuine progress is being made in payment processing.
Unit of account

The second function of money is acting as a unit of account, without which buyers and sellers would have to know how many chickens an iPhone would be worth, how many iPhones would buy a house, and so forth. Such a system quickly becomes complex: just ten products already have 45 bilateral pairs of prices.

Money simplifies the comparisons of value between products. VCs fail this test - none of them are generally accepted as a unit of account. A unit of account is like a flag or an anthem, a representation of commonness backed by assets and values which is even accepted beyond the territory of legal tender.

In part this is due to the lack of widespread recognition. VCs are not legal tender, and are not backed by a central bank. Retailers accepting such assets as payment undertake notable risks, including potential expropriation by hacking or by an enforced rollback.

But the lack of acceptance as a unit of account is also down to the final function of money - being a store of value.

Store of value

Wild fluctuations in the value of VCs mean that businesses pricing in VCs could find themselves with a large and detrimental gap between their actual price and their optimal price.

A stable value is required to underpin effective pricing. Similarly, households benefit from being able to optimise their spending over time by saving. To do so, they need an effective store of value that they can be sure will enable them to buy goods and services in the future.

When there is considerable uncertainty around how many goods and services an asset can buy in the future, or indeed whether it can be used to purchase anything at all, it is a poor store of value.

Traditional currencies have a trusted issuing authority that acts as a guarantor of the stability of the currency, and a legal framework that punishes counterfeitors.
The ECB's mandate for price stability, bolstered by the treaty provision for independence, provides consumers with the confidence that the purchasing power of their euro will remain stable from year to year.

The political capital the leaders of the euro area's countries invested during the crisis to confirm the integrity of the euro proved all sceptics wrong.

There are no equivalent structures in place for VCs. They have neither intrinsic value, such as the commodity content of gold coins, nor extrinsic value, such as the value assigned to traditional fiat currencies by the trusted public issuing authority.

VCs do not even provide the dividend or coupon payments that tie down the prices of equities and bonds. They are in fact a classic Keynesian beauty contest, where investors buy what they perceive others view as the most attractive investment.

Like in Mr Ponzi's schemes, those investors hope for future price gains and believe they will find a greater fool to sell to before the inevitable crash. Under these conditions, VCs exhibit wild fluctuations in value, meaning that they cannot be trusted as a store of value.

It is this failure, more than any other, that makes the label "currency" a misnomer.

**Public versus private provision of money**

Having a widely accepted unit of account and medium of exchange helps smooth economic transactions, reduce costs and enable some interactions to take place that would not be possible under a pure barter system.

There are clear network and scale effects with money, which provide one justification for public issuance. Even Milton Friedman recognised this, noting that "a moderately stable monetary framework seems an essential prerequisite for the effective operation of a private market economy."

It is dubious that the market can by itself provide such a framework. Hence, the function of providing one is an essential governmental function on a par with the provision of a stable legal framework."

But that does not mean that private sector money is either impossible or undesirable. Forgotten amid the hype surrounding VCs is that a widely accepted form of private sector digital money already exists: bank deposits.
This private sector money dwarfs the amount of public sector money - i.e. cash - in circulation. In November 2017, euro notes and coins in circulation amounted to €1.1 trillion, compared with the €17.5 trillion deposited by euro area residents with MFIs.

Certainly this private sector money acts as an effective medium of exchange and, a few episodes aside, as an effective store of value. But such private sector money is not truly independent; it shares its unit of account with the official currency.

The implicit promise underlying bank deposits is that customers can redeem them whenever they wish and one to one with public sector cash, if they need a safe refuge in a time of crisis.

By providing liquidity to the banking sector and acting as lenders of last resort, central banks de facto recognise this private sector money, even if it is not legal tender.

But that recognition comes with obligations - including regulations on capital, liquidity, anti-money laundering (AML) and counter terrorist financing (CTF).

For VCs to cross over into the mainstream, regulatory acceptance is necessary, and that acceptance requires equivalent measures for governance and legal certainty.

**Potential impact of virtual currencies**

Yet even if VCs are not money, central banks should still be aware of the potential risks they pose for price stability and financial stability. The magnitude of such risks depends on the total value of VCs outstanding, their interconnectedness with the rest of the economy, and the extent to which investors in VCs are leveraged.

In terms of interconnectedness, the main concerns would be if a significant crash caused losses of wealth that were large enough to affect consumer behaviour, or caused contagion through the financial system. The bursting of the tech bubble in 2000 provides a useful comparison for the first scenario.

The market valuation of the NASDAQ fell by around $5 trillion between March 2000 and October 2002, roughly 20 times the current total value of VCs outstanding. How holders of VCs consume out of their perceived
wealth and how much is built on leverage are crucial to determining the impact of a crash.

Until recently, VCs have lacked perceptible connections to the financial system. Regulatory requirements on the use of certain types of money or settlements, the high risk of money laundering associated with the lack of customer identification, the speculative pricing of VCs and the limited liquidity are some of the reasons why regulated institutions have refrained from getting involved in this asset class.

Yet there are signs that greed has weakened their resolve and some have begun to form tentative linkages. A number of derivative products pertaining to VCs have recently been launched.

There is rising activity in euro at VC exchanges and some jurisdictions are falling over each other to issue licences to largely unregulated platforms and exchanges in a misplaced competitive race.

What happens if this trend continues and VCs become more commonplace as settlement assets in some niches of financial markets? What if credit institutions start developing larger exposures to these assets? What if retail investors take out mortgages to buy VCs?

Amid the growing risks of contagion and contamination of the existing financial system, regional regulatory solutions have to be explored while we await an outcome from G20 discussions. Indeed, we ultimately need global answers in the absence of a defined jurisdiction for VC issuance.

This is crucial to safeguard the integrity of financial sector services, avoid the undue mutualisation of risks, protect investors and consumers and prevent negative spillovers to the real economy.

Resolute ring-fencing measures might be needed. Reviewing and updating legislation in a timely fashion is a continuous challenge, yet inaction could be perceived as condoning VCs.

The four broad areas that require particular attention are:

- VCs themselves;
- the facilitators - VC exchanges, wallet-providers and brokers;
- financial market infrastructures (FMIs); and,
- the banking sector.
Regulating virtual currencies

Beginning with the VCs themselves, it is clear that they cannot be directly regulated or overseen in the absence of a centralised governance and legal framework.

In fact, most VCs are "mined" peripherally by a computer programme explicitly to prevent any legal entity being in control. Recognising their limits here, most countries tolerate the usage of VCs, without trying to ban them.

Many regulatory bodies and central banks have issued warnings, and this is certainly important from a consumer protection viewpoint. Retail investors need to understand the predominantly speculative nature of VCs and the risks they entail.

Statements regarding returns on investment in VC-related advertisements targeting potential investors should be under the same level of scrutiny as advertisements for financial products.

In the United States, awareness of the growing inherent risks to investors and consumers is on the rise. The Securities and Exchange Commission (SEC), which oversees the US investment industry, warned in a letter sent last month to two trade groups that, "there are a number of significant investor protection issues that need to be examined before sponsors begin offering these funds to retail investors."

The SEC outlined more than 30 questions that had to be answered before it would give the green light to mutual funds and exchange-traded funds (ETFs) that invest in Bitcoin and its peers.

The concerns refer in particular to the establishment of Bitcoin ETFs, some of which even use leverage to amplify the price movements. The extreme volatility in recent months highlights the large degree of speculation involved.

Likewise, the lack of liquidity is concerning. If many investors want to withdraw their money from the ETFs on a particular day, the funds might struggle to meet the redemptions because they would struggle to sell off their atypical assets.

And how would such funds deal with cases of market manipulation, as have happened in the past? Clarity on such aspects is vital.
In the same vein, relevant market authorities should monitor, analyse and regulate the use of ICOs. An ICO is a way of raising money from the public, often to start a project or to finance a company, using coins or tokens. In an ICO, an entity issues newly created coins or tokens and offers them in exchange for fiat currencies, such as the euro, but more often VCs.

In 2016, the total amount of funds raised through ICOs was less than €82 million. This number has dramatically increased to over €3 billion raised through ICOs in 2017.

Potential explanations for the increasing popularity of ICOs is that they allow companies to raise funds without ceding control to venture capital investors, or enduring the rigour and expense of an IPO process involving a legally binding prospectus, among other things.

Depending on their features and characteristics, ICOs can be regarded as either the issuance of VCs, as utility tokens to access or purchase a service or product, or as securities. In the latter case in particular, clarification is needed on the extent to which ICOs should be bound by existing regulations, such as on disclosure and prospectuses. This is particularly relevant when tokens are exchanged for fiat money.

**Restraining the facilitators**

Let me turn to the facilitators of the spread of VCs.

Vigilance is warranted in view of the repeated incidents, most recently the hack of the Tokyo-based VC exchange Coincheck, where €430 million of virtual currency was stolen.

Although there is no specific evidence to confirm the suspicions, security experts are increasingly warning that VCs could offer rogue states a route to circumvent sanctions and gain access to foreign currency and world markets.

The ECB takes an active role within our mandate, for example our opinion on the 5th Anti-Money Laundering Directive, which will extend the scope of obliged entities to cover exchanges and wallet-providers handling VCs, in order to avoid anonymous transfers into fiat currencies.

The ECB reminded the EU legislative bodies that they should not be perceived, through regulatory forbearance, to be promoting VCs, and should take VCs’ inherent stability risks into consideration.
But we need a broader perspective on regulatory intervention for VC facilitators that extends beyond the fields of AML and CTF.

Possible regulatory action should be explored, as well as amending or broadening existing frameworks such as the revised Payment Services Directive (PSD2) so that the licensing and supervision rules also apply to VC facilitators.

Protecting financial market infrastructures

Third, I would like to cover financial market infrastructure services. One could envisage a major incident involving VCs triggering contagion from the market infrastructure services themselves to their participants, and even beyond.

Against this background, we have to review whether the regulatory and oversight tools in the field of trading, clearing and settlement require updating.

One of the key questions is whether VCs could become a settlement asset in payments and settlement services or be used in the clearing domain. Existing standards for FMIs, for example, refer to the usage of "a settlement asset with little or no credit and liquidity risk".

While it could be argued that this by and large excludes settlement involving VCs in payment systems, it should be borne in mind that this definition currently does not systematically apply to all FMIs. The situation is similar in the field of securities settlement.

The question is whether VCs could be used as an asset for settling securities transactions or constitute a security per se. The answer hinges on whether they could be legally characterised as "financial instrument/financial asset" under the applicable regulation.

Certain authorities have already qualified VCs as financial instruments or commodities and this may prepare the ground for the issuance of some specific VC-related products, including derivatives.

VC derivative activities need to be fully transparent and records must be collected, maintained and made available by trade repositories.
The use of VCs at **central counterparties (CCP)** should also be monitored. The European Market Infrastructure Regulation (EMIR) states that a CCP shall accept highly liquid collateral with minimal credit and market risk to cover its initial and ongoing exposure to its clearing members.

While it is doubtful that a VC would meet such a requirement, clear guidelines ex ante would be helpful, and financial stability considerations will need to be taken into account by the relevant authorities.

In my view, it should be examined whether any VC activity carried out by FMIs must be ring-fenced from their other activities. The enforcement of segregated accounts and liabilities could be discussed.

FMIs play an important role in financial markets, and any liquidity support offered by central banks should be to mitigate shocks emanating from the real economy, not from gambling in risky assets.

Certainly, FMIs should not be obliged by legislation to provide settlement services for VCs and VC-related products. In the same vein, the Eurosystem market infrastructure services - TARGET2 and TARGET2-Securities - cannot grant access to VC business according to their existing framework.

**Regulating credit institutions**

Finally, we need to look at the banking sector, whose profitability and stability might be impaired by VC activities. EU credit institutions are already required to have adequate frameworks in place to assess the capital they need to cover the nature and level of risks they are, or might be, exposed to.

Given the volatile nature of VCs, it could seem appropriate that any trading in VCs would be backed by adequate rates of capital, and segregated from their other trading and investment activity.

Any VC business of credit institutions needs to be rigorously supervised to ensure that risks emerging from such activities are contained.

This includes ensuring that **proper protocols** are in place to meet obligations under AML and CTF regulations.

Furthermore, given the risks posed by leverage, credit institutions should not accept VCs as collateral, or only accept them with haircuts that
appropriately reflect past volatility, liquidity, and market and operational risks. Likewise, limits on leverage could be examined.

Central bank issuance of digital currency

The advent of VCs has triggered suggestions that central banks should provide central bank digital currency, or digital base money (DBM), as I have previously called it.

DBM already exists in terms of the reserves of the banking sector held at the central bank, but the more recent question is whether central banks should make DBM more widely available.

As with every central bank policy decision, any such move would need to be both necessary and proportionate. There would need to be a clear motivation within our mandate to issue DBM, and such issuance would need to be done in a way that did not bring about risks and costs that exceeded the benefits.

It is important to avoid being beguiled by the flashing lights of novelty and assuming that, just because a technology is new, it is also better.

There is no material evidence that abolishing cash will inhibit crime. Electronic storage and transfer may well prove easier for criminals than banknotes. I’m also uncertain why cash is being singled out; mobile phones and cars are also used in crime, but there are no calls for their abolition.

Moreover, there does not appear to be a global trend towards a cashless society. A recent study conducted by the ECB finds that around 79% of all payments at point-of-sale were made with cash.

Indeed, the demand for cash in the euro area currently outstrips the rate of nominal GDP growth. And people who currently prefer electronic payments already have a wide range of options available, without needing the central bank to provide the digital money.

A further argument for introducing DBM and abolishing cash is framed in terms of monetary policy.

Several authors have proposed DBM as a way to eliminate the effective lower bound on interest rates, and impose much more negative interest rates than are currently possible.
But such rates are not necessary; the unconventional measures put in place by central banks over the past decade have proven sufficient to meet the challenges of the crisis.

And while sharply negative interest rates may work well in some macroeconomic models, unforeseen changes in real-world behaviour by households and businesses could inhibit the effectiveness of this tool and achieve nothing more than the destruction of confidence in central bank money. Whether this would work to the advantage of private moneys with large disorders in exchangeability remains to be seen from a social welfare point of view.

The decision on issuing DBM also needs to be assessed in relation to the impact on the financial system. During a systemic banking crisis, holding risk-free central bank issued DBM could become vastly more attractive than bank deposits. There could be a sector-wide run on bank deposits, magnifying the effects of the crisis.

Even in the absence of a crisis, readily convertible DBM could completely crowd out bank deposits - putting the existence of the two-tier banking system at risk. In this situation, the efficient flow of credit to the economy would likely be impaired.

The central bank - now holders of deposit funding - would have to decide which projects were financed, either directly by replacing commercial banks, or indirectly by deciding which banks received funding. This is an undesirable situation for European central bankers for two reasons:

- Legally, the Treaty provides for the ECB to operate in an open market economy.

- And, by the same logic, we are well aware of Friedrich von Hayek's warnings about "the pretence of knowledge". Decentralised market decisions are the "first choice" when it comes to allocating resources in an optimal way. This includes the allocation of credit.

Overall, there is currently no convincing motivation for the Eurosystem to issue DBM to the general public. It is unnecessary at present and, when the likely negative impacts on the financial system are taken into account, such a move appears disproportionate to the aims put forward by its proponents. There is no need to fix something that is not broken.
If anything, one could imagine a digital representation of cash that replicates the features of cash in the reasonably distant future, if citizens demanded it.

Such an approach seems more appropriate for jurisdictions whose currencies face domestic regress as they are also not widely accepted beyond their territory - which is certainly not the case for the euro.

**Conclusion**

Let me conclude.

Virtual currencies are not money, nor will they be for the foreseeable future. Their market share is still small and their ties to the real economy are still limited.

But this can be subject to change. Regulators and legislators on all levels should therefore urgently pay close attention to mitigating the potential risks that could stem from growing VC business.

It is not unknown for new innovations to bring about euphoria and hype, which in turn fuel bubbles that eventually burst. And indeed, the hot air is already escaping from some of these bubbles.

But just because the initial euphoria and hype subsequently fade, it does not mean that the innovation is without virtue, even if early market leaders may not last the distance.

Despite the many defaulted railroad bonds, railways are a common mode of transport today. From London you can even take a train directly to many parts of Europe through the Channel Tunnel - whose now profitable operator filed for bankruptcy protection in 2006.

Netscape and AltaVista were titans in the early days of the internet. Web browsers and search engines are still with us, but those names are no more. So it may well prove with VCs. The technology may in time become widespread and useful, but early versions of it may fade from view.
The Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) announced its 2018 examination priorities.

OCIE publishes its exam priorities annually to improve compliance, prevent fraud, monitor risk, and inform policy.

Of particular interest this year will be matters involving critical market infrastructure, duties to retail investors, and developments in cryptocurrency, initial coin offerings, and secondary market trading.

"I appreciate OCIE's dedication to maximizing the effectiveness of their resources with a keen eye toward asset verification, market infrastructure, and duties owed to retail investors," said SEC Chairman Jay Clayton.

"As the markets continually evolve and the products and services available to investors adapt, OCIE remains committed in its risk-based examination program to prioritizing the interests of retail investors and examining those aspects of securities firms posing risks to investors and the proper functioning of our capital markets," said OCIE Director Pete Driscoll.

This year, OCIE's examination priorities are broken down into five categories:

(1) compliance and risks in critical market infrastructure;

(2) matters of importance to retail investors, including seniors and those saving for retirement;

(3) FINRA and MSRB;

(4) cybersecurity; and

(5) anti-money laundering programs.
Compliance and Risks in Critical Market Infrastructure – OCIE will continue to examine entities that provide services critical to the proper functioning of capital markets.

OCIE will conduct examinations of these firms which include, among others, clearing agencies, national securities exchanges, and transfer agents, focusing on certain aspects of their operations and compliance with recently effective rules.

Retail Investors, Including Seniors and Those Saving for Retirement – Protecting Main Street investors continues to be a priority in 2018.

OCIE will focus examinations on the disclosure and calculation of fees, expenses, and other charges investors pay, the supervision of representatives selling products and services to investors, and the execution of customer orders in fixed income securities.

OCIE will continue to monitor the growth of cryptocurrencies and initial coin offerings and examine registrants involved in their offer and sale to ensure that investors receive adequate disclosures about the risks associated with these investments.

FINRA and MSRB – OCIE will continue its oversight of FINRA by focusing examinations on FINRA’s operations and regulatory programs and the quality of FINRA’s examinations of broker-dealers and municipal advisors.

OCIE will also examine MSRB to evaluate the effectiveness of select operations and internal policies, procedures, and controls.

Cybersecurity – Each of OCIE’s examination programs will prioritize cybersecurity with an emphasis on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

Anti-Money Laundering Programs – Examiners will review for compliance with applicable anti-money laundering requirements, including whether firms are appropriately adapting their AML programs to address their regulatory obligations.

The published priorities for 2018 are not exhaustive. Further, additional priorities may be added in light of market conditions or as OCIE identifies emerging risks and trends. The collaborative effort to formulate the annual examination priorities starts with feedback from examination staff, who are
uniquely positioned to identify the practices, products, and services that may pose significant risk to investors or the financial markets. OCIE staff also seek advice of the Chairman and Commissioners, staff from other SEC Divisions and Offices, the SEC's Investor Advocate, and the SEC's fellow regulators.
At the crossroads - innovation and inclusive growth

Carolyn Wilkins, Senior Deputy Governor of the Bank of Canada, at the G7 Symposium on Innovation and Inclusive Growth, Montebello, Quebec.

Ooh, standin' at the crossroad, tried to flag a ride
Ooh-ee, I tried to flag a ride
Didn't nobody seem to know me, babe, everybody pass me by
"Cross Road Blues" by Robert Johnson, 1936

Introduction

Welcome to Canada-and to a snowy Montebello. This day is dedicated to a discussion about innovation and inclusive growth. It is great to have so many experts with us today. Thank you.

We know that technological advances are key to improving an economy’s potential to grow. They have raised living standards in G7 countries and across the globe, and have helped lift more than one billion people around the world out of extreme poverty since the Second World War.

The current wave of innovation—digitalization and automation—promises to raise trend growth in the economy even more.

However, as we are discussing today, technological advances can leave people behind. It is perhaps only in the last decade or so that mainstream macroeconomists have sharpened their focus on how income distribution may affect long-term growth and macro dynamics. There is compelling evidence that innovation has been an important reason behind rising income inequality in advanced economies in recent decades.

Research also finds that rising inequality can result in weaker and less-stable macroeconomic outcomes. This places us, as policy-makers, at a
crossroads. Do we choose to stay on the same road and repeat the past? Or do we apply fresh thinking to policy and choose a new road where innovation delivers even stronger and more-inclusive growth?

This is the challenge that the G7 countries have set for themselves for 2018. Canada is proud to lead the G7’s work this year to better understand the issues so that we can set priorities for policy.

The context we are working in matters. The global economy is enjoying the most robust and synchronous growth we’ve seen in close to a decade. Businesses and consumers are feeling more confident. Yet, we know that many people in advanced economies are also anxious about what digitalization and automation might bring.

They are worried about being left behind. For workers in some industries, such as manufacturing, this may seem like old news. For drivers, lawyers, investment advisors and many others, it's new. By some estimates, close to half of the tasks done by workers could already be automated using current technology.

This anxiety has real costs. It has eroded trust in the framework for international co-operation in areas that have served us well in the past: trade policy and financial sector regulation are good examples.

As a way of spurring discussion today, I will cover three points:

- Technological progress will raise economic growth, although the channels through which it contributed to rising inequality in the past are still forces to be reckoned with.

- It doesn't have to be this way—if we apply fresh thinking in some key areas, we can make policy choices that manage the side effects of innovation, without stifling it.

- Policy-makers themselves need to dig into the technology—the better we understand it and the underlying business incentives, the better policy choices we will make.

The past provides insight for the future

Technology has transformed our daily lives at an astonishing pace. Google is not yet 20 years old. Who knew, even 5 years ago, that some people would be making a small fortune as professional video-game players?
And, while parents have been worrying about how much screen time their kids should have, a growing number of professions—from firefighters to surgeons—have embraced the "gamification" trend, integrating video exercises into their training programs.

Let's remember that per capita output has increased around five times in G7 countries since the early 1950s. Our average life expectancy during this period has risen from 67 to 81 years.

Not bad. Yet, recent voting behaviour and public discourse make it clear that many people question what is in it for them and their families when it comes to technology and globalization. A study here at home showed that the more pessimistic people were about technology, the more worried they were about their own prospects.

Many of us would agree that the data point to a concerning trend. The share of income going to labour has been declining in many economies, including the G7.

The share of income going to the top 1 per cent has nearly doubled since 1980 in some of our countries, amounting now to as much as 20 per cent.

If we want to find a better road forward, identifying the underlying issues is the right place to start. One question is, what is it exactly about innovation—and, to a lesser extent, globalization—that opens the door to these outcomes? There’s a lot of good research, including by people in this room, pointing to many possible forces at play. I think three stand out:

- **Technology has benefited skilled workers more than other workers because it has made them more productive.** People in more-routine jobs have tended to be replaced entirely. Digitalization will likely reinforce this dynamic. Machine learning and other technologies mean that tasks requiring routine cognitive skills, such as reading medical scans or preparing legal and investment advice, can now be automated too.

That said, I do not share the dystopian view of a world without workers. People will still have an absolute advantage in tasks that require common sense and a human touch. And they will also find employment in areas where they have a comparative advantage. The question is not so much whether there will be jobs for people, but, rather, how well they will pay, and what the working arrangements will be.
Some types of technology lead to market concentration and the rise of "superstar" firms. These firms tend to have fewer employees than conventional companies and can earn impressive monopoly profits. Market concentration happens quite naturally in industries with prominent network effects and other scale economies. There is nothing new in that.

Phone companies are traditional examples, and social media companies and online marketplaces are more-modern examples. What is new is that the "winner-takes-all" effect is magnified in the digital economy because user data have become another source of monopoly power.

Data from a large network create a formidable barrier to entry. Another barrier to entry can come from firms using their position as gatekeepers to crucial online services to impede their competitors. And, it's easier to avoid taxes when production is not tied to a large factory with a fixed physical location.

Technology has helped to separate work into discrete tasks, allowing businesses to make more use of short-term, temporary jobs to maintain flexibility or respond to changing needs. Workers in these types of jobs tend to have less bargaining power than regular employees. They usually earn lower incomes, get fewer benefits and have less job security.

This may be one reason why we have seen relatively weak wage growth in Canada and other G7 countries despite improving labour market conditions. With the current wave of innovation, the "gig economy" is likely to keep growing.

It doesn't have to be this way

We do not have to be hostage to these forces. That's my second point. Canada's priority as G7 host is to find ways to embrace technological progress while handling the challenges of digitalization and automation.

Adequate income and equality of opportunity are critical to handling the challenges of the digital economy. Adequate financial incentives to innovate and take ideas to market are critical to embracing technological progress. Trade-offs need to be made between these two objectives, and there are different views about what "adequate" means in practice. It is the job of governments to make these important choices, not central banks.
In any case, central bankers do not have the mandate or the tools to directly influence the pace of technological progress or the distribution of income. We do have a stake in supporting strong and sustainable growth, and that is why we play an important advisory role and help shed light on some of the trade-offs at play.

There are many policy areas to consider. Let me talk about a couple that I think should be priorities: developing skilled workers through inclusion, and keeping market power in check.

**Developing a skilled workforce**

Developing a skilled workforce is about education, training and continuous learning. It’s also about reducing the barriers to participation in the workforce.

We know that the fields of science, technology, engineering and mathematics (STEM) are an important part of the equation. Businesses in Canada tell us that it is increasingly difficult to find the right people in these areas, and I imagine this is the case globally.

The obvious implication is that we need to find better ways to make these fields of study more accessible and interesting to students, starting at an early age. **Improving our track record** in terms of gender balance would add to the pool of STEM skills, but this will require some new ideas.

We also know that on-the-job training and reskilling will become even more important because of the accelerating pace of change. Even a recent graduate may not have the exact skills needed to be a perfect match for the job. An increasing number of mid-career employees may find that their skills have become obsolete and that retraining is needed.

As Governor Stephen S. Poloz mentioned recently, we will need more engagement from businesses to tackle this issue. They are **best placed to know their own people and their own business needs in real time**.

The question is, how can public policy and academic institutions encourage and complement any new efforts by businesses? Each of our countries has interesting approaches to build on. **Germany’s apprenticeship program** is well known and established. It has been successful in giving students valuable vocational training while also meeting business needs.
The Creative Destruction Lab in Canada is a lesser-known example in the tech field of universities working with students and businesses to bring the best ideas in science, machine learning and artificial intelligence to market.

Let's not forget that technology itself can be used to better match people with jobs, and to attract people into the labour force and keep them there. This will strengthen sustainable economic growth while supporting inclusiveness at the same time. Finding ways to include more women in the labour force, and empower them, is a priority for the G7 this year.

Another promising avenue to explore is how to adopt technologies that remove barriers for people with disabilities. Right now, just over 10 per cent of the labour force across the G7 consists of persons with disabilities. If their employment rate were raised to the same level as that for the rest of the labour force, we could add up to 12 million workers.

Chat and email functions on our phones have already transformed workplace accessibility for the hearing-impaired. Entrepreneurs in Canada and elsewhere are developing technology to help people who are visually impaired see far-away details. Soon, driverless cars will help make people with a range of disabilities more mobile. As governments work to nurture innovative tech start-ups, they could emphasize technologies to enhance workplace and social inclusion.

**Keeping market power in check**

We are not going to get the full benefits of innovation if we leave market power unchecked.

I'm focusing on the tech industry because the discussion is about digitalization, but some of my points could apply elsewhere. The five biggest global technology companies have a market capitalization of about US$3.5 trillion. That's almost one-fifth of the size of the US economy.

The tech industry is making a valuable contribution to our economic performance. That said, the size and market dominance of some of the tech firms raise many of the usual concerns about the potential effects of monopoly power on prices and competition.

A new source of market dominance relates to data. Access to and control of user data could make some firms virtually unassailable.
They can easily drive out competition by combining their scale with innovative use of data to anticipate and meet evolving customer needs, at a lower price (and sometimes for free). This has a couple of undesirable consequences.

**First**, firms operating in less-competitive environments innovate less; we need the dynamism from firm entry and the contestability of markets to raise the trend line on growth as much as possible.

**Second**, the biggest firms may well return to monopoly pricing in the long run. These consequences get in the way of stronger, more-inclusive growth.

That is why we should prioritize the modernization of anti-trust and competition policy, as well as the relevant legal frameworks. There are many unanswered questions, especially about how best to remove barriers to entry.

If user data are the primary source of monopoly rents in the digital age, how should we regulate who owns these data and how they are shared? Some interesting ideas include giving users control of their data—perhaps even making firms pay users for their data—and regulating tech platforms as utilities. Intellectual property rights present similar issues.

Patents are a key way to protect the return on valuable research and development. Given that they create barriers to entry and that the pace of technological change is accelerating, do we need to rethink our approach? It is good to see authorities across the G7 countries looking at all these issues.

International collaboration is necessary because of the ubiquity and cross-border nature of many digital services.

**New technologies pose additional regulatory and legal questions.** For example, the sheer complexity of algorithms used for data analytics makes them difficult to interpret, audit and govern. In some cases, algorithmic pricing could lead to tacit collusion-price fixing without the quiet glass of scotch between commercial rivals.

Even if it were identified, tacit collusion would not meet some current legal definitions of collusion.

Legal clarity is also required in many jurisdictions with respect to data privacy, information security and consumer rights.
We also need to determine how best to manage the risks that concentration in digital services can pose for the financial system.

Top of mind for me are the growing operational risks (including cyber risks) from a very concentrated set of third-party service providers that our financial institutions use—cloud services, data aggregators and related analytics.

How concerned should we be about these third parties—telecommunications companies and tech companies—given that they typically fall outside the current regulatory perimeter? This is another question that would benefit from concerted attention at the international level. Good progress is already being made on issues related to international taxation to avoid base erosion and profit shifting.

**Policy-makers need to dig in**

This brings me to my final point. Policy-makers need to dig in and be proactive. Good policy decisions can only come from a clear understanding of the new technologies and the related business incentives.

Let me give some examples from my own backyard.

At the Bank of Canada, we are focused on understanding the many ways in which digitalization and automation are affecting the economy and the financial system. For example, as non-traditional pricing models become more prevalent, we are rethinking how best to measure inflation.

We are looking at how digitalization might be affecting labour markets and the transmission of monetary policy, and how a global digital marketplace for goods and services changes the ways in which domestic inflation pressures are generated.

Our researchers are also studying emerging technologies in financial services to understand how the ecosystem is evolving, and to spot new risks as they emerge.

The workforce needs to have the right skills for the digital economy. So do public policy-makers. The Bank of Canada has several irons in the fire that take a learning-by-doing approach; one example is the work staff are undertaking to apply machine learning and techniques such as distant reading to analyze vast amounts of unstructured information.
The goals are to increase the range and depth of skills of our staff, improve our projections and reduce the uncertainty we face when making policy decisions.

We are also working on how we could use machine-learning applications to increase efficiencies and manage operational risks in all parts of our business. All the institutions represented in this room are doing interesting work in this area.

Public sector institutions need to innovate in their business cultures. We should be open to more-diverse perspectives and expertise, work more often with private sector experts and take manageable risks.

The Bank of England and the Monetary Authority of Singapore are leaders in exploring fintech with the private sector.

The Bank of Canada also has several experiments under way. One is in partnership with the TMX Group and Payments Canada. It uses distributed ledger technology to build a delivery versus payment settlement system for securities.

Our experience with these types of partnerships so far is that we can quickly harness deep subject matter and business expertise, define realistic yet ambitious objectives and make faster progress than if we were working alone.

It's good to see that G7 central banks, among others, have already been comparing notes on our work in these areas.

**Conclusion**

It is time to conclude. I do not need to convince you that the digital economy is a promising way to raise trend growth and overall living standards. We cannot be satisfied, though, if some of the potential gains are left on the table, because many people will be left behind and important markets will be virtually uncontestable.

It does not have to be this way if we choose a road for policy that effectively manages the downsides of innovation without stifling it. Of all the areas where we could develop and implement a better strategy, here are my top three:
(i) develop a dynamic workforce with the skills to match the jobs, and encourage more labour force participation;

(ii) keep market power in check, particularly the power that comes from control of consumer data, to encourage competition and limit monopoly profits; and

(iii) manage the growing operational risks associated with the digital services that are provided by a concentrated set of firms to systemically important financial institutions.

We will need to judge wisely when it is best to use public policy tools to manage risks and when to let private enterprise work its magic. We'll need to work together and in the field to inform these judgments.

I am confident that, together, the G7 will show leadership and will build with the private sector a shared sense of responsibility for the future.

I would like to thank Gurnain K. Pasricha, Lori Rennison and Eric Santor for their help in preparing this speech.
For the fifth consecutive year, last October the European Cyber Security Month (ECSM) campaign was successfully executed across Europe.

The campaign was coordinated and supported by ENISA, the European Commission, Europol’s Cyber Crime Centre (EC3), European Banking Federation, the Estonian Information Systems Authority and cyber security organisations from the Member States.

The support for which propelled the campaigns success as measured by both the qualitative and quantitative data compiled.

Although this year’s campaign continues to break new records, the conclusions of this report highlight a number of fundamental areas that need to be addressed in the coming years if the campaign is to continue to grow and more importantly influence the security behaviour of citizens online.

Citizens across Europe face similar information security threats and information asset vulnerabilities; this is because most of the platforms, operating systems and devices used are produced by the incumbent global product/service providers.

This applies to mobile phones, email messaging services, laptops and social media channels, since the vast majority of European citizens use similar technologies.

However, citizens of each Member State have different levels of cyber security knowledge and behaviour.

These differences across Member States may be triggered by the disparity of Member States in their commitment to awareness raising.
In particular some Member States have a dedicated team of experts for planning and executing national security awareness campaigns; for example, the BSI in Germany and the ANSSI in France.

Other Member States assign this role to a Ministry or Government CERT alongside their other core activities without a dedicated representative.

The effects of this is that there is a discrepancy between the measures that citizens may apply for the same or similar vulnerability or risk is one Member State compared to that of another Member State.

An example of the situation, the Eurobarometer survey highlights many differences across Member States in the use of cyber security measures, such as firewalls or the awareness of phishing attacks.

Therefore, the different level of citizens’ awareness and the potential risk-taking behaviour across Europe in turn leads to an increase in the risk level of Europe as a whole.

The concept for the European Cyber Security Month is to address this disparity across Member States in two stages.

**The first stage** is to support the Member States so that the awareness and behaviour of citizens in each Member State is raised to a mature baseline.

This becomes the reference baseline across the whole of Europe and thereby the European Cyber Security Month aligns the risk levels across Europe.

**The second stage** is to further lower this risk by raising the maturity of citizen’s behaviour in unison; at the European level.

ENISA and the European Commission can achieve the objectives of the European Cyber Security Month by driving the pan-European campaign so as to ensure all Member States are actively committed to the European Cyber Security Month and that industry is also involved at all levels of the campaign both at the local and European level.

The ground work is in place for the European Cyber Security Month to move to the next level. **This next level will be achieved** only once a governance structure has been put in place as highlighted in the conclusions of this report.
Furthermore a governance structure will ensure that the campaign is driven by MS as they are ultimately the benefactors of the campaign.

A secondary reason for establishing a governance structure is to achieve another goal raised in the conclusions of this report which is to increase the commitment of the MS to the campaign and to bring on board those MS that have yet to designate a competent body to the campaign.

This report provides an overview of the activities organised and presents a synthesis of findings on the basis of evaluation and performance information gathered via a questionnaire and media monitoring data.

The report is structured into three main parts: an introduction, the implementation phase and an evaluation of the campaign. The introduction will provide readers with the policy context, scope and target audience of the campaign.

The implementation phase of the report highlights the milestones that were achieved during the planning and execution phase of the campaign.

This includes how events were organized and co-ordinated with partners, marketing materials used and insights into the execution of the campaign including results.

The final section of the report deals with the evaluation of the campaign, comparing this year’s results with the previous year’s and also provides input from the partners that was generated via a questionnaire; and finishes with a conclusion and outlook for the future.

Documenting the activities of ECSM 2017 will assist in the organization and execution of future ECSM campaigns and allow for comparing the campaign with the results from previous years.

The evaluation results and estimated impact of ECSM activities will provide the opportunity to discuss lessons learned deriving from this exercise and to help draw attention to related concerns and opportunities for further improvement.

Finally the report is intended to provide a basis for discussion among the Member States, the European Commission and ENISA on how the ECSM can best be organised in the years to come.
All Member States will need to face up to similar challenges, namely how to engage citizens and organizations so as to affect their information security behaviour.

Cryptomining trends

News articles have focused recently on the value and volatility of cryptocurrencies, over the past year, most notably Bitcoin which had a peak value of $20,089.00 in December 2017.

Cryptocurrencies can be earned, or ‘mined’, by performing computationally intensive operations to support the running of the currency. Malware intended to mine cryptocurrencies on victim computers has been available since at least 2013 and surged in popularity in late 2017 as the currencies’ value increased.

Cryptomining malware is attractive to cyber criminals as they are able to use botnets of compromised machines as miners without having to cover the infrastructure costs (e.g. the cost of electricity would be covered by the victim).

Despite the potentially lucrative rewards, cryptomining is becoming increasing economically unviable for some legitimate users as the running costs (hardware and associated electricity costs) often outweigh any potential gains in this increasingly competitive environment.

This has also had real world implications on the price and availability of graphic cards as many are now being purchased specifically for cryptomining.

For cyber criminals, cryptomining malware has some advantages over ransomware. It doesn’t rely on the victim being willing and/or capable of making payment. It is also not confrontational but is designed to operate undetected in the background over a long period, potentially earning more money than a ransomware campaign.

More importantly, it can be distributed through same delivery mechanisms as ransomware (e.g. exploit kits) and, once established, a network of mining bots can generate a respectable amount of money with minimal effort (e.g. the Smominru botnet generates 24 XMR per day (approximately £8,500)).
Monero is the preferred currency as the processing power required to mine it is minimal compared to that required to mine Bitcoin.

It is highly likely that the criminal deployment of cryptomining malware will increase during 2018 as cyber criminals either shift their focus away from other forms of malware or run these campaigns alongside their established cyber criminal activities.
IT security: BaFin specifies requirements for the banking industry
Bundesanstalt für Finanzdienstleistungsaufsicht

BaFin has published the Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT).

The BAIT have now become the cornerstone of IT supervision for all credit and financial services institutions in Germany.

The requirements are directed at the management boards of such companies.

The objective of the BAIT is to create a comprehensible and flexible framework for the management of IT resources, information risk and information security.

They also aim to contribute towards increasing awareness of IT risks throughout the institutions and in relation to external service providers.

Furthermore, they provide transparency about what banking supervisors expect from the institutions with regard to the management and monitoring of IT operations, including the user access management that this necessitates as well as requirements for IT project management and application development.

Overall, the BAIT address those subject areas which BaFin has identified as particularly important based on its experience of IT inspections.

One on the primary objectives of the BAIT is to improve awareness of IT risks at institutions, especially at management levels.

Banking supervisors understand the term "IT risk" as meaning all risks to the institution's financial position and financial performance that arise from deficiencies relating to IT management, the availability, confidentiality, integrity and authenticity of data, the internal control
system for IT organisation, the IT strategy, IT guidelines and IT topics in the rules of procedure, or the use of information technology.

To read more:
The future relationship between Germany and the UK in finance after Brexit

Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at UK Finance, London.

1. Introduction

Ladies and gentlemen

Thank you for your kind introduction and thank you for the invitation to talk about financial services after Brexit.

Although I am in London to talk about finance issues, I have to confess that the United Kingdom, and especially London, has always been much more to me than just business. This is the birthplace of the industrial revolution and the modern market economy - and the centre of the first wave of globalisation in the 19th century.

And this great country and this wonderful city are where the future is made: a place of rare art and cultural diversity and of economic dynamism and innovation. So I am more than happy to be here with you today.

When I read the news of the Brexit vote, I was shocked. As I looked at the news, I simply couldn't believe it. I imagine I was not the only one among us.

It's needless to say that I respect the decision. Yet I am convinced that the UK and the EU going separate ways will be a tremendous loss for both sides.
And that's why the state of shock had to be just a very brief moment. We all have to do our best during the coming months to find pragmatic ways to establish a new, respectful, and friendly partnership.

Today, I will talk about the formal aspects of this future partnership in the realm of finance. However, formalities alone will not make for a partnership founded on mutual trust and amity.

What is equally important is the direct involvement of citizens and businesses - because, in the end, this is what underscores friendship and economic partnership. That is why this visit here today is so important to me.

I will start by outlining where we are in the talks about a future agreement and will then discuss the odds of something more than no deal happening. Given that a "no deal" on financial services is - like it or not - a realistic outcome, I will then discuss what pragmatic approaches to this new reality are feasible from my point of view.

2. Where we are: The debate on financial services

Since the leave vote in June 2016, we have seen a steady decline in expectations of how close economic integration between the UK and the EU27 will be after Brexit.

Against this background, it was positive that in December of last year the EU27 and the UK reached broad agreement on the three fundamental divorce issues.

After this preliminary settlement, we can now talk about the future model of cooperation and integration. This has improved the chances of reaching a reasonable settlement before the March 2019 deadline.

The plan is to have a political declaration on what the future partnership will look like by October this year; at the same time negotiation parties should have a draft withdrawal treaty ready.

But we should make no mistake: in light of the fact that the goals of the UK government are yet unclear to me and in light of the not fully unified positions within Whitehall, such an agreement is anything but a sure thing.

First of all, we have to keep in mind that substantial progress has yet to be made on the details of the three separation issues I have just mentioned.
Second, a sufficient transition period is not assured at the moment, either. And finally, even the no deal scenario remains possible in light of the fundamental differences between the negotiation blocs.

So what are the implications? What they have been since the beginning: the private sector and authorities have to prepare for a no deal scenario starting March 2019. I will come back to what this means for the financial sector.

But, let's remain at once realistic and optimistic. There is still at least a 50 percent chance of avoiding a "no deal" scenario. So let's think about what this would mean for financial services. Would they be part of an overall deal? And if yes, what would that deal look like?

Like with the overall negotiation, for financial services we have also seen a steady decline in expectations of how deep the integration will be after Brexit. It quickly fell from remaining part of the single market and passporting to the approach of equivalence in supervisory regimes, on the basis of which access could have been granted. The next step down the stairway of expectations was mutual recognition, at least in selected areas - or alignment and mutual recognition, as UK Finance has proposed.3

Yet I am sceptical as to whether such a mutual recognition framework is actually possible. Moreover, a future agreement may very well be quite limited - for example, to the exchange of goods.

Labour migration is likely to be excluded; at least, this has been mentioned as a red line for the UK government. And free trade in services also seems less and less likely. To quote the negotiator for the EU, Michel Barnier: "There is no place [for financial services]. There is not a single trade agreement that is open to financial services. It doesn't exist."

3. Facing difficult realities: The "no deal" scenario

Thus, it is not that unlikely that there will be no free trade agreement for financial services - or other services sectors, for that matter.

What would that mean for financial transactions between the UK and the EU? It would mean that the EU and the UK would trade under rules set by the World Trade Organization - where services sectors are only thinly covered.
Service providers would then have to apply for comprehensive licenses in both jurisdictions and have all the necessary elements of a fully functioning bank ready in both places.

I am very much aware that this sounds like a worst case scenario. And I very much do understand that. We are coming from a highly comfortable position: the single market and the passporting rights allow free trade in services without much legal and regulatory friction.

After more than two decades of this freedom we have gotten used to it; it has become our point of reference in debates and for policy proposals.

But it is time to face the facts. The point of reference has changed since the Brexit vote. Where it was the single market and passporting, it is now trade agreements with third countries that do not accept the EU’s legal jurisdiction - we all know Mr Barnier's stairway to Brexit.

In these arrangements, the free exchange of workers and services tends to be very limited.

It is imperative to accept this new political point of reference, because the old one has somewhat lost democratic legitimacy.

Yes, this is inconvenient and it creates frictions. However, if we take a broader historical perspective, we can see that - in the past - full integration has not been a necessary condition for vibrant international economic exchange.

Innovation, growth, and close economic ties are possible even in a world where firms have to adhere to different sets of rules in different countries. This competition of rulesets may even foster institutional innovation and diversity and may contribute to stability.

Rather than clinging to an almost somewhat anachronistic point of reference, we must explore new approaches. And that is why we need constructive proposals from all sides, including the industry.

UK Finance has tabled a proposal as well, and I welcome the effort. Yet I am sceptical as to whether the mutual recognition framework proposed is actually 100 percent feasible.

By giving substantial powers to technical cooperative committees of supervisors, it would most likely undermine national sovereignty and
It is not obvious to me that this would be efficient.

The substantial effort necessary to make this technical, cooperative arrangement work may outweigh the benefits to society. In the end, the effort put into keeping such an arrangement alive might be better invested in making sure that we make the licensing procedures as smooth as possible.

At the end of the day, the decision about the future for financial services will be a political one. But, in any case, it is important that we all work together to find pragmatic solutions under any kind of framework. And a lot of difficult tasks lie ahead of us - for financial firms as well as for central banks and supervisors.

4. Transition phase to the rescue?

In light of these tremendous tasks, many firms and officials seem to be counting on a transition phase that could provide some breathing space for businesses and give them more time for their preparations.

Talks about such a phase have just started: last week the EU’s chief negotiator Michel Barnier has received directives reflecting the stance of the EU27 on a potential transition phase until the end of 2020.

Roughly eight weeks are scheduled for the talks about transition in total, so that an agreement on transition could be reached by March and talks about future relations can take centre stage thereafter.

Many businesses are holding out high hopes that a transition phase will give them certainty on the shape of relations between the UK and the EU, at least until year-end 2020.

Some observers seem quite confident that there will be a transition phase. But a number of potential stumbling blocks remain. For one thing, while there would certainly be economic merits to such an arrangement, it’s politically tricky to design.
Furthermore, a vague, in-principle political agreement on transition wouldn't tell you too much and would be very fragile. But even if both sides managed to reach a consensus on a detailed legal text by March, this would still only be a preliminary part of the greater deal.

Both sides would still have to reach an overall divorce deal, roughly by October of this year. If this endeavour fails or if parliaments don't subsequently ratify the deal, the transition period would be off the table, too.

Put bluntly: a deal on the transition phase hinges on an agreement on the overall future relationship - if the UK and the EU can reach a deal on the end state of the future partnership, I am confident it will be easier to find a suitable solution for the transition phase.

The point is: Even if one is cautiously optimistic that a transition phase can be agreed upon - which I continue to be - it still wouldn't give businesses the certainty they crave. Just this Monday, Mario Draghi has underlined in the European Parliament that political uncertainty will remain for quite some time to come. The transition phase is not a safety net.

5. Acknowledging realities: timely preparation is key

This is why I see no alternative to timely preparation. This holds for all businesses affected, and it holds for the financial sector in particular. Financial institutions should not fall prey to a false sense of certainty that, come what may, there will be an agreement and that they will have sufficient time left to adapt to the new framework.

The economic consequences of insufficient preparation in the event of a hard Brexit would far exceed the costs of proper preparation.

Looking at banks, proper preparation includes establishing at least basic entities in the other economic area - that is, the EU 27 or the UK - in order to continue doing business there. The concept of a "basic entity" is not easy to define. From our side, I can repeat that we will certainly not accept empty shells or "letterbox companies" where the business effectively continues to be run from London.

For critical functions such as management, controlling and compliance, qualified personnel need to be present at the EU entity at all times. We expect any branch or subsidiary to retain chief responsibility for its business.
That is our general approach. When it comes to the details, things get much more complicated very quickly - as has been demonstrated by our experience with the applications of banks for licenses in the context of Brexit. It is not enough to make a decision about what business to move and to submit a ten-page application for a banking license to the supervisor.

In reality, it is quite common that applications are changed and amended during the process as a result of ongoing discussions between the supervisor and the applying bank or due to the applying bank having a change of heart due to the emergence of new information.

This should by no means come as a surprise. In many ways, both banks and supervisors are in new territory here. And not only businesses have got their hands full managing the fallout from Brexit, supervisors do, too.

In normal times, the European Single Supervisory Mechanism issues about 10 licenses for credit institutions under the Capital Requirements Regulation (CRR) per year, plus a couple of licenses issued nationally for entities such as securities trading banks. But in the context of Brexit, we are looking at more than 100 financial institutions - many of which are highly significant and complex institutions - currently operating out of the UK that potentially need a new or modified license in the EU.

Therefore, we have increased our resources both in the European banking supervision and in the national supervisory authorities. However, our capacities are obviously finite. Should there be a flood of applications at the very last minute, we cannot guarantee that we will be able to prevent capacity constraints that could prolong the application process.

Therefore, I strongly advise banks not to slow down in their preparatory efforts because of a vague possibility of a transitional period. The first quarter of this year has been named by many in the financial industry as a point of no return for pushing the button on their Brexit contingency plans. In my view, this is still a fair estimate.

Those who do not complete their plans and start implementing them by March this year risk being left high and dry by Brexit one year later.

To be clear, this also applies to German and other European institutions that operate in the UK. We have learned that there are institutions that have not yet approached the PRA even though they want to maintain their UK business after Brexit.
6. What can bank supervisors do?

Some have voiced the concern that warnings from European officials towards businesses, including financial institutions, currently operating out of the UK to prepare for a hard Brexit could be an attempt to lure business and jobs to the EU27. I want to make crystal clear that this is not our intention.

From the day after the referendum I have repeatedly emphasized that we are not the marketing agency for the city of Frankfurt - or any other European financial centre, for that matter. We are supervisors interested in the stability and smooth functioning of the financial sector.

And as long as there is no deal on future relations, no divorce deal and not even a reliable and consistent declaration of intent, we have no other choice than to warn financial institutions of the risk of being caught unprepared. This would not be in the interest of either the EU or the UK.

Whatever political decision is taken, bank supervisors will not only do all they can to make the transition to a new regime as smooth as possible; they will also, in the long run, try to reduce unnecessary inefficiencies where possible.

In December last year, the PRA published a draft proposal for a post-Brexit supervisory approach. I very much appreciate the spirit behind this approach. It reflects a solution-oriented, pragmatic, yet stability-oriented approach.

In the same vain, the SSM has developed quite pragmatic, cooperative "policy stances" on many of the relevant issues. I am confident that this cooperative style can be an important contribution towards a smooth transition.

7. Conclusion

Ladies and gentlemen, the point of reference for future regulatory alignment has changed since the Brexit vote. It used to be the single market and passporting; now it is trade agreements with third countries that do not accept the EU’s legal jurisdiction.

The free exchange of workers and services will tend to be very limited under these scenarios.
It is imperative to accept this new political point of reference, because the old one has somewhat lost its democratic legitimacy.

The tasks that come with this new reality are unchartered territory for all of us. But, irrespective of the framework, it is important that we work together to find pragmatic solutions that sustain the strong links between our economies and financial sectors.

I am confident that, even without a financial services agreement, our economies and financial sectors will remain closely integrated. Furthermore, I am confident - and glad, even - that Germany and the UK will maintain their long tradition of partnership based on close cooperation and mutual trust.

Thank you for your attention.
Ladies and Gentlemen,

I would like to congratulate the National Bank of Belgium, Jean Hilgers and his colleagues, for organising this event and thank you for the invitation to deliver the introductory speech, which I do with great pleasure.

Ten years after the emergence of the financial crisis, we are now in a different phase of the regulatory cycle naturally influenced by the new political priorities of increasing investment and economic growth.

While in my view it makes perfect sense to evaluate and review the recent reforms in order to mitigate any unintended consequences and increase proportionality, I strongly believe that we should not abandon the core values of stability and consumer protection that presided to these reforms.

We cannot forget that the post-crisis regulatory agenda was the right response to restore the loss of confidence in the financial sector.

Furthermore, to build up sustainable long-term investment and economic growth we need a stable and strong insurance sector that adequately prices risks, applies robust risk management strategies and treats customers fairly.

Regulatory certainty is an important value that we all should preserve. In line with this principle, the review of Solvency II follows a structured process envisaged in the legislative texts:
- by 2018, the review of the Solvency Capital Requirement (SCR) and,

- by 2021, the overall review of the regime, including the treatment of long-term guarantees (LTG).

**Review of the SCR**

EIOPA received calls for advice from the EU Commission focused on three main themes:

- Reducing complexity,
- Enhancing proportionality and,
- Removal of unjustified constraints to financing.

EIOPA is committed to evidence-based policymaking and to the overall principles of Solvency II. That means that our proposals will be based on the data available on the different risks and our judgements will be always focused on the main objectives of Solvency II, namely the protection of policyholders and beneficiaries and the stability of the market.

Changes must be carefully justified and clearly necessary. If there are unintended consequences, we must tackle them.

In terms of evaluation, we always put to ourselves a number of basic questions:

- What is the evidence available?

- Is this a material issue?

- Would the change be prudent and in line with the Solvency II objectives?

- Are there trade-offs, for example between greater granularity and simplicity?

- What is the overall impact of the changes?

We developed very detailed technical and analytical work and followed an open and transparent consultation process, which allowed all stakeholders to contribute to the review.
At the end of October last year, we submitted to the EU Commission the first set of advice covering a number of important issues.

EIOPA’s proposed changes foresee simplifications to the calculation of risks such as lapse and mortality. To reduce over-reliance of insurance undertakings on external credit ratings in the calculation of the SCR, EIOPA recommended applying simplified calculations by nominating only one credit rating agency and calculating capital requirements for the remaining non-complex assets only subject to credit quality step 3 (i.e. BBB rating).

EIOPA also advised to create a new asset class for non-listed guarantees issued by regional governments and local authorities to ensure improved risk-sensitivity of the calculations.

Furthermore, the advice identified the need for the extension of the application of the look-through approach to related undertakings that invest on behalf of the insurer.

It also included the proposal for the use of undertaking specific parameters for reinsurance stop-loss treaties to allow for better reflection of the risk profile.

With respect to risk mitigation techniques, EIOPA recommended to better recognise strategies to hedge financial risks where the exposure is changing frequently.

Finally, EIOPA carried out an analysis of the loss-absorbing capacity of deferred taxes (LAC DT) across the European Economic Area including supervisory and industry practices.

The results of the analysis showed that for 75% of the close to 100 billion euros of LAC DT there are consistent practices but for the remaining 25% of LAC DT, namely the part related to the calculation of expected future profits, there are material differences in approach.

Our second Advice, to be submitted to the European Commission at the end of this month, will include proposals to deal with this issue.

This second advice will also cover, in between others:

- The recalibration of a number of risks (standard parameters of premium and reserve risks, mortality and longevity risks and
natural catastrophe risks)

- The review of the methodology on interest rate risk, in light of the emergence of negative interest rates

- The review of the cost of capital methodology included in the calculation of the risk margin

- A more granular treatment of the risks related to unrated debt and unlisted equity

**Long-term guarantees**

Another important area in the overall review of Solvency II is the LTG. What is our role here? We are required to provide an annual report on the LTG measures until 1 January 2021.

We already published two of our annual reports in December 2016 and December 2017. These reports are fact based and provide a good basis to understand the impact and the sensitivity of these measures.

It is already clear that the LTG measures, taken collectively, are being widely used. More than 25% (783 out of 2945) of the undertakings in the European Economic Area use one of voluntary measures, accounting for 74% of technical provisions of European insurers. On a Europe-wide basis, the volatility adjustment is the most frequently used measure.

The impact of the LTG measures is significant. For the ones using them, they result in an increase in the SCR ratio of an average of 69 percentage points.

In line with the SII Directive requirements, EIOPA will continue to publish annual reports on the LTG and intend to finalize its work by 2020 with an advice to the EU Commission.

**Analysing the impacts of Solvency II**

Building up evidence and knowledge towards the 2021 overall review, EIOPA is attentive to the different impacts on the market.

The recent investment survey points to a search-for-yield behaviour of insurers, which is a natural reaction to the low interest rate environment.
The increased exposure to more illiquid investments and to non-traditional asset classes, such as infrastructure, improves asset diversification but also demands new risk management capabilities from insurers and closer supervisory scrutiny. At the same time, in line with our expectations, the first observations from the impact of Solvency II point to an increase in long-term investment and a stable allocation to equity.

Another consequence of the low interest rate environment is the acceleration of the pace of change in business models, especially in life insurance, with the move towards contracts with lower and more flexible guarantees and, in some countries, the significant increase of pure unit-linked products.

While this is a natural management reaction to ensure the long-term sustainability of the insurers commitments and optimize capital in a Solvency II environment, it also increases the transfer of risks to policyholders. I believe that this last evolution deserves further reflection from a regulatory perspective.

We will thoroughly analyse the new evidence available on the risks and characteristics of the long-term life insurance products, especially concerning the illiquidity characteristics of the liabilities and the corresponding ability of insurers to mitigate short-term volatility by holding assets throughout the duration of the commitments, even in times of market stress.

There is specific work to do in this area, in order to explore the development of a specific regulatory treatment to the spread and equity risk charges associated to long-term assets backing certain types of truly long-term illiquid liabilities, while maintaining the sound market consistent orientation and the principles of policyholder protection of Solvency II.

The intention should be to study possible adjustments to the regime to better recognize the true risks of long-term transparent retirement savings products, for the benefit of consumers and the whole economy.

Towards a comprehensive insurance regulatory framework

While Solvency II is undoubtedly a great achievement for the European Union insurance sector and for the protection of policyholders, there are still some areas where progress is needed to complete a comprehensive
European Union insurance regulatory framework. I am talking about a macro-prudential framework, including the specific issue of systemic risk, recovery and resolution mechanisms and insurance guarantee schemes.

**The macro-prudential framework**

The insurance sector plays a relevant role in achieving a stable financial system, supporting long-term sustainable economic growth. Thus, mitigating the likelihood and the impact of a systemic crisis in insurance should be an important policy objective.

Work needs to be done towards the establishment of a comprehensive European Union macro-prudential framework for insurance that takes into account the specific nature of the insurance business and funding models and defines insurance specific objectives and instruments. In our view, this framework needs to be consistent with Solvency II.

EIOPA will be publishing in the coming days two papers in this area, covering a possible holistic framework to analyse systemic risk in the insurance sector and the Solvency II tools with a macro-prudential impact. We want to foster a proper discussion with all stakeholders on these important issues and we look forward for your input.

**Recovery and resolution mechanisms and insurance guarantee schemes**


The existing fragmented landscape of national recovery and resolution frameworks could cause significant barriers to the resolution of (re)insurers, particularly of cross-border groups. To reduce this risk, to avoid unnecessary economic cost stemming from uncoordinated decision making processes between national authorities and to ensure orderly resolution, European action is required.

Therefore, EIOPA calls for a minimum degree of harmonisation in the field of recovery and resolution for (re)insurers with the objective to increase policyholder protection and financial stability in the European Union. To achieve this objective EIOPA proposes the following four building blocks
where the definition of a common approach is key:

- Preparation and planning
- Early intervention
- Resolution
- Cross-border cooperation and coordination

The harmonised recovery and resolution framework should cover all (re)insurers subject to the Solvency II framework and be applied in a proportionate manner.

EIOPA is continuing its work in this area focussing on resolution funding and insurance guarantee schemes.

We believe that the overall review of Solvency II in 2021 should consider all these issues to ensure the coherence between the micro and the macro elements, avoid the emergence of conflicting incentives to insurers, and facilitate the implementation of the regimes by the respective authorities.

To finalise I would like to emphasize that the work on the review of Solvency II will benefit from the ongoing EIOPA initiatives on ensuring a consistent implementation of the new regime.

**Supervisory convergence** is the main strategic priority of EIOPA and its objectives are to develop a common supervisory culture, guaranteeing a level playing field and preventing regulatory arbitrage in the internal market with the ultimate goal of safeguarding a similar level of protection to all policyholders and beneficiaries in the European Union.

Thank you for your attention.
Meltdown and Spectre – Updated Advice

Malware making use of Meltdown and Spectre, the two CPU vulnerabilities highlighted back in January, is now being seen in the wild.

Security researchers are reporting they have seen over 140 malware samples based on the proof of concept code.

Whilst there have not been instances of Meltdown and Spectre actually being leveraged to compromise a system, it is a timely reminder that miscreants will take published security vulnerabilities and weaponise them into malware quickly, making it all the more important to patch.

As previously reported by the NCSC, Meltdown and Spectre are two related, side-channel attacks against modern microprocessors that can result in the unprivileged code reading data it should not be able to access.

Most devices may be vulnerable to some extent with many vendors releasing patches to secure systems.

The NCSC have previously advised users and business enterprise users to follow vendor advice and apply patches.

For more detailed advice regarding these vulnerabilities, please see the latest guidance from the NCSC at: https://www.ncsc.gov.uk/guidance/meltdown-and-spectre-guidance
Playing 20 Questions with Bacteria to Distinguish Harmless Organisms from Pathogens

New biosurveillance technology would quickly identify potentially harmful traits in unfamiliar bacterial strains

Bacteria underpins much of our world, acting behind the scenes to affect the health and behavior of animals and plants. They help produce food, provide oxygen, and even reshape the environment through a vast array of biological processes.

They come in a phenomenal number of strains—many still unknown—and thrive in different ecological and environmental niches all over the world. But while their diverse behaviors makes them essential to life, bacteria can also be deadly.

This threat only grows as greater global travel brings people into contact with new places, foods, and animals, dramatically increasing the chances of exposure to dangerous microbial species known as pathogens.

How can the Department of Defense—whose forces, deployed around the world, constantly come into contact with new bacteria—discriminate between harmless and virulent strains to prevent a disease outbreak that threatens military readiness?

Friend or Foe, a new program from DARPA’s Biological Technologies Office, proposes to develop a platform technology that rapidly screens unfamiliar bacteria to establish their pathogenicity and even discover unknown pathogenic traits, necessary first steps for designing effective biosurveillance and countermeasures.

“Trends such as rising global population, changes in the environment, and the growing accessibility of tools for genetic engineering mean that our armed forces are increasingly likely to face new bacterial pathogens, whether they occur naturally or are engineered by adversaries,” said Paul Sheehan, the program manager for Friend or Foe.
“Our existing biosurveillance strategies don’t work on previously undiscovered bacteria or on bacteria that have been specifically designed to evade detection by current tests. We need new screening tools that can quickly characterize the threat to enable a rapid response.”

Existing forensic technologies for identifying bacteria are limited in their application and fall primarily into two categories: rapid diagnostic microbiology, which is confined to approximately 350 known strains and requires cultured bacteria; and metagenomics, which only inventories previously known bacteria present in a sample.

Both technologies take 36 hours or longer to deliver results, and neither is capable of quickly evaluating previously unknown bacteria, especially strains that cannot be cultured in a laboratory.

This means that, at present, the vast majority of bacteria species cannot be readily evaluated for risk to humans.

Yet within this diversity of bacteria—at least 10^7 to 10^9 species—there lies a large pool of unknown traits that could contribute to future pathogenicity. And, since bacteria can transfer traits between species fairly rapidly, individual strains can acquire new capabilities to help them evade the body’s innate immune response or to resist antibiotics.

Although new genetic sequencing tools are being developed that can quickly read a bacterium’s genotype—its genetic makeup—sequencing alone will unlikely solve the challenge of assessing risk.

That’s because simply knowing genotype is not the same as knowing phenotype—how that bacterium’s genetic code leads to function. The sheer sequence of a bacterial genome does not indicate whether or not the bacterium is pathogenic in humans.

To directly and efficiently test for pathogenicity, Friend or Foe aims to build a portable platform that screens many unfamiliar strains of bacteria at once to reveal their phenotypes. Developing such a platform will require overcoming numerous engineering challenges.

First, without killing the bacteria, the technology must extract and isolate them from complex environments such as soil, runoff, sewage, biofilms, and medical samples, where numerous strains of bacteria live together.
Second, the system must sustain the bacteria in simulated host environments long enough to conduct testing.

And third, it must run and evaluate a gauntlet of physical and chemical tests on the bacteria—the biological equivalent of the game “Twenty Questions”—to determine their pathogenicity.

The Friend or Foe system will test for three traits of pathogenicity.

First, can the bacteria survive and establish a niche in a host organism? Does it, for instance, adhere to the host’s cell membranes?

Second, can the bacteria harm its host? For example, does it secrete toxins or have flagella that could disrupt the host’s mucosal tissue? And third, can the bacterium protect itself? Does it inactivate the host’s protective antibodies or resist antibiotics?

Dangerous bacteria would be flagged for genetic sequencing to map the newly discovered pathogenic trait to specific genes, leading to simpler biochemical tests for that pathogen in the future.

A side benefit of the program would be speeding up all future efforts to identify new bacterial traits and the genes that provide them, which would support research ranging from antibiotic production to the degradation of pollutants.

“There are millions of species of unidentified bacteria in the world, and we now have no quick way of knowing which of those might endanger our troops,” Sheehan said. “If we’re successful in creating a tool for rapid evaluation of bacterial phenotype, we’ll deliver the Defense Department a powerful new capability for force protection and a powerful deterrent to the development of engineered bio-threats.”

DARPA envisions Friend or Foe as a four-year, fundamental research program. Once the program begins, a separate independent verification and validation (IV&V) team contracted by DARPA will work with performer teams to provide standardized biological samples that simulate different environments and include mixtures of known bacteria. The IV&V team will also evaluate the effectiveness of the performers’ systems following demonstrations.

Researchers supporting Friend or Foe must adhere to all applicable guidelines for biosecurity. DARPA has structured the program so that
potential discovery of new pathogens can only take place under the guidance and supervision of federal agencies tasked with preventing the spread of disease.
Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:
- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;
- should not be relied on in the context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of an interpretative document;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.
The International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. **Membership** – Become a standard, premium or lifetime member.

   You may visit:  
   [www.risk-compliance-association.com/How_to_become_member.htm](http://www.risk-compliance-association.com/How_to_become_member.htm)

   Become a lifetime member of the association, and to continue your journey without interruption and without renewal worries. You will get a lifetime of benefits as well.

   You can check the benefits at:  
   [www.risk-compliance-association.com/Lifetime_Membership.htm](http://www.risk-compliance-association.com/Lifetime_Membership.htm)

2. **Weekly Updates** - Subscribe to receive every Monday, the Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next:  
   [http://forms.aweber.com/form/02/1254213302.htm](http://forms.aweber.com/form/02/1254213302.htm)

3. **Training and Certification** - The Certified Risk and Compliance Management Professional (CRCMP) training and certification program has become one of the most recognized programs in risk management and compliance.

   There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

   You can find more about the demand for CRCMPs at:  

   For the distance learning programs, you may visit:  
   [www.risk-compliance-association.com/Distance_Learning_and_Certification.htm](http://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm)
For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements. We tailor presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.

4. IARCP Authorized Certified Trainer (IARCP-ACT) Program - Become a Certified Risk and Compliance Management Professional Trainer (CRCMPT) or Certified Information Systems Risk and Compliance Professional Trainer (CISRCPT).

This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit: www.risk-compliance-association.com/IARCP_ACT.html

5. Approved Training and Certification Centers (IARCP-ATCCs) - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor-led CRCMP and CISRCP training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more: www.risk-compliance-association.com/Approved_Centers.html