Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341
Dammstrasse 16, 8810 Horgen, Switzerland
Tel: +41 79 505 89 60 Web: https://www.cyber-risk-gmbh.com

June 2021, top cyber risk and compliance related local news stories and world events

Dear readers,

The Swiss Federal Intelligence Service (Nachrichtendienst des Bundes, NDB) has published its latest situation report, intended to provide with information on threats and dangers to Switzerland's security.

The NDB hopes that this intelligence-based analysis of today's world will help clarify what the threats to Switzerland are – not so much today's flashpoints, but more importantly tomorrow's trouble spots.

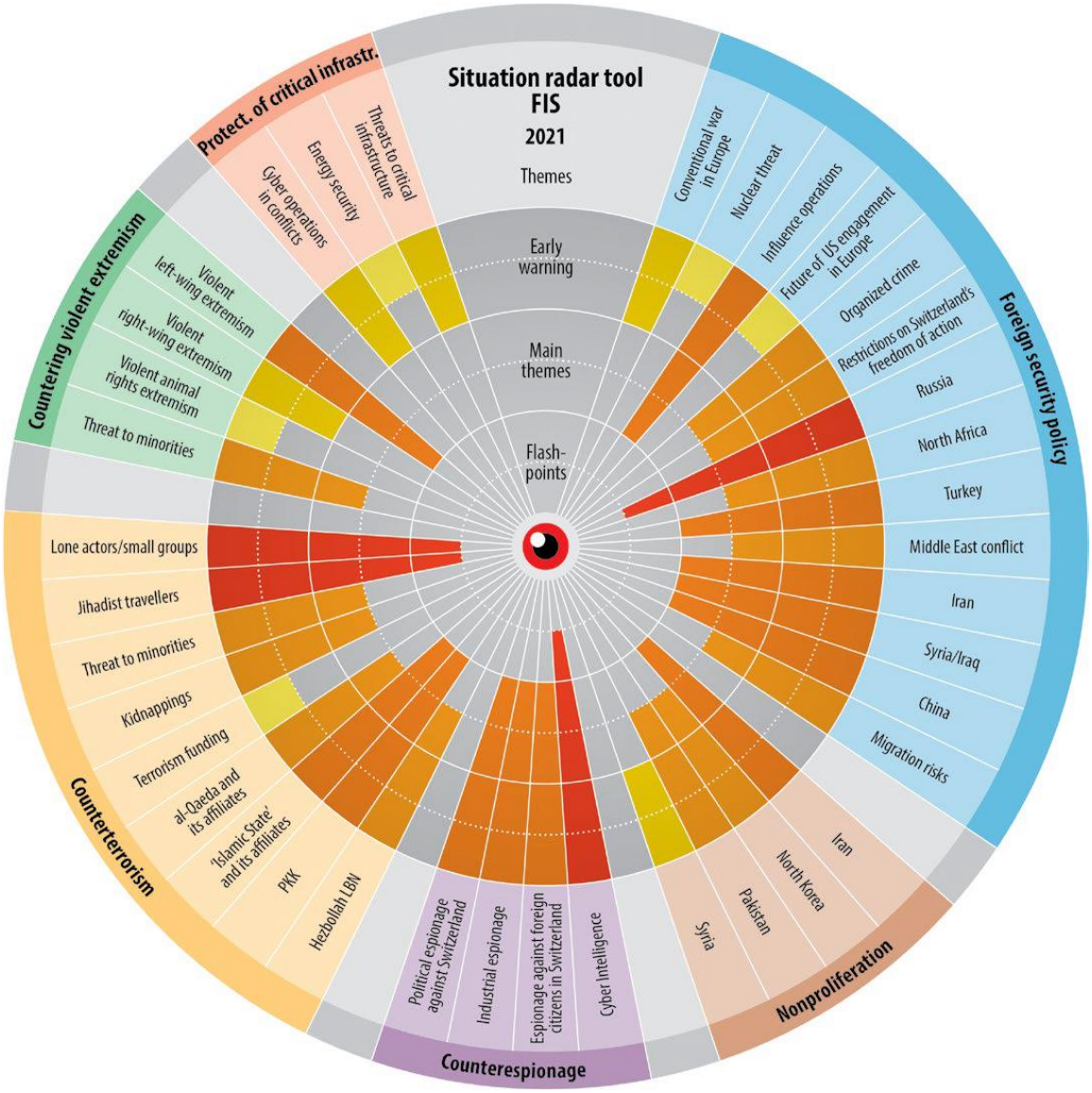
According to the report, espionage remains an ever-present challenge. Digitalisation and interconnectedness have made a sharp increase in espionage in cyberspace possible. The targets of foreign espionage have not changed, and Geneva is still a prime target because of the international organisations and the large number of diplomatic missions based there.

Foreign intelligence services pose a direct threat to certain target groups in Switzerland and may also be involved in influence operations against Swiss

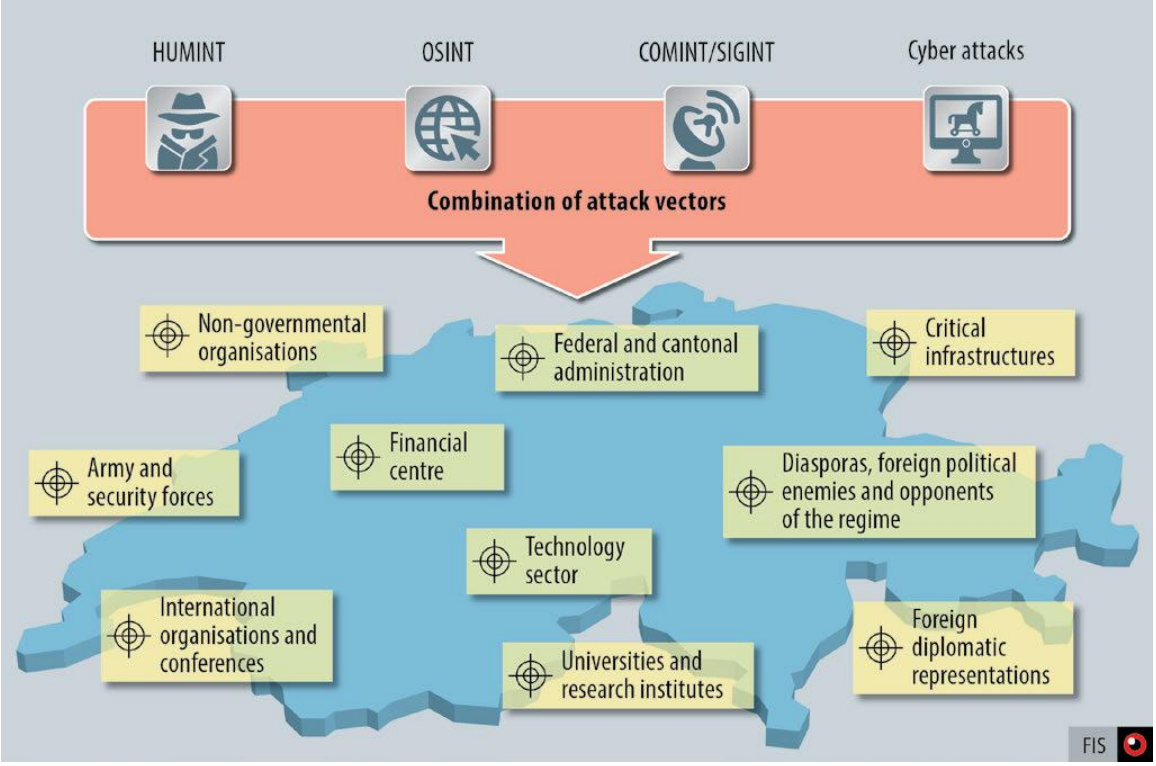
interests.

Foreign actors continue to attempt to procure materials and cutting-edge technology in Switzerland for weapons of mass destruction programmes or for the manufacture of delivery systems. Furthermore, with its many innovative companies, Switzerland is vulnerable to strategic proliferation efforts.

The FIS uses a *situation radar tool* to depict the threats affecting Switzerland. A simplified version of the situation radar, without confidential data, has also been incorporated into this report. This public version lists the threats that fall within the responsibilities of FIS, with the addition of the topics 'Migration risks' and 'Organized crime', which are relevant for security policy.



Espionage attack vectors and targets in Switzerland



You must read the report at:
https://www.newsd.admin.ch/newsd/message/attachments/67047.pdf

---

Virginia Woolf has said that *for most of history, anonymous was a woman*. Today anonymous are also shell corporations, without beneficial ownership information.

I liked this presentation. Kenneth A. Blanco, Director, Financial Crimes Enforcement Network, testified before the US Senate Committee on Banking, Housing and Urban Affairs, and he did an excellent job.

He has discussed the elimination of anonymous shell corporations by collecting beneficial ownership information, in order to preserve national security and protect people from harm.

He spoke about:

- an arms dealer who sold weapons to a terrorist organization,
- executives from a supposed investment group that perpetrated a Ponzi scheme that defrauded more than 8,000 investors, most of them elderly, of over $1 billion,

- a complex nationwide criminal network that distributed oxycodone by flying young girls and other couriers carrying pills all over the United States,
- a New York company that was used to conceal assets, including those designated for providing financial services to entities involved in a nuclear and ballistic missile program,
- a former college athlete who became the head of a gambling enterprise and a violent drug kingpin who sold recreational drugs and steroids to college and professional football players,
- a corrupt treasurer who received over $1 billion in bribes.

He said that these crimes are very different, as are the dangers they pose and the damage caused to innocent and unsuspecting people. The defendants and bad actors come from every walk of life and every corner of the globe. The victims—both direct and indirect—include Americans exposed to terrorist acts; elderly people losing life savings; a young mother becoming addicted to opioids; a college athlete coerced to pay extraordinary debts by violent threats; and an entire country driven to devastation by corruption. But all these crimes have *one thing in common:* shell corporations were used to hide, support, prolong, or foster the crimes and bad acts committed against them.

These criminal conspiracies thrived at least in part because the perpetrators could hide their identities and illicit assets behind shell companies. Had beneficial ownership information been available, and more quickly accessible to law enforcement and others, it would have been harder and more costly for the criminals to hide what they were doing.

Law enforcement could have been more effective and efficient in preventing these crimes from occurring in the first place, or could have intercepted them sooner and prevented the scope of harm these criminals caused from spreading.

Learn more at number 7 below.

This summer we will read an interesting paper about the Federal Reserve Board's current thinking on *digital payments,* with a particular focus on the benefits and risks associated with *central bank digital currencies (CBDCs).* Today we can have a feeling about the content of this paper.

Lael Brainard, Member of the Board of Governors of the Federal Reserve System, gave an interesting presentation at the Consensus by CoinDesk 2021 Conference in Washington DC, with title *"Private money and central bank money as payments go digital - an update on CBDCs"*

She said: “There is a risk that the widespread use of private monies for consumer payments could fragment parts of the U.S. payment system in ways that impose burdens and raise costs for households and businesses.”

She also said: “A predominance of private monies may introduce consumer protection and financial stability risks because of their potential volatility and the risk of run-like behavior.

Indeed, the period in the nineteenth century when there was active competition among issuers of private paper banknotes in the United States is now notorious for inefficiency, fraud, and instability in the payments system. It led to the need for a uniform form of money backed by the national government.”

Lael Brainard explained that a stablecoin is a type of digital asset whose value is tied in some way to traditional stores of value, such as government-issued, or fiat, currencies or gold. Stablecoins vary widely in the assets they are linked to, the ability of users to redeem the stablecoin claims for the reference assets, whether they allow unhosted wallets, and the extent to which a central issuer is liable for making good on redemption rights.

Unlike central bank fiat currencies, stablecoins do not have legal tender status. Depending on underlying arrangements, some may expose consumers and businesses to risk.

If widely adopted, stablecoins could serve as the basis of an alternative payments system oriented around new private forms of money.

Read more at number 10 below.

Horace believed that *the pen is the tongue of the mind*. Of course, he had never seen a keyboard.

Selecting the suitable paper for a fountain pen is like pairing a fine wine with a great cheese. Matching flavour intensity and character is an art and a science.

Unfortunately for many of us the keyboard has replaced the fountain pen for ever. There are young persons that never write anything with a pen, if you can believe it.

This is a major challenge for the forensic handwriting examiners that authenticate handwritten notes and signatures (or reveal them to be fakes), by analyzing distinctive features in our writing. As people write less by hand, will handwriting examination become irrelevant?

A recently updated report from the National Institute of Standards and Technology (NIST) suggests that the answer is no — if the field changes to keep up with the times. But the times are changing in more ways than one, and the decline in handwriting is only one of the challenges that the field will have to reckon with.

We also have another interesting problem: The field of forensic handwriting examination may have trouble attracting new blood. A report from NIST earlier this year found that the median age for handwriting examiners is 60, compared with 42 to 44 for people in similar scientific and technical occupations.

To increase recruitment, the report recommends replacing the unpaid apprenticeships that have been the traditional route of entry into the field with grants and fellowships. The report also recommends cross-training with other forensic disciplines that involve pattern matching, such as fingerprint examination.

A forensic handwriting examination involves a series of decisions that depend on careful observation and interpretation of the handwriting evidence. Given the human element of this interpretation process, it also requires awareness and mitigation of the potential for contextual bias.

According to Voltaire, *to hold a pen is to be at war*. I have just realized that I have never read a good quote about keyboards.

Read more at number 12 below. Welcome to our monthly newsletter.

Best regards,

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Number 1 (Page 11)

UK, Crown Prosecution Service (CPS)

COVID-19 fraudster jailed for mass cyber scam

Number 2 (Page 15)

The money laundering business – making dirty money look clean

How criminals use banks to launder money and how good banks are at protecting themselves from such criminal activities.

BaFin Federal Financial Supervisory Authority

Number 3 (Page 20)

US Government Accountability Office

Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market

Number 4 (Page 23)

Breaking the Specification: PDF Certification

RUHR-UNIVERSITÄT BOCHUM

Simon Rohlmann
Ruhr University Bochum
simon.rohlmann@rub.de

Vladislav Mladenov
Ruhr University Bochum
vladislav.mladenov@rub.de

Christian Mainka
Ruhr University Bochum
christian.mainka@rub.de

Jörg Schwenk
Ruhr University Bochum
joerg.schwenk@rub.de

Number 5 (Page 25)

Cyber resilience practices - Executive Summary

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

Number 6 (Page 27)

Whom do consumers trust with their data? US survey evidence

Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster, Kelly Shue

BIS

Number 7 (Page 30)

Testimony before the Senate Committee on Banking, Housing and Urban Affairs

Kenneth A. Blanco, Director, Financial Crimes Enforcement Network

FINANCIAL CRIMES ENFORCEMENT NETWORK

Number 8 (Page 37)

Another Nobelium Cyberattack

Tom Burt, Corporate Vice President, Customer Security & Trust

Microsoft

Number 9 (Page 40)

Undated Privacy Policy for users having their usual residence in the US

TikTok

Number 10 (Page 46)

Private money and central bank money as payments go digital - an update on CBDCs

Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Consensus by CoinDesk 2021 Conference, Washington DC

Number 11 (Page 56)

Can Digital Identity Solutions Benefit from Blockchain Technology?

The knowledge building seminar organised by the EU Agency for Cybersecurity explores the possible applications of blockchain technology in the field of digital identity and online trust.

Number 12 (Page 58)

Handwriting Examiners in the Digital Age

As the use of handwriting declines, a forensic discipline finds itself at a crossroads.

Number 13 (Page 61)

Slilpp Marketplace Disrupted in International Cyber Operation

Slilpp was a Marketplace for Allegedly Stolen Online Account Login Credentials, Offering Over 80 Million Stolen Credentials for Over 1,400 Victim Providers Worldwide

Number 14 (Page 64)

Using a mineral 'sponge' to catch uranium

Remediation technology reduces uranium levels ten-thousandfold at legacy site in Colorado

Number 15 (Page 67)

Enabling Human Control of Autonomous Partners

DARPA program to help humans maintain situational awareness when AI behaves in unexpected ways

Number 16 (Page 70)

Targets for Addressing the Four Challenges of Cross-Border Payments: Consultative document

Number 17 (Page 73)

PUBLIC CONSULTATION ON THE DRAFT CANDIDATE EUCC SCHEME

Number 18 (Page 75)

How AI Could Alert Firefighters of Imminent Danger

Number 19 (Page 79)

FBI Targets Encrypted Platforms Used by Criminal Groups

Global Partners Announce Results of Innovative Operation Trojan Shield

Number 1

UK, Crown Prosecution Service (CPS)

COVID-19 fraudster jailed for mass cyber scam

The Crown Prosecution Service (CPS) prosecutes criminal cases that have been investigated by the police and other investigative organisations in England and Wales. The CPS is independent, and we make our decisions independently of the police and government.

A COVID-19 fraudster has been jailed for using fake digital messages to trick people into providing bank details to receive a vaccine.

Teige Gallagher, 21, was sentenced at the Old Bailey to four years and three months' imprisonment.

Gallagher had been sending out bulk text messages to members of the public claiming to be from various commercial organisations such as banks and from the NHS. The victims were asked for personal financial information, including questions relating to their bank accounts and bank cards.

In the case of the NHS, Gallagher set up web pages based on the GOV.UK website, which claimed it needed this information to verify who victims were and their entitlement to receive the vaccine.

The police found iPhones at Gallagher's home containing messages purporting to be from the NHS, various banks, and Netflix. On one of the phones more than 2,000 telephone numbers were found, believed to be a list of victims who were sent scam SMS messages.

Gallagher used specialist tools to be able to send out bulk SMS text messages to a list of mobile phone numbers which came from a data breach. He would then tailor a fake SMS message from an organisation relevant to the victim.

Within the fake message there would be a link to a fraudulent website and once taken in by the scam the intent was to 'socially manipulate' the victim to disclose personal details. In this way he intended to obtain the victims' full names, credit and debit card numbers, bank account numbers and passwords.

Gallagher was engaging in smishing and phishing frauds. Smishing is when fraudsters obtain personal details of a victim by SMS text messages, while phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords.

John Werhun, from the CPS, said: "At a time when the country is looking to the COVID-19 vaccination rollout to help our society return to normal, Gallagher was seeking to exploit this by prising vital personal financial information from vulnerable victims eagerly wanting their vaccine.

"Criminals are increasingly using sophisticated on-line methods to try and extract information and money from unsuspecting members of the public. We need to be agile in our response to these phishing and smishing threats and our new Economic Crime Strategy will allow us to adapt and enhance our capability.

"Working closely with City of London Police, we have brought a rapid close to Gallagher's fraudulent operation. Hopefully, this sends a message out to other fraudsters and reassures the public that work is underway to prevent it happening. Please remember to report any incidents like this to Action Fraud."

Detective Chief Inspector Gary Robinson, head of unit at the Dedicated Card and Payment Crime Unit (DCPCU), said: "Gallagher wrongfully thought he could get away with impersonating organisations and sending out scam text messages, including ones related to the COVID-19 vaccine to commit fraud.

"The DCPCU will continue to crack down on those seeking to exploit this pandemic to defraud the public, through close collaboration with the CPS, mobile phone companies and the banking industry.

"Criminals are experts at impersonating trusted organisations like the NHS, banks or the government and will try to play on people's concerns about their finances at this difficult time. It's therefore vital that the public follow the advice of the Take Five to Stop Fraud campaign and stop and think before parting with any money or information in case it's a scam."

In the last year the CPS has seen cyber criminals look to exploit the COVID-19 pandemic. In response to this, the CPS has issued an ambitious Economic Crime Strategy to combat these offences.

Notes

- John Werhun is a specialist prosecutor for the CPS Specialist Fraud Division

- The CPS Economic Crime Strategy is available at: https://www.cps.gov.uk/publication/economic-crime-strategy-2025

Introduction

Our Economic Crime Strategy provides a high-level vision of where we want to be by 2025, helping to focus our work where it really matters. The strategy is supported by a commitment to ensure the right person is prosecuted for the right offence in a timely manner, that victims and witnesses are at the heart of our casework and that any proceeds of crime are recovered. It represents a clear articulation of the role that the Crown Prosecution Service (CPS) will play in contributing to improving criminal justice outcomes in economic crime.

Economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. This poses a threat to the UK's economy and its institutions and causes serious harm to society and individuals. It includes criminal activity which:

- allows criminals to benefit from the proceeds of their crimes or fund further criminality;
- damages our financial system and harms the interests of legitimate business;
- undermines the integrity of the UK's position as an international financial centre; and
- poses a risk to the UK's prosperity, national security and reputation.

- The *Specialist Fraud Division* is a dedicated CPS team playing a leading role in the fight against serious and complex economic crime and the financial exploitation of the public, using specialist legal expertise to deliver justice. You may visit: https://www.cps.gov.uk/specialist-fraud-division

Specialist Fraud Division

The Specialist Fraud Division is a dedicated prosecuting team within the CPS which deals with the most serious, complex and difficult economic crime cases, including bribery and corruption. It has a national remit and the specialist expertise to prosecute cases investigated by police and a range of other investigative agencies throughout England and Wales.

The Division primarily takes economic crime from specialist units in the City of London Police and the Metropolitan Police Service, but has a number of cases investigated by other forces and has arrangements in place to work with the National Crime Agency (NCA) and regional police fraud units.

SFD also prosecutes serious and complex criminal tax, excise and strategic export cases, which are subject to criminal investigations by Her Majesty's Revenue and Customs (HMRC), in England and Wales.

In addition, SFD prosecutes all criminal cases relating to NHS fraud investigated by NHS Protect and criminal matters investigated by the Medicines and Healthcare Products Regulatory Agency (MHRA).

- The *Dedicated Card and Payment Crime Unit (DCPCU)* is a unique pro-active police unit, with a national remit, formed as a partnership between UK Finance, the City of London Police and the Metropolitan Police together with the Home Office.

  It is fully sponsored by the cards and banking industries, with an on-going brief to investigate, target and, where appropriate, arrest and seek successful prosecution of offenders responsible for card, cheque and payment fraud crimes.

It is headed up by a Detective Chief Inspector and comprises officers from the Metropolitan and City of London police forces who work alongside banking industry fraud investigators and support staff.

In 2020, the unit prevented almost £20 million of fraud, disrupted 26 organised crime groups (OCGs), arrested 122 suspected criminals, and secured 54 convictions

- Teige Gallagher (DOB: 23/01/2000) was sentenced to four years and three months' imprisonment.

Number 2

The money laundering business – making dirty money look clean

How criminals use banks to launder money and how good banks are at protecting themselves from such criminal activities.

BaFin Federal Financial Supervisory Authority

Thomas B. runs a restaurant, but business is not exactly thriving. Five tables and only a handful of guests at the best of times. Yet astonishingly enough he is still able to pay in huge amounts of cash at his bank every Monday and Thursday. Not only friends and neighbours find this a little surprising. The bank employee is equally puzzled whenever B. turns up at the bank in a glamorous limousine.

He broaches the subject with the customer, curious to know how it is that B. regularly pays in such high amounts of money when he has hardly any guests. The bank steps into action in response to a kind of warning system set up by credit institutions in order to track down suspicious transactions.

By now, Thomas B. should be feeling nervous, because the money did not come from his restaurant's culinary delights but from a thriving drug trade. For a long time, his main problem has been finding ways to dispose of all that cash and channel the illicit funds into the legal economic system without attracting attention.

This is where the restaurant comes into play. The only reason he is running it is to conceal the source of his income and make the dirty money look clean. There is just one thing he overlooked – huge earnings and a poorly frequented restaurant simply do not add up. The bank noted this discrepancy, and reported it to the Financial Intelligence Unit (FIU) of the German customs authorities.

This case is purely fictional, but things like this do happen, time and again. And the channels through which the funds flow are often far more convoluted and difficult to trace.

Al Capone and his laundromats

Al Capone was the first to launder money in this way, but not with restaurants. The legendary gangster invested the profits from criminal activities such as prostitution, racketeering, illegal gambling and alcohol trading in a whole chain of laundromats. Capone, who it is claimed never had a bank account, managed to conceal his proceeds by maintaining that they were earnings from the laundromats.

Whether this is fact or mere fiction is unclear. When asked about the source of his earnings at the trial in Chicago in 1931, Capone allegedly replied that he was “in the laundering business”. In any case, it is safe to say that he was probably the first to coin the term “money laundering”. Although this ploy failed to spare him a term in prison, he was not sentenced for murder or blackmail – none of which could be proved against him – but for tax evasion.

Nowadays, criminal investigators have more efficient tools for exposing tricks of this kind, thanks not least to BaFin and the FIU. Banks are obliged to notify the FIU if they regard customers or payments as suspicious. The FIU follows up on these suspicious transaction reports (STRs) and analyses them.

Money laundering prevention during the pandemic

BaFin for its part is responsible for monitoring whether the institutions of the financial sector under its supervision are adequately protecting themselves against being abused for money laundering purposes.

Normally, teams from BaFin travel to the institutions in order to gain an impression on-site of the quality of the institutions’ anti-money laundering (AML) measures. This has become much more difficult since the outbreak of the coronavirus pandemic.

But cancelling the inspections because of the pandemic was out of the question. “From April 2020, we initially conducted our inspections by telephone and then very quickly developed remote solutions which could also be used when working from home“, explained Dr Thorsten Pötzsch, BaFin’s Chief Executive Director also responsible for money laundering prevention.

Following a brief period in the summer, when it was possible to conduct on-site inspections at least subject to certain restrictions, remote inspections then became the norm.

The usual difficulties with lines engaged or microphones and cameras not working properly had been overcome by then and the inspection priorities adapted to take account of a remote working environment. For example, the main focus was placed on risk analysis, questions regarding the AML officer functions and the STR procedure.

BaFin tracks down errors

The inspections were successful. BaFin detected errors, particularly in the institutions' risk analyses, some of which were serious. The institutions had failed to correctly determine and evaluate AML risks.

BaFin's supervisors also identified shortcomings in the suspicious transactions reported by the institutions, although these were generally less serious.

Moreover, many institutions had failed to document cases in accordance with the specifications under the German Money Laundering Act (Geldwäschegesetz – GwG), which made it difficult for BaFin to understand why certain decisions were taken.

At some institutions, BaFin examined the procedure for establishing and verifying the identity of customers, which is crucial in the prevention of money laundering.

It transpired that the institutions had made errors here, too, albeit less when identifying the customers themselves than when establishing the identity of beneficial owners, or persons used by a customer as a representative or messenger for the bank.

But errors had also been made in the identification procedure for politically exposed persons (PEPs). This group of persons includes heads of state, heads of government, ministers, members of the European Commission, members of parliament and constitutional judges to whom particularly strict AML provisions apply.

The inspections also revealed that a number of institutions had failed to update their customer data in due time. A by-product of the inspections was the realisation that many institutions were saving money in the wrong places and should be investing more in IT and in staff.

"Not all institutions are where they should be", said Pötzsch, but an awareness for money laundering has been developed. There has been a sharp rise in the number of suspicious transactions reported to the FIU in recent years, with more than 90 percent of these reports deriving from those sections of the financial sector under BaFin's supervision. Pötzsch notes that institutions and authorities have become more vigilant. "All parties involved are now also far better networked within Germany", he adds, referring to the Anti Financial Crime Alliance (AFCA).

BaFin, the FIU and 14 banks have joined forces in this alliance to address the problem of money laundering (see expert article on the BaFin website dated 18 November 2019).

Plans for the times after the pandemic

When asked how BaFin expects the inspections to be conducted this year, Pötzsch gave a cautious response.

"We don't know how the pandemic will develop and when we will be able to conduct on-site inspections again. One thing is certain – in 2020, we were unable to inspect all the priority areas in the way we had intended. But nothing will be omitted."

BaFin will also deal in-depth with a number of issues, in particular the crypto currency business of institutions, the money-remittance business and the procedure for reporting suspicious transactions.

BaFin is therefore still conducting its inspections off-site and is unlikely, as things currently stand, to return completely to the old system of inspections.

On the one hand, the teams prefer to be present in the institutions' offices as they find the personal contact with the employees important.

On the other hand, the pandemic has shown that remote inspections are possible.

There is one other positive aspect to consider – the teams do not need to travel anywhere and they have more time for the actual inspection. Pötzsch could therefore envisage combining the two forms of inspection in the future – depending on the risk of the institution and inspection priorities.

Money laundering prevention across the EU

The EU Commission plans to present several proposals for more effective joint action against money laundering in Europe.

The proposals are expected to mainly concern the enforcement of standard rules applicable throughout the entire EU. There is also talk of setting up a central European anti-money laundering supervisor.

"What we need is a truly harmonised European legal framework – a regulation that is directly applicable, not just directives that grant the member states too much leeway for implementation, as in the past", said Pötzsch.

A patchwork of supervisory practices will not adequately equip supervisors to combat money laundering effectively, much less prevent it.

The Chief Executive Director is confident that the negotiations will be completed by the end of 2022 and that the regulation will be approved and the legal foundations thus laid for a European anti-money laundering authority.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2103_GW_Fallkonstellationen_en.html

Number 3

US Government Accountability Office

Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market

What GAO Found

Key trends in the current market for cyber insurance include the following:

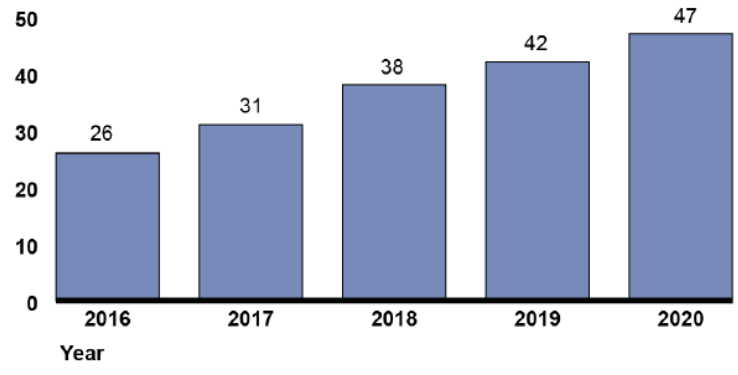
• *Increasing take-up*. Data from a global insurance broker indicate its clients' take-up rate (proportion of existing clients electing coverage) for cyber insurance rose from 26 percent in 2016 to 47 percent in 2020 (see figure).

• *Price increases*. Industry sources said higher prices have coincided with increased demand and higher insurer costs from more frequent and severe cyberattacks. In a recent survey of insurance brokers, more than half of respondents' clients saw prices go up 10–30 percent in late 2020.

• *Lower coverage limits*. Industry representatives told GAO the growing number of cyberattacks led insurers to reduce coverage limits for some industry sectors, such as healthcare and education.

• *Cyber-specific policies*. Insurers increasingly have offered policies specific to cyber risk, rather than including that risk in packages with other coverage. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.

Cyber Insurance Take-up Rates for a Selected Large Broker's Clients, 2016–2020



Source: GAO presentation of data from Marsh McLennan. | GAO-21-477

The cyber insurance industry faces multiple challenges; industry stakeholders have proposed options to help address these challenges.

• *Limited historical data on losses*. Without comprehensive, high-quality data on cyber losses, it can be difficult to estimate potential losses from cyberattacks and price policies accordingly. Some industry participants said federal and state governments and industry could collaborate to collect and share incident data to assess risk and develop cyber insurance products.

• *Cyber policies lack common definitions*. Industry stakeholders noted that differing definitions for policy terms, such as "cyberterrorism," can lead to a lack of clarity on what is covered. They suggested that federal and state governments and the insurance industry could work collaboratively to advance common definitions.

Background

A cyber incident is defined as a cyber event that jeopardizes the cybersecurity of an information system or the information the system processes, stores, or transmits; or an event that violates security policies, procedures, or acceptable use policies, whether resulting from malicious activity or not.

Cyber incidents, including cyberattacks, can damage information technology assets, create losses related to business disruption and theft, release sensitive information, and expose entities to liability from customers, suppliers, employees, and shareholders.

Some private insurance companies offer businesses and other entities cyber insurance to protect against first-party (policyholder) and third-party losses (policyholder's clients or customers) from an event that jeopardizes the confidentiality, integrity, and availability of an information system.

The insurance can be provided through a standalone policy that provides only cyber insurance coverage or as a part of a package policy that provides multiple types of coverage, such as a general commercial liability insurance policy.

States regulate the private insurance market, including for cyber insurance.

The regulators seek to ensure that insurance policy provisions comply with state law, are reasonable and fair, and do not contain major gaps in coverage that might be misunderstood by consumers and leave them unprotected.

States generally do not establish minimum standards for cyber insurance policy coverage; they largely have focused on the solvency of cyber insurers, according to NAIC.

Some states and NAIC have promoted cybersecurity and data protections for insurers.

The Federal Insurance Office in Treasury administers the Terrorism Risk Insurance Program (TRIP), which requires the federal government to share some losses with private insurers in the event of a certified act of terrorism. Losses from cyberattacks might be reimbursed under TRIP if the attacks met certain certification criteria specified by the program.

We will be issuing a report later in 2021 that examines

(1) the risks and costs of cyberattacks on U.S. critical infrastructure;

(2) insurance coverage that is available for losses related to cyber risk, including cyberterrorism; and

(3) the extent to which TRIP, under the Terrorism Risk Insurance Act (TRIA), is structured to respond to cyberattacks and cyberterrorism.

To read more: https://www.gao.gov/assets/gao-21-477.pdf

Number 4

Breaking the Specification: PDF Certification

RUHR-UNIVERSITÄT BOCHUM

Simon Rohlmann
Ruhr University Bochum
simon.rohlmann@rub.de

Vladislav Mladenov
Ruhr University Bochum
vladislav.mladenov@rub.de

Christian Mainka
Ruhr University Bochum
christian.mainka@rub.de

Jörg Schwenk
Ruhr University Bochum
joerg.schwenk@rub.de

Abstract

The Portable Document Format (PDF) is the defacto standard for document exchange.

The PDF specification defines two different types of digital signatures to guarantee the authenticity and integrity of documents: approval signatures and certification signatures.

Approval signatures testify one specific state of the PDF document. Their security has been investigated at CCS'19.

Certification signatures are more powerful and flexible. They cover more complex workflows, such as signing contracts by multiple parties.

To achieve this goal, users can make specific changes to a signed document without invalidating the signature.

This paper presents the first comprehensive security evaluation on certification signatures in PDFs. We describe two novel attack classes – Evil Annotation and Sneaky Signature attacks which abuse flaws in the current PDF specification.

Both attack classes allow an attacker to significantly alter a certified document's visible content without raising any warnings.

Our practical evaluation shows that an attacker could change the visible content in 15 of 26 viewer applications by using Evil Annotation attacks and in 8 applications using Sneaky Signature by using PDF specification compliant exploits.

We improved both attacks' stealthiness with applications' implementation issues and found only two applications secure to all attacks.

On top, we show how to gain high privileged JavaScript execution in Adobe. We responsibly disclosed these issues and supported the vendors to fix the vulnerabilities.

We also propose concrete countermeasures and improvements to the current specification to fix the issues.

To read more: https://www.nds.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2021/05/25/Breaking_the_Specification__PDF_Certification.pdf

Number 5

Cyber resilience practices - Executive Summary

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

The financial sector faces significant exposure to cyber risk given that it is information technology-intensive and highly interconnected through payment systems.

Therefore, it is important for financial firms to strengthen their cyber resilience, which is defined by the Financial Stability Board (FSB) as "the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents."

Within the financial sector, banks typically have the most public-facing products and services.

Bank systems have multiple points of contact with outside parties, which can mean significant vulnerability to cyberattacks, with those interfaces being used as entry points for attacks targeting other parts of the financial system.

Bank supervisory authorities have established regulatory and supervisory frameworks to enhance banks' cyber resilience.

Cyber-resilience:

Range of practices

December 2018

In 2018, the Basel Committee on Banking Supervision (BCBS) issued a report entitled *Cyber-resilience: Range of practices* that describes and compares regulatory approaches and supervisory practices across BCBS member jurisdictions. You may visit:
https://www.bis.org/bcbs/publ/d454.pdf

Regulation and supervision

Regulators expect banks to address cyber risk either in their risk management and/or information security frameworks or in their specific cybersecurity strategies.

The latter includes requirements related to governance and oversight; risk ownership and accountability; information security; periodic evaluation and monitoring of cybersecurity controls; incident response; business continuity; and recovery planning.

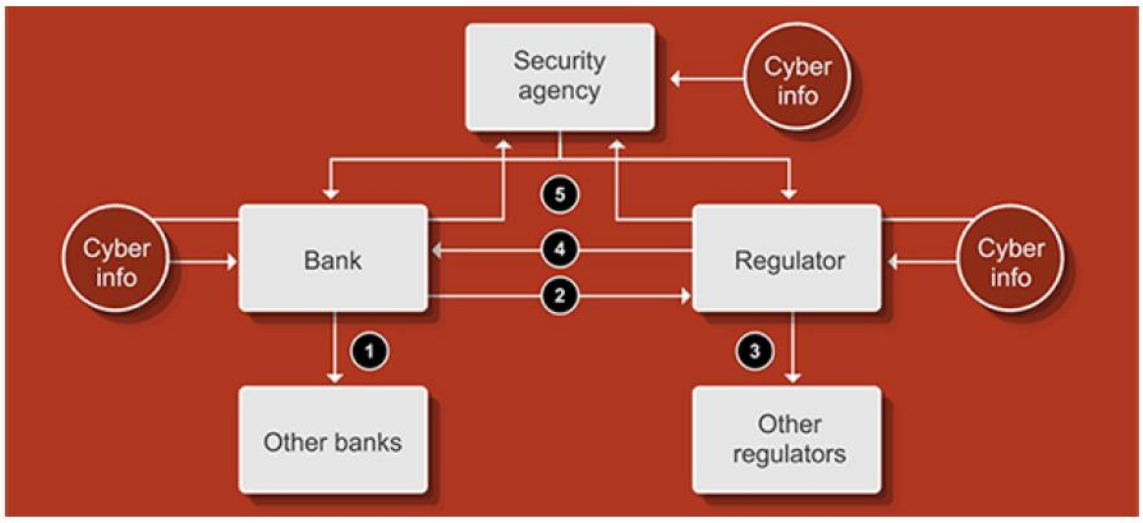
Supervisors assess banks' cybersecurity controls and their monitoring and surveillance of emerging threats. These assessments are based on banks' adherence to existing industry standards.

Supervisory assessments also include challenges to bank approaches to testing controls and the remediation of issues identified.

Challenges can include the review of control testing reports, which may be part of a more formal testing programme.

Such a programme could employ various testing methodologies and practices, such as vulnerability assessment, penetration testing and red team testing.

To read more: https://www.bis.org/fsi/fsisummaries/cyber_resilience.pdf



Number 6

Whom do consumers trust with their data? US survey evidence

Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster
and Kelly Shue

BIS

Key takeaways

- In a recent survey, US households say they are more likely to trust traditional financial institutions than government agencies or fintechs to safeguard their personal data. They have far less trust in big techs.

- This pattern differs across demographic groups: respondents from racial minorities have less trust in financial institutions, while younger respondents trust fintechs relatively more. Female, minority and younger respondents are more concerned about implications of data-sharing for their personal safety.

- A quarter of respondents say Covid-19 made them less willing to share data. In this group, nearly half became less willing to share with big techs. Concerns centred on identity theft and abuse of data.

- As the economy becomes increasingly digital, and new players expand further into financial services, strong data protection policies will become more important to shield consumers from these harms.

Personal data lie at the heart of the digital economy. Recommendations for online shopping, personalised financial advice or credit increasingly rely on users' digital footprints (Berg et al (2020)).

Large technology companies (big techs) are muscling their way into payments and lending, leveraging the vast amounts of personal data they have collected in other business lines.

The Covid-19 pandemic has accelerated these trends, forcing many employees to work remotely and consumers to shop online (Alfonso et al (2021)).

The resulting increase in online activity makes personal data even more abundant, and more valuable.

Currently, companies often collect and analyse these personal data without consumers' explicit consent or full understanding.

While the analysis of such data can benefit consumers through improved movie recommendations or better targeted online ads, not everybody is equally comfortable with sharing their data.

Rather, this unrestrained collection of personal data represents an unprecedented erosion of consumer privacy, raising important concerns around data abuse and even personal safety – even if the degree of these concerns may vary across different segments of society.

This Bulletin focuses on the willingness of consumers to share data and trust in different actors, based on a representative high-quality survey of US household heads.

It assesses Americans' trust in different counterparties to safely handle their data – governments, traditional financial institutions (FIs), fintechs and large technology firms (big techs) – according to differences in the respondents' gender, ethnicity and age.

The Bulletin also investigates how Covid-19 has changed attitudes and concerns towards privacy. It concludes by discussing the implications for data privacy and digital identity in financial services.

The Survey of Consumer Expectations

We investigate the attitudes towards data privacy of Americans in the Survey of Consumer Expectations (SCE).

The SCE is a high-quality monthly, internet-based survey produced by the Federal Reserve Bank of New York.

Launched in 2013, it is used extensively to help researchers and policymakers understand how expectations are formed and how they affect consumer behaviour.

The SCE is a 12-month rotating panel of roughly 1,300 nationally representative US household heads.

New respondents are drawn each month to match demographic targets from the American Community Survey, and they stay on the panel for up to 12 months before rotating out.

The survey's main aim is to collect expectations for a wide range of economic outcomes (eg inflation, income, spending, household finance, employment and housing).

The survey includes a wealth of detailed demographic information, including the respondent's gender, race, age, income, education, financial literacy and willingness to take risks (Armantier et al (2017)).

To understand how consumers value their data privacy, what determines their willingness to share data and how much they trust different counterparties, the September 2020 survey contained an additional module.

The module asked detailed questions on respondents' attitudes towards data privacy, for example how much they trust different counterparties to safeguard their data, and how the Covid-19 pandemic has affected these attitudes.

In what follows, we use this information to investigate how consumers' attitudes towards and concerns about privacy differ across demographic groups and whether they have changed in response to the pandemic.

To read more: https://www.bis.org/publ/bisbull42.pdf

Number 7

Testimony before the Senate Committee on Banking, Housing and Urban Affairs

Kenneth A. Blanco, Director, Financial Crimes Enforcement Network

Chairman Crapo, Ranking Member Brown, Members of the Committee, thank you for having me here today to discuss eliminating anonymous shell corporations by collecting beneficial ownership information in order to preserve our national security and protect our people from harm.

A Russian arms dealer nicknamed the "The Merchant of Death," who sold weapons to a terrorist organization intent on killing Americans. Executives from a supposed investment group that perpetrated a Ponzi scheme that defrauded more than 8,000 investors, most of them elderly, of over $1 billion. A complex nationwide criminal network that distributed oxycodone by flying young girls and other couriers carrying pills all over the United States.

A New York company that was used to conceal Iranian assets, including those designated for providing financial services to entities involved in Iran's nuclear and ballistic missile program. A former college athlete who became the head of a gambling enterprise and a violent drug kingpin who sold recreational drugs and steroids to college and professional football players. A corrupt Venezuelan treasurer who received over $1 billion in bribes.

These crimes are very different, as are the dangers they pose and the damage caused to innocent and unsuspecting people. The defendants and bad actors come from every walk of life and every corner of the globe. The victims—both direct and indirect—include Americans exposed to terrorist acts; elderly people losing life savings; a young mother becoming addicted to opioids; a college athlete coerced to pay extraordinary debts by violent threats; and an entire country driven to devastation by corruption. But all these crimes have one thing in common: shell corporations were used to hide, support, prolong, or foster the crimes and bad acts committed against them.

These criminal conspiracies thrived at least in part because the perpetrators could hide their identities and illicit assets behind shell companies. Had beneficial ownership information been available, and more quickly accessible to law enforcement and others, it would have been harder and more costly for the criminals to hide what they were doing. Law enforcement could have been more effective and efficient in preventing

these crimes from occurring in the first place, or could have intercepted them sooner and prevented the scope of harm these criminals caused from spreading.

Financial sanctions could have been leveraged sooner to disrupt global threats, block assets within U.S. jurisdiction, identify sanctions evaders, and incentivize behavior change. With clearer information on the actors behind front companies, the efficacy of the Office of Foreign Assets Control's (OFAC) sanctions and the Financial Crimes Enforcement Network's (FinCEN) anti-money laundering authorities would improve, enabling us to more effectively secure our nation and achieve our foreign policy goals.

Case Examples

Viktor Bout was engaged in international arms trafficking for many years, arming some of the most violent conflicts around the globe. Known as "The Merchant of Death," Bout was finally apprehended when he agreed to sell millions of dollars' worth of weapons to confidential informants representing they were acting on behalf of the Fuerzas Armadas Revolucionarias de Colombia (the "FARC"), a U.S. designated terrorist organization, with the specific understanding that the weapons were to be used to attack U.S. helicopters in Colombia.

Specifically, he agreed to sell 700-800 surface-to-air missiles, over 20,000 AK-47 firearms, 10 million rounds of ammunition, five tons of C-4 plastic explosives, "ultralight" airplanes outfitted with grenade launchers, and unmanned aerial vehicles. To support his vast arms dealing business, Bout incorporated at least twelve shell corporations in Texas, Florida, and Delaware.

Robert Shapiro, owner of Woodbridge Group of Companies LLC, and his former Directors of Investments were charged with orchestrating a massive Ponzi scheme from 2012 to 2017. They promoted speculative and fraudulent securities to potential investors, targeting elderly investors who had Individual Retirement Accounts ("IRAs") through high-pressure sales tactics, deception, material misrepresentations, and investor manipulation.

Shapiro and his group were responsible for fraudulently stealing $1.2 billion from more than 8,000 retail investors, most of them elderly retirees. At one point, Shapiro and his co-conspirators had approximately 600 employees working for them, and used roughly 100 U.S. shell corporations to hide assets and further their Ponzi scheme.

Kingsley Iyare Osemwengie and 17 other co-conspirators used call girls, couriers, commercial carriers, and the U.S. mail to distribute oxycodone

pills all over the United States, thereby contributing to our current opioid addiction epidemic. More than 70 couriers took nearly 800 flights to 40 different U.S. cities that the conspiracy used to move drugs and money. Osemwengie and other co-conspirators netted millions of dollars of drug proceeds that allowed them to live opulent lifestyles. They maintained luxury residences in Las Vegas, Nevada, and Miami, Florida and drove high-end automobiles, including two Mercedes-Benzes and four Bentleys. Osemwengie's complex oxycodone network hid the source of their income behind several U.S. shell companies.

Bank Melli, a bank owned and run by the Government of Iran that was designated under a counter-proliferation authority and now is subject to counterterrorism sanctions, hid the fact that it owned and operated a skyscraper on Manhattan's Fifth Avenue generating millions upon millions of dollars for the Iranian government and its malign activities, right under the nose of U.S. authorities. Bank Melli violated U.S. sanctions by, among other things, creating two shell companies in New York to generate revenue for the Iranian regime.

Owen Hanson, leader of the violent "ODOG Enterprise," operated an international drug trafficking, gambling, and money laundering enterprise in the United States, Central and South America, and Australia from 2012 to 2016. Hanson trafficked hundreds of kilograms of cocaine, heroin, methamphetamine, MDMA ("ecstasy"), anabolic steroids, and Human Growth Hormone ("HGH"), including to numerous professional athletes, earning millions of dollars in illegal proceeds.

He also operated a vast illegal gambling operation focused on high-stakes wagers placed on sporting events, using threats and violence against his gambling and drug customers to force compliance. Hanson set up numerous domestic shell companies to launder the proceeds of his crimes, hide assets, and continue his criminal enterprise.

Alejandro Andrade Cedeno, a former Venezuelan national treasurer, received over $1 billion in bribes from co-conspirators in exchange for using his position as Venezuelan national treasurer to select them to conduct currency exchange transactions at favorable rates for the Venezuelan government.

He received cash as well as private jets, yachts, cars, homes, champion horses, and high-end watches from his co-conspirators. As part of his plea agreement, Andrade agreed to a forfeiture money judgment of $1 billion and forfeiture of all assets involved in the corrupt scheme, including real estate, vehicles, horses, watches, aircraft, and bank accounts. This corrupt Venezuelan public official funneled the proceeds of his bribery to U.S. shell companies.

Impact on National Security and Safety of Citizens

Stories of ordinary people and taxpayers victimized by criminals exploiting and hiding behind the secrecy of shell companies are all too common. Opaque corporate structures such as shell corporations facilitate anonymous access to the financial system for every type of criminal and terrorist activity.

Narcotraffickers, corrupt leaders, rogue states, terrorists, and fraudsters of all kinds establish domestic shell companies to mask and further criminal activity, to invest and buy assets with illicit proceeds, and to prevent law enforcement and others from efficiently and effectively investigating tips or leads. We recognize that corporations, limited liability companies, partnerships, and other entity structures play a vital role in domestic and global commerce, but they are also vulnerable to abuse, and currently pose a gap—a dangerous gap—in our national security apparatus that we need to address.

FinCEN's recent Customer Due Diligence Final Rule (CDD rule), which requires the collection of beneficial ownership information when opening an account at a bank or other financial institution, is but one critical step toward closing this national security gap. The second critical step in closing this national security gap is collecting beneficial ownership information at the corporate formation stage.

One of the most effective ways to deter criminals and to stem the harms that flow from their actions—including harm to American citizens and our financial system—is to follow the money, expose illicit activity, and prevent networks from operating undetected or secretly benefiting from the enormous power of our economy and financial system.

Identifying and disrupting illicit financial networks not only assists in the prosecution of criminal activity of all kinds, but also allows law enforcement to halt and dismantle criminal organizations and other bad actors before they harm our citizens or our financial system.

It also allows us to use economic statecraft to expose and dissuade nefarious activity that threatens our country and the integrity of the global financial system, including through OFAC's sanctions and FinCEN's authorities, such as identifying primary money laundering concerns under Section 311 of the USA PATRIOT Act.

Money laundering and its associated crimes and bad acts undermines the rule of law and our democracy because it supports and rewards corruption and other crimes, allowing it to grow and fester. As such, our efforts to

combat money laundering directly affect the safety and security of the American public, the stability of our nation, and its national security.

As a former State and Federal prosecutor, I know firsthand how difficult it is to trace assets hidden through a variety of legal entities. To determine the true owner of a shell company or front company in the United States today requires law enforcement to undertake a time-consuming and resource-intensive process.

It often requires human source information, grand jury subpoenas, surveillance operations, witness interviews, search warrants, and foreign legal assistance requests to get behind the outward facing structure of these shell companies.

This takes an enormous amount of time—time that could be used to further other important and necessary aspects of an investigation—and wastes resources, or prevents investigators from getting to other equally important investigations.

The collection of beneficial ownership information at the time of company formation would significantly reduce the amount of time currently required to research who is behind anonymous shell companies, and at the same time, prevent the flight of assets and the destruction of evidence.

Global Impact

As cross-border crime continues to proliferate—and it is most certainly proliferating—our efforts to combat the most sophisticated white-collar and cyber criminals require law enforcement to work with our partners all over the world to seek the evidence and witnesses necessary to build their cases.

We need to collaborate with our foreign counterparts, not only to investigate crimes that have been committed and to cooperate on sanctions, but also to intercept ongoing crimes and to prevent crimes from occurring in the first place.

We must be nimble in order to coordinate quickly, effectively, and fluently with our counterparts abroad. Criminals and other bad actors do not have borders and do not comport with the rule of law. To combat them, we need to work seamlessly with our foreign counterparts in a way that is efficient and effective.

Just as we receive significant assistance from our foreign partners in our investigations and prosecutions, we too must provide significant assistance to them in researching the beneficial owners of U.S. shell companies. This

coordination is especially important when crimes are being planned by overseas actors targeting victims in the United States, or when bad actors use our financial system or opaque corporate structures to victimize people globally, including in the United States.

The bottom line is that we need our foreign partners to have important information in a timely way, in order to stop and arrest criminals overseas to prevent harm caused to us here at home. This balanced model of reciprocity in information sharing is a vital tool in modern prosecution—whether the prosecutor is sitting in the United States, Europe, South America or elsewhere.

However, identifying beneficial ownership information in the United States can only be achieved today through a long, drawn-out process with many hoops, twists, and turns. This often dissuades some of our partners overseas from working with us.

Indeed, the Financial Action Task Force (FATF)—a global inter-governmental body responsible for developing and promoting policies to protect the global financial system against money laundering and other threats, composed of thirty eight members, including all the G-7 countries and our most reliable partners—recognized and highlighted in the 2016 Mutual Evaluation this issue as one of the most critical gaps in the United States' compliance with its standards.

FATF noted that the lack of beneficial ownership information significantly slows investigations because determining the true ownership of bank accounts and other assets often requires that law enforcement undertake a time-consuming and resource-intensive process.

While we have since implemented customer due diligence requirements, more must be done. Collecting beneficial ownership information at company formation would assist us and our foreign partners as we collaborate to stop criminals, seize and forfeit illicit assets, and protect the public.

As more and more of our allies begin to collect beneficial ownership information at the incorporation stage in their countries and make it accessible to law enforcement, the U.S. risks becoming a safe haven for bad actors looking to hide their assets.

As Americans, we have always led in the areas of rule of law, security, and law enforcement. Our failure to lead here is perplexing to the global community that has come to rely on and expect our leadership.

Conclusion

In conclusion, the time to address this important issue is now. As Treasury Secretary Mnuchin has stated several times in Congressional testimony, beneficial ownership information at corporate formation is an important issue to the Department of the Treasury.

It is critical for the security of our nation and its citizens that Congress act to eliminate one of the most useful tools used by criminals to perpetrate their crimes, hide their proceeds, and subvert law enforcement.

That is why we appreciate this Committee's work on this issue, and we hope to work with Congress on developing a bipartisan solution to collecting this important information to protect our national security and the people of our nation. I am happy to take any questions you may have.

Number 8

Another Nobelium Cyberattack

Tom Burt, Corporate Vice President, Customer Security & Trust

Microsoft

UPDATE (May 28, 2021, 1pm PT): Our teams have continued to investigate the latest wave of phishing attacks launched by Nobelium.

Based on what we currently know, the security community should feel good about the collective work done to limit the damage done by this wave of attacks.

As we have notified our targeted customers and watched closely for other reports, we are not seeing evidence of any significant number of compromised organizations at this time.

More importantly, antivirus services, like Microsoft Defender Antivirus, and endpoint detection and response products, such as Microsoft Defender for Endpoint, are identifying and protecting against the malware being used in this wave of attacks and are working in combination with Microsoft Defender for Office 365.

It is important for all users to employ basic cybersecurity hygiene, including using multi-factor authentication, using antivirus/antimalware software and being careful not to click on links in email, unless you can confirm reliability to minimize the risk of being phished.

We will continue to monitor the situation.

This week we observed cyberattacks by the threat actor Nobelium targeting government agencies, think tanks, consultants, and non-governmental organizations.

This wave of attacks targeted approximately 3,000 email accounts at more than 150 different organizations.

While organizations in the United States received the largest share of attacks, targeted victims span at least 24 countries.

At least a quarter of the targeted organizations were involved in international development, humanitarian, and human rights work. Nobelium, originating from Russia, is the same actor behind the attacks on SolarWinds customers in 2020.

These attacks appear to be a continuation of multiple efforts by Nobelium to target government agencies involved in foreign policy as part of intelligence gathering efforts.

Nobelium launched this week's attacks by gaining access to the Constant Contact account of USAID. Constant Contact is a service used for email marketing.

From there, the actor was able to distribute phishing emails that looked authentic but included a link that, when clicked, inserted a malicious file used to distribute a backdoor we call NativeZone.

This backdoor could enable a wide range of activities from stealing data to infecting other computers on a network.

You can read more about the technical aspects of these attacks in this blog post from the Microsoft Threat Intelligence Center (MSTIC).

Many of the attacks targeting our customers were blocked automatically, and Windows Defender is blocking the malware involved in this attack.

We're also in the process of notifying all of our customers who have been targeted.

We detected this attack and identified victims through the ongoing work of the MSTIC team in tracking nation-state actors.

We have no reason to believe these attacks involve any exploit against or vulnerability in Microsoft's products or services.

These attacks are notable for three reasons.

First, when coupled with the attack on SolarWinds, it's clear that part of Nobelium's playbook is to gain access to trusted technology providers and infect their customers.

By piggybacking on software updates and now mass email providers, Nobelium increases the chances of collateral damage in espionage operations and undermines trust in the technology ecosystem.

Second, perhaps unsurprisingly, Nobelium's activities and that of similar actors tend to track with issues of concern to the country from which they are operating. This time Nobelium targeted many humanitarian and human rights organizations.

At the height of the Covid-19 pandemic, Russian actor Strontium targeted healthcare organizations involved in vaccines.

In 2019, Strontium targeted sporting and anti-doping organizations. And we've previously disclosed activity by Strontium and other actors targeting major elections in the U.S. and elsewhere.

This is yet another example of how cyberattacks have become the tool of choice for a growing number of nation-states to accomplish a wide variety of political objectives, with the focus of these attacks by Nobelium on human rights and humanitarian organizations.

Third, nation-state cyberattacks aren't slowing. We need clear rules governing nation-state conduct in cyberspace and clear expectations of the consequences for violation of those rules.

We must continue to rally around progress made by the Paris Call for Trust and Security in Cyberspace, and more widely adopt the recommendations of the Cybersecurity Tech Accord, and the CyberPeace Institute. But, we need to do more.

Microsoft will continue to work with willing governments and the private sector to advance the cause of digital peace.

To read more: https://blogs.microsoft.com/on-the-issues/2021/05/27/nobelium-cyberattack-nativezone-solarwinds/

Number 9

Undated Privacy Policy for users having their usual residence in the US

TikTok

Last updated: June 2, 2021. We have updated our Privacy Policy. Among other clarifying changes, we have added more details about the information we collect and how it's used, including clarifications related to, for example, collection of user content information, use of data for verification, ad related choices, data sharing with third party services, and data storage/processing practices.

Welcome to TikTok (the "Platform"). The Platform is provided and controlled by TikTok Inc. ("TikTok", "we" or "us"). We are committed to protecting and respecting your privacy.

This Privacy Policy covers the experience we provide for users age 13 and over on our Platform. For information about our under-13 experience ("Children's Platform") and our practices in the United States regarding children's privacy, please refer to our Privacy Policy for Younger Users.

Capitalized terms that are not defined in this policy have the meaning given to them in the Terms of Service at: https://www.tiktok.com/legal/terms-of-service?lang=en#terms-us

What information do we collect?

We collect information when you create an account or use the Platform. We also collect information you share with us from third-party social network providers, and technical and behavioral information about your use of the Platform.

We also collect information contained in the messages you send through our Platform and, if you grant us access, information from your phone book on your mobile device. More information about the categories and sources of information is provided below.

Information you choose to provide

For certain activities, such as when you register, upload content to the Platform, or contact us directly, you may provide some or all of the following information:

- Registration information, such as age, username and password, language, and email or phone number

- Profile information, such as name, social media account information, and profile image

- User-generated content, including comments, photographs, livestreams, audio recordings, videos, and virtual item videos that you choose to create with or upload to the Platform ("User Content").

  We collect User Content through pre-loading at the time of creation, import, or upload, regardless of whether you choose to save or upload that User Content, in order to recommend audio options and provide other personalized recommendations. If you apply an effect to your User Content, we may collect a version of your User Content that does not include the effect.

- Content, including text, images, and video, found in your device's clipboard, with your permission. For example, if you choose to initiate content sharing with a third-party platform, or choose to paste content from the clipboard into the TikTok App, we access this information stored in your clipboard in order to fulfill your request.

- Payment information, including payment card numbers or other third-party payment information (such as PayPal) where required for the purpose of payment

- Your phone and social network contacts, with your permission. If you choose to find other users through your phone contacts, we will access and collect the names and phone numbers and match that information against existing users of the Platform. If you choose to find other users through your social network contacts, we will collect your public profile information as well as names and profiles of your social network contacts

- Your opt-in choices and communication preferences

- Information to verify an account such as proof of identity or age

- Information in correspondence you send to us

- Information you share through surveys or your participation in challenges, sweepstakes, or contests such as your gender, age, likeness, and preferences.

Information we obtain from other sources

We may receive the information described in this Privacy Policy from other sources, such as:

Social Media and Login Services. If you choose to link or sign up using a third-party social network or login service (such as Facebook, Twitter, Instagram, or Google), we may collect information from these services, including your contact lists for these services and information relating to your use of the Platform in relation to these services. If you link your TikTok account to another service, we may receive information about your use of that service.

Third-Party Services. We may collect information about you from third-party services, such as advertising partners, data providers, and analytics providers.

Other Users of the Platform. Sometimes other users of the Platform may provide us information about you, including through customer service inquiries.

Other Sources. We may collect information about you from other publicly available sources.

Information we collect automatically

We automatically collect certain information from you when you use the Platform, including internet or other network activity information such as your IP address, geolocation-related data (as described below), unique device identifiers, browsing and search history (including content you have viewed in the Platform), and Cookies (as defined below).

Usage Information

We collect information regarding your use of the Platform and any other User Content that you generate through or upload to our Platform.

Device Information

We collect certain information about the device you use to access the Platform, such as your IP address, user agent, mobile carrier, time zone settings, identifiers for advertising purposes, model of your device, the device system, network type, device IDs, your screen resolution and operating system, app and file names and types, keystroke patterns or rhythms, battery state, audio settings and connected audio devices. Where you log-in from multiple devices, we will be able to use your profile information to identify your activity across devices. We may also associate

you with information collected from devices other than those you use to log-in to the Platform.

Location data

We collect information about your approximate location, including location information based on your SIM card and/or IP address. With your permission, we may also collect precise location data (such as GPS).

Image and Audio Information

We may collect information about the images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content.

We may collect this information to enable special video effects, for content moderation, for demographic classification, for content and ad recommendations, and for other non-personally-identifying operations.

We may collect biometric identifiers and biometric information as defined under US laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you prior to any such collection.

Messages

We collect and process, which includes scanning and analyzing, information you provide when you compose, send, or receive messages through the Platform's messaging functionality.

That information includes the content of the message and information about when the message has been sent, received and/or read, as well as the participants of the communication.

Please be aware that messages sent to other users of the Platform will be accessible by those users and that we are not responsible for the manner in which those users use or disclose messages.

Metadata

When you upload or create User Content, you automatically upload certain metadata that is connected to the User Content. Metadata describes other data and provides information about your User Content that will not always be evident to the viewer.

In connection with your User Content the metadata can describe how, when, where, and by whom the piece of User Content was created, collected, or modified and how that content is formatted.

It also includes information, such as your account name, that enables other users to trace back the User Content to your user account. Additionally, metadata includes data that you choose to provide with your User Content, e.g. any hashtags used to mark keywords to the video and captions.

Cookies

We and our service providers and business partners use cookies and other similar technologies (e.g. web beacons, flash cookies, etc.) ("Cookies") to automatically collect information, measure and analyze which web pages and advertisements you click on and how you use the Platform, enhance your experience using the Platform, improve the Platform, provide you with advertising on the Platform and elsewhere across your devices, and measure the effectiveness of advertisements.

Cookies enable the Platform to provide certain features and functionality. Web beacons are very small images or small pieces of data embedded in images, also known as "pixel tags" or "clear GIFs," that can recognize Cookies, the time and date a page is viewed, a description of the page where the pixel tag is placed, and similar information from your computer or device. To learn how to disable Cookies, see the "Your choices" section below.

We and our service providers and business partners may link your contact or account information with your activity on and off our Platform across all your devices, using your email or other log-in or device information.

Our service providers and business partners may use this information to display advertisements on our Platform and elsewhere online and across your devices tailored to your interests, preferences, and characteristics.

We are not responsible for the privacy practices of these service providers and business partners, and the information practices of these service providers and business partners are not covered by this Privacy Policy.

We may aggregate or de-identify the information described above. Aggregated or de-identified data is not subject to this Privacy Policy.

To read more: https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-eea

If you are a user having your usual residence in the EEA, United Kingdom or Switzerland, this Privacy Policy shall apply: https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-eea

If you are not in the US, EEA, United Kingdom or Switzerland,this Privacy Policy shall apply: https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-row

Number 10

Private money and central bank money as payments go digital - an update on CBDCs

Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Consensus by CoinDesk 2021 Conference, Washington DC

Technology is driving dramatic change in the U.S. payments system, which is a vital infrastructure that touches everyone.

The pandemic accelerated the migration to contactless transactions and highlighted the importance of access to safe, timely, and low-cost payments for all.

With technology platforms introducing digital private money into the U.S. payments system, and foreign authorities exploring the potential for *central bank digital currencies (CBDCs)* in cross-border payments, the Federal Reserve is stepping up its research and public engagement on CBDCs.

As Chair Powell discussed last week, an important early step on public engagement is a plan to publish a discussion paper this summer to lay out the Federal Reserve Board's current thinking on digital payments, with a particular focus on the benefits and risks associated with CBDC in the U.S. context.

Sharpening the Focus on CBDCs

Four developments—the growing role of digital private money, the migration to digital payments, plans for the use of foreign CBDCs in cross-border payments, and concerns about financial exclusion—are sharpening the focus on CBDCs.

First, some technology platforms are developing stablecoins for use in payments networks.

A stablecoin is a type of digital asset whose value is tied in some way to traditional stores of value, such as government-issued, or fiat, currencies or gold.

Stablecoins vary widely in the assets they are linked to, the ability of users to redeem the stablecoin claims for the reference assets, whether they allow unhosted wallets, and the extent to which a central issuer is liable for making good on redemption rights.

Unlike central bank fiat currencies, stablecoins do not have legal tender status.

Depending on underlying arrangements, some may expose consumers and businesses to risk.

If widely adopted, stablecoins could serve as the basis of an alternative payments system oriented around new private forms of money.

Given the network externalities associated with achieving scale in payments, there is a risk that the widespread use of private monies for consumer payments could fragment parts of the U.S. payment system in ways that impose burdens and raise costs for households and businesses.

A predominance of private monies may introduce consumer protection and financial stability risks because of their potential volatility and the risk of run-like behavior.

Indeed, the period in the nineteenth century when there was active competition among issuers of private paper banknotes in the United States is now notorious for inefficiency, fraud, and instability in the payments system.

It led to the need for a uniform form of money backed by the national government.

Second, the pandemic accelerated the migration to digital payments. Even before the pandemic, some countries, like Sweden, were seeing a pronounced migration from cash to digital payments.

To the extent that digital payments crowd out the use of cash, this raises questions about how to ensure that consumers retain access to a form of safe central bank money.

In the United States, the pandemic led to an acceleration of the migration to digital payments as well as increased demand for cash.

While the use of cash spiked at certain times, there was a pronounced shift by consumers and businesses to contactless transactions facilitated by electronic payments.

The Federal Reserve remains committed to ensuring that the public has access to safe, reliable, and secure means of payment, including cash.

As part of this commitment, we must explore—and try to anticipate—the extent to which households' and businesses' needs and preferences may migrate further to digital payments over time.

Third, some foreign countries have chosen to develop and, in some cases, deploy their own CBDC.

Although each country will decide whether to issue a CBDC based on its unique domestic conditions, the issuance of a CBDC in one jurisdiction, along with its prominent use in cross-border payments, could have significant effects across the globe.

Given the potential for CBDCs to gain prominence in cross-border payments and the reserve currency role of the dollar, it is vital for the United States to be at the table in the development of cross-border standards.

Finally, the pandemic underscored the importance of access to timely, safe, efficient, and affordable payments for all Americans and the high cost associated with being unbanked and underbanked.

While the large majority of pandemic relief payments moved quickly via direct deposits to bank accounts, it took weeks to distribute relief payments in the form of prepaid debit cards and checks to households who did not have up-to-date bank account information with the Internal Revenue Service.

The challenges of getting relief payments to these households highlighted the benefits of delivering payments more quickly, cheaply, and seamlessly through digital means.

Policy Considerations

In any assessment of a CBDC, it is important to be clear about what benefits a CBDC would offer over and above current and emerging payments options, what costs and risks a CBDC might entail, and how it might affect broader policy objectives.

I will briefly discuss several of the most prominent considerations.

Preserve general access to safe central bank money

Central bank money is important for payment systems because it represents a safe settlement asset, allowing users to exchange central bank liabilities without concern about liquidity and credit risk.

Consumers and businesses don't generally consider whether the money they are using is a liability of the central bank, as with cash, or of a commercial bank, as with bank deposits.

This is largely because the two are seamlessly interchangeable for most purposes owing to the provision of federal deposit insurance and banking supervision, which provide protection for consumers and businesses alike.

It is not obvious that new forms of private money that reference fiat currency, like stablecoins, can carry the same level of protection as bank deposits or fiat currency.

Although various federal and state laws establish protections for users, nonbank issuers of private money are not regulated to the same extent as banks, the value stored in these systems is not insured directly by the Federal Deposit Insurance Corporation, and consumers may be at risk that the issuer will not be able to honor its liabilities.

New forms of private money may introduce counterparty risk into the payments system in new ways that could lead to consumer protection threats or, at large scale, broader financial stability risks.

In contrast, a digital dollar would be a new type of central bank money issued in digital form for use by the general public. By introducing safe central bank money that is accessible to households and businesses in digital payments systems, a CBDC would reduce counterparty risk and the associated consumer protection and financial stability risks.

Improve efficiency

One expected benefit is that a CBDC would reduce or even eliminate operational and financial inefficiencies, or other frictions, in payments, clearing, and settlement.

Today, the speed by which consumers and businesses can access the funds following a payment can vary significantly, up to a few days when relying on certain instruments, such as a check, to a few seconds in a real-time payments system.

Advances in technology, including the use of distributed ledgers and smart contracts, may have the potential to fundamentally change the way in

which payment activities are conducted and the roles of financial intermediaries and infrastructures.

The introduction of a CBDC may provide an important foundation for beneficial innovation and competition in retail payments in the United States.

Most immediately, we are taking a critical step to build a strong foundation with the introduction of the FedNowSM Service, a new instant payments infrastructure that is scheduled to go into production in two years.

The FedNow Service will enable banks of every size and in every community across America to provide safe and efficient instant payment services around the clock, every day of the year.

Through the banks using the service, consumers and businesses will be able to send and receive payments conveniently, such as on a mobile device, and recipients will have full access to funds immediately.

Promote competition and diversity and lower transactions costs

Today, the costs of certain retail payments transactions are high and not always transparent to end users.

Competition among a diversity of payment providers and payment types has the potential to increase the choices available to businesses and consumers, reduce transactions costs, and foster innovation in end-user services, although it could also contribute to fragmentation of the current payments system.

By providing access to a digital form of safe central bank money, a CBDC could provide an important foundation on which private-sector competition could flourish.

Reduce cross-border frictions

Cross-border payments, such as remittances, represent one of the most compelling use cases for digital currencies.

The intermediation chains for cross-border payments are notoriously long, complex, costly, and opaque.

Digitalization, along with a reduction in the number of intermediaries, holds considerable promise to reduce the cost, opacity, and time required for cross-border payments.

While the introduction of CBDCs may be part of the solution, international collaboration on standard setting and protections against illicit activity will be required in order to achieve material improvements in cost, timeliness, and transparency.

We are collaborating with international colleagues through the Bank for International Settlements, Committee on Payments and Market Infrastructures, and the G7 to ensure the U.S. stays abreast of developments related to CBDC abroad.

We are engaging in several international efforts to improve the transparency, timeliness, and cost-effectiveness of cross-border payments. It will be important to be engaged at the outset on the development of any international standards that may apply to CBDCs, given the dollar's important role as a reserve currency.

Complement currency and bank deposits

A guiding principle for any payments innovation is that it should improve upon the existing payments system. Consumers have access to reliable money in the forms of private bank accounts and central bank issued currency, which form the underpinnings of the current retail payments system. The design of any CBDC should complement and not replace currency and bank accounts.

Preserve financial stability and monetary policy transmission

The introduction of a CBDC has the potential to have wide-reaching effects, and there are open questions about how CBDC could affect financial stability and monetary policy transmission.

Some research indicates that the introduction of a CBDC might raise the risk of a flight out of deposits at weak banks in favor of CBDC holdings at moments of financial stress.

Other research indicates that the increase in competition could result in more attractive terms on transactions accounts and an overall increase in banking system deposits.

Banks play a critical role in credit intermediation and monetary policy transmission, as well as in payments.

Thus, the design of any CBDC would need to include safeguards to protect against disintermediation of banks and to preserve monetary policy transmission more broadly.

While it is critical to consider the ways in which a CBDC could introduce risks relative to the current payments system, it may increase resilience relative to a payments system where private money is prominent.

Protect privacy and safeguard financial integrity

The design of any CBDC would need to both safeguard the privacy of households' payments transactions and prevent and trace illicit activity to maintain the integrity of the financial system, which will require the digital verification of identities.

There are a variety of approaches to safeguarding the privacy of payments transactions while also identifying and preventing illicit activity and verifying digital identities.

Addressing these critical objectives will require working across government agencies to assign roles and responsibilities for preventing illicit transactions and clearly establishing how consumer financial data would be protected.

Increase financial inclusion

Today 5.4 percent of American households lack access to bank accounts and the associated payment options they offer, and a further 18.7 percent were underbanked as of 2017.

The lack of access to bank accounts imposes high burdens on these households, whose financial resilience is often fragile.

At the height of the pandemic, the challenges associated with getting relief payments to hard-to-reach households highlighted that it is important for all households to have transactions accounts.

The Federal Reserve's proposals for strengthening the Community Reinvestment Act emphasize the value of banks providing cost-free, low-balance accounts and other banking services targeted to underbanked and unbanked communities.

And a core goal of FedNow is to provide ubiquitous access to an instant payments system via depository institutions.

CBDC may be one part of a broader solution to the challenge of achieving ubiquitous account access.

Depending on the design, CBDC may have the ability to lower transaction costs and increase access to digital payments. In emergencies, CBDC may

offer a mechanism for the swift and direct transfer of funds, providing rapid relief to those most in need.

A broader solution to financial inclusion would also need to address any perceived barriers to maintaining a transaction account, along with the need to maintain up-to-date records on active accounts to reach a large segment of the population.

To explore these broader issues, the Federal Reserve is undertaking research on financial inclusion. The Federal Reserve Bank of Atlanta is launching a public–private sector collaboration as a Special Committee on Payments Inclusion to ensure that cash-based and vulnerable populations can safely access and benefit from digital payments.

This work is complemented by a new Federal Reserve Bank of Cleveland initiative to explore the prospects for CBDC to increase financial inclusion. The initiative will identify CBDC design features and delivery approaches focused on expanding access to individuals who do not currently use traditional financial services.

Technology Considerations

Multidisciplinary teams at the Federal Reserve are investigating the technological and policy issues associated with digital innovations in payments, clearing, and settlement, including the benefits and risks associated with a potential U.S. CBDC.

For example, the TechLab group at the Federal Reserve Board is performing hands-on research and experimentation on potential future states of money, payments, and digital currencies.

A second group, the Digital Innovations Policy program, is considering a broad range of policy issues associated with the rise of digital payments, including the potential benefits and risks associated with CBDC.

To deepen our research on the technological design of a CBDC, the Federal Reserve Bank of Boston is partnering with Massachusetts Institute of Technology's (MIT) Digital Currency Initiative on Project Hamilton to build and test a hypothetical digital currency platform using leading edge technology design options.

This work aims to research the feasibility of the core processing of a CBDC, while remaining agnostic about a range of policy decisions.
MIT and the Boston Fed plan to release a white paper next quarter that will document the ability to meet goals on throughput of geographically

dispersed transactions with core processing and create an open source license for the code.

Subsequent work will explore how addressing additional requirements, including resiliency, privacy, and anti-money-laundering features, will impact core processing performance and design.

Banking Activities

Research and experimentation are also occurring at supervised banking institutions to explore new technology to enhance their own operations and in response to demands from their clients for services such as custody of digital assets.

While distributed ledger technology may have the potential to improve efficiencies, increase competition, and lower costs, digital assets pose heightened risks such as those related to Bank Secrecy Act/anti-money laundering, cybersecurity, price volatility, privacy, and consumer compliance.

The Federal Reserve is actively monitoring developments in this area, engaging with the industry and other regulators, and working to identify any regulatory, supervisory, and oversight framework gaps.

Given that decisions at one banking agency can have implications for the other agencies, it is important that regulators work together to develop common approaches to ensure that banks are appropriately identifying, monitoring, and managing risks associated with digital assets.

Public Engagement

In light of the growing role of digital private money in the broader migration to digital payments, the potential use of foreign CBDCs in cross-border payments, and the importance of financial inclusion, the Federal Reserve is stepping up its research and public engagement on a digital version of the U.S. dollar.

Members of Congress and executive agencies are similarly exploring this important issue.

As noted above, to help inform these efforts, the Federal Reserve plans to issue a discussion paper to solicit public comment on a range of questions related to payments, financial inclusion, data privacy, and information security, with regard to a CBDC in the U.S. context.

The Federal Reserve remains committed to ensuring a safe, inclusive, efficient, and innovative payments system that works for all Americans.

To read more:
https://www.federalreserve.gov/newsevents/speech/brainard20210524a.htm

Number 11

Can Digital Identity Solutions Benefit from Blockchain Technology?

The knowledge building seminar organised by the EU Agency for Cybersecurity explores the possible applications of blockchain technology in the field of digital identity and online trust.

What is blockchain technology used for?

Blockchain technology was first introduced as a technology for digital currencies, but recently new application areas are emerging. There are proposals to use blockchain technology for electronic voting and secure sharing of medical data. Besides, there is now a booming market of NFTs (non-fungible tokens) underpinned by blockchain technology.

A new field, which could also benefit from blockchain technology is digital identities. Resorting to blockchain-based digital identity frameworks would allow users greater control over their identity data, and at the same time offer a resilient and decentralised system without single points of failure.

Who was the seminar intended for?

Organised by the EU Agency for Cybersecurity (ENISA) in collaboration with the Delft Blockchain Lab of the Dutch Delft University of Technology, the knowledge building seminar held today was intended for national authorities overseeing the trust services market and for authorities involved with digital identity schemes.

This seminar was organised in the context of ENISA's support of the ENISA Article 19 Expert Group, a working group of national authorities supervising the trust service providers in the EU.

What did the seminar focus on?

The seminar introduced the basic concept of blockchain technology, and explored its application in the area of trust services and electronic identification, making a comparison with traditional centralised hierarchical ones in terms of user control and single points of failure. The focus here was on advantages and disadvantages, potential abuse and misuse, potential impact on society and the economy as well as the issue of governance.

The seminar concluded with an overview of several existing initiatives, such as the European Blockchain Services Infrastructure (EBSI), Sovrin, and the TU Delft Trustchain. It also included an overview of real-life scenarios, such as controlling access to a construction site and the confirmation of diplomas by a university.

About ENISA's knowledge building seminars

This seminar is part of a broader series of knowledge building seminars that ENISA organises for national authorities in the EU on new technologies and the cybersecurity opportunities and risks associated with them. Previous seminars for authorities covered topics such as cloud security, internet backbone security and applications of cryptography.

To learn more:
https://www.blockchain-lab.org/#aboutus

https://resilience.enisa.europa.eu/article-19

Number 12

Handwriting Examiners in the Digital Age

As the use of handwriting declines, a forensic discipline finds itself at a crossroads.

NIST
National Institute of Standards and Technology

People are writing more than ever with their keyboards and phones, but handwritten notes have become rare. Even signatures are going out of style. Most credit card purchases no longer require them, and if they do, you can usually just scratch one out with your fingernail. The age-old art of handwriting is in decline.

This marks a profound shift in how we communicate, but for one group of experts it also raises an existential question. Forensic handwriting examiners authenticate handwritten notes and signatures — or reveal them to be fakes — by analyzing distinctive features in our writing. As people write less by hand, will handwriting examination become irrelevant?

A recently updated report from the National Institute of Standards and Technology (NIST) suggests that the answer is no — if the field changes to keep up with the times. But the times are changing in more ways than one, and the decline in handwriting is only one of the challenges that the field will have to reckon with. You may visit:
https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8282r1.pdf

Forensic Handwriting Examination and Human Factors: Improving the Practice Through a Systems Approach

The Expert Working Group for Human Factors in Handwriting Examination

Updated May 2021

NIST National Institute of Standards and Technology

NIJ National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

How the Experts Do It

Emily Will is a board-certified handwriting examiner in private practice in North Carolina. She has examined signatures on countless checks, wills, deeds and trusts.

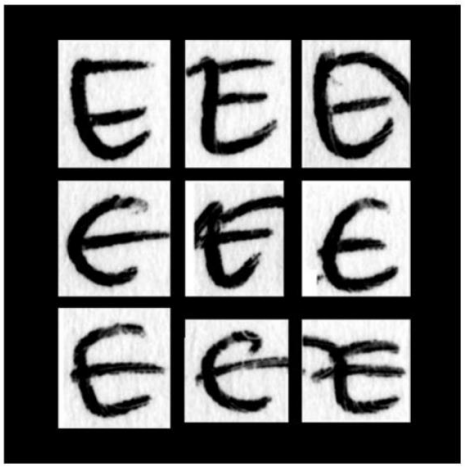
She has inspected medical records to assess whether a doctor's signature may have been added at a later date than indicated, perhaps after a lawsuit was filed.

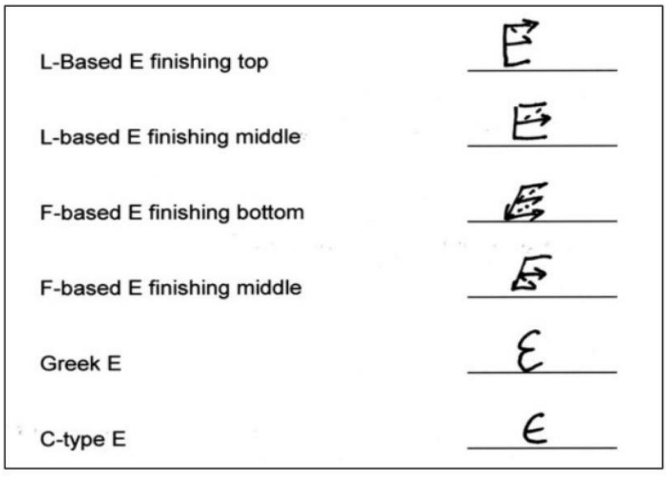
She has also examined longer forms of writing, such as threatening or harassing letters and suicide notes. If the apparent suicide victim didn't write the note, the police might have a homicide on their hands.

To assess whether a piece of handwriting was written by a particular person, examiners need something to compare it against, so they collect writing samples that are known to be from that person. The type of writing has to be the same, whether a signature, cursive writing, or hand printing.

The known samples should be from roughly the same time period as the handwriting in question, because our handwriting evolves over time. And having multiple known samples to compare against is key, as that will allow the examiner to consider the variability in a person's writing style.

"You're not a robot, so every time you sign your name, it'll look different," Will said. "That's what makes handwriting examination so interesting."





Nonprofessionals might think that since most people know how to produce handwriting, pretty much anyone can examine it. They might assume that the expert compares such things as the size, slant and spacing of the letters and the connections between them. Indeed, examiners do that. But they also look beyond those features of writing for subtler signs of how the writing was made.

“Say you want to forge a signature,” Will said. “You may be able to execute a good facsimile. But is the ‘O’ clockwise when it should be counterclockwise? Are there pen lifts where there shouldn’t be? When you sign your name it’s all muscle memory. But forging a signature requires deliberation. The pen slows down. It stops and starts.” Those hesitations show up under a microscope as tiny puddles of ink.

“It’s not so much how the signature looks, but how it was executed that’s important,” Will said.

Here’s what Will carries in her go bag: a jeweler’s loupe, a small optical microscope and a hand-held digital microscope. A flashlight. A paper micrometer, to measure the thickness of paper. A laptop and portable scanner. A camera that hooks up to her microscopes. “And frankly,” she says, “I use my iPhone a lot these days.”

Will’s practice extends to the broader field of “questioned document examination,” which involves scrutinizing an entire document for signs of fraud. At her lab, she has equipment for analyzing papers and inks and viewing them under different types of light.

Some inks that look identical in daylight appear starkly different under infrared. She identifies erasures, alterations and obliterations and reveals indented writing — the impressions left on sheets of paper beneath the written note.

But most of Will’s work involves handwriting and signatures, and there are a lot fewer of them these days. Check-cashing fraud is way down now that paychecks and Social Security checks are direct deposited.

Medical malpractice lawsuits involve fewer signatures since electronic health records have become the norm. Even celebrities have noticed the change. In a 2014 opinion article in The Wall Street Journal, Taylor Swift wrote, “I haven’t been asked for an autograph since the invention of the iPhone with a front-facing camera.”

Enough handwriting still passes under Will’s microscope to keep her in business. But, she says, “If I were a young person starting out today, I might consider cybersecurity.”

According to the NIST, as the use of handwriting declines, a forensic discipline finds itself at a crossroads.
To read more: https://www.nist.gov/news-events/news/2021/06/handwriting-examiners-digital-age

https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8282r1.pdf

Number 13

Slilpp Marketplace Disrupted in International Cyber Operation

Slilpp was a Marketplace for Allegedly Stolen Online Account Login Credentials, Offering Over 80 Million Stolen Credentials for Over 1,400 Victim Providers Worldwide

The Justice Department announced its participation in a multinational operation involving actions in the United States, Germany, the Netherlands, and Romania to disrupt and take down the infrastructure of the online marketplace known as Slilpp.

According to a seizure warrant affidavit that was unsealed today, since 2012, the Slilpp marketplace has been selling stolen login credentials, including usernames and passwords for bank accounts, online payment accounts, mobile phone accounts, retailer accounts, and other online accounts.

According to the affidavit, the Slilpp marketplace allowed vendors to sell, and customers to buy, stolen login credentials by providing the forum and payment mechanism for such transactions; Slilpp buyers subsequently used those login credentials to conduct unauthorized transactions (such as wire transfers) from the related accounts.

To date, over a dozen individuals have been charged or arrested by U.S. law enforcement in connection with the Slilpp marketplace.

According to the affidavit, the FBI, working in coordination with foreign law enforcement partners, identified a series of servers that hosted the Slilpp marketplace infrastructure and its various domain names.

Those servers and domain names were seized pursuant to domestic and international legal process.

“The Slilpp marketplace allegedly caused hundreds of millions of dollars in losses to victims worldwide, including by enabling buyers to steal the identities of American victims,” said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department’s Criminal Division.

“The department will not tolerate an underground economy for stolen identities, and we will continue to collaborate with our law enforcement

partners worldwide to disrupt criminal marketplaces wherever they are located."

"With today's coordinated disruption of the Slilpp marketplace, the FBI and our international partners sent a clear message to those who, as alleged, would steal and traffic in stolen identities: we will not allow cyber threats to go unchecked," said Acting U.S. Attorney Channing D. Phillips of the District of Columbia.

"We applaud the efforts of the FBI and our international partners who contributed to the effort to mitigate this global threat."

"American identities are not for sale," said Assistant Director in Charge Steven M. D'Antuono of the FBI Washington Field Office. "The FBI remains committed to working with our international partners to dismantle global cyber threats."

At the time of the disruption, the affidavit alleges that stolen account login credentials for over 1,400 account providers were available for sale on the Slilpp marketplace.

According to the affidavit, a fraction of the victimized account providers have calculated losses so far; based on limited existing victim reports, the stolen login credentials sold over Slilpp have been used to cause over $200 million in losses in the United States. The full impact of Slilpp is not yet known.

The U.S. Attorney's Office for the District of Columbia, the FBI Washington Field Office, and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) conducted the operation in close cooperation with investigators and prosecutors from several jurisdictions, including Germany's Bundeskriminalamt, the Netherlands' National High Tech Crime Unit, and Romania's Directorate for the Investigation of Organized Crime and Terrorism. The Justice Department's Office of International Affairs also provided significant assistance.

CCIPS Senior Counsel Laura-Kate Bernstein and Assistant U.S. Attorney Demian Ahn of the District of Columbia led the U.S. efforts.

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats.

The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships.

Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) at https://www.ic3.gov

For more information on ransomware prevention, visit: https://www.ic3.gov/media/2016/160915.aspx

Number 14

Using a mineral 'sponge' to catch uranium

Remediation technology reduces uranium levels ten-thousandfold at legacy site in Colorado

Sandia National Laboratories

A team of researchers from Sandia, Lawrence Berkeley and Pacific Northwest national laboratories tested a "sponge-like" mineral that can "soak up" uranium at a former uranium mill near Rifle, Colorado. The researchers found that the mineral, calcium apatite, soaks up and binds uranium from the groundwater, reducing it by more than ten-thousandfold.

"The apatite technology has successfully reduced the concentration of uranium, vanadium and molybdenum in the groundwater at the Rifle site," said Mark Rigali, the Sandia geochemist leading the project. "Moreover, the levels of uranium have remained below the Department of Energy's target concentration for more than three years."

The contaminated mill site near Rifle is about 180 miles west of Denver. Since 2002, the DOE's Office of Legacy Management has used the site to test a variety of different uranium-remediation technologies.

All forms of uranium are radioactive, and it is toxic when ingested. Molybdenum and vanadium, on the other hand, are beneficial at very, very low levels, but are toxic at high concentrations.

While the Rifle test site is remote, there are thousands of sites around the world that are similarly contaminated with radioactive elements and heavy metals that threaten groundwater, surface water and food supplies.

Calcium apatite is a mineral commonly used in fertilizer and is also a major component of bones and teeth. The researchers formed a "sponge" in the ground by injecting two inexpensive and nontoxic chemicals, calcium citrate and sodium phosphate, into a well especially designed for injecting solutions underground at the former uranium mill.

Once in the ground, helpful soil bacteria ate the calcium citrate and excreted calcium in a form that allows it to rapidly react with the sodium phosphate to form calcium apatite, which coated sand and soil particles underground, forming the sponge. The apatite sponge captures contaminants, such as uranium, as it forms on the soil particles around the injection well, and afterward as the groundwater flows through the rough

sponge. Once formed, the apatite is incredibly stable, and can hold onto captured contaminants for millennia.

Soaking up half of the periodic table

"The apatite-based approach for uranium remediation has been by far the most effective and long-lasting without any significant negative side effects," said Ken Williams, the environmental remediation and water resources program lead at Lawrence Berkeley.

"It's basically been a win-win-win situation. The first win is the ease of operation with only one injection needed. The next win is uranium being removed to incredibly low levels. The third win is the lack of significant deleterious consequences."

Williams has been testing different uranium remediation techniques at the Rifle site for more than a decade, since he was a graduate student. As a student, he was involved in a project at the site where they fed soil bacteria vinegar to remediate uranium that had some unfortunate side effects.

The apatite remediation technology was invented by former Sandia chemical engineer Robert Moore. It has been used at the DOE's Hanford Site in southeastern Washington state to protect the Columbia River from strontium-90, another radioactive isotope.

Geologists know that apatite can capture elements from more than half of the periodic table of elements, Rigali said, but the team conducted initial laboratory-based tests to confirm apatite would bind dissolved uranium. These tests were conducted by Jim Szecsody, a geochemist at the Pacific Northwest National Laboratory.

In addition to reducing the amount of uranium in groundwater more than ten-thousandfold, Williams and Rigali found that the apatite reduced the amount of vanadium by more than a hundredfold.

Vanadium is another contaminant left over from uranium milling, along with molybdenum, selenium and arsenic. Auspiciously, the apatite-based remediation technology captures these other toxic chemicals too, they said.

The future of apatite remediation

Computer modeling by Sandia geoscientist Pat Brady suggests that the uranium will remain contained within the apatite mineral for tens of thousands of years — possibly longer than the mill site flood plain will remain in its current location adjacent to the Colorado River, Rigali said.

Williams will continue measuring the amount of contaminants in the groundwater downstream of the apatite sponge every month until the sponge is "full." This will allow the research team to learn how much uranium and other contaminants the apatite can hold, and when the sponge would need to be "refreshed" with more apatite, he said.

The apatite technology is being considered for use at several other contaminated locations, both federally managed and privately owned, said Rigali. Also increasing the potential applicability of apatite remediation is the fact that it can be "tuned" to capture different contaminants of concern including lead and arsenic.

"The apatite family of minerals is very large," he added. "And they all have varying abilities to capture and store contaminants. You can literally tune the structure of apatite to go after specific contaminants of concern."

Copper apatite, for example, is a great sponge for arsenic.

"This has been one of the most rewarding projects that I've gotten to work on at Sandia," Rigali said. "It's great to have these types of opportunities because you feel like you're doing something that is solving a problem and making a difference. I know this technology could be used at dozens of sites for uranium remediation."

The test in Rifle was funded by DOE's Office of Legacy Management, while the development of original apatite remediation technology was supported by Sandia's Laboratory Directed Research and Development program.

To read more: https://share-ng.sandia.gov/news/resources/news_releases/uranium_remediation/

Number 15

Enabling Human Control of Autonomous Partners

DARPA program to help humans maintain situational awareness when AI behaves in unexpected ways

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

A major benefit of increasingly advanced automation and artificial intelligence technology is decreased workload and greater safety for humans – whether it's driving a vehicle, piloting an airplane, or patrolling a dangerous street in a deployed location with the aid of autonomous ground and airborne squad mates.

But when there's a technology glitch and machines don't function as designed, human partners in human-machine teams may quickly become overwhelmed trying to understand their environment at a critical moment – especially when they've become accustomed to and reliant on the machine's capabilities.

Without situational awareness of the system and environment, the human team member may be unable to adapt, reducing safety and threatening mission success.

This reality played out in crashes of modern jetliners in recent years killing hundreds, because advanced automated systems failed in flight and pilots weren't able to assess the situation and respond appropriately in time.

Such examples underscore the need to design human-machine interfaces (HMIs) that allow humans to maintain situational awareness of highly automated and autonomous systems so that they can adapt in the face of unforeseen circumstances.

DARPA today announced its Enhancing Design for Graceful Extensibility (EDGE) program, which aims to create a suite of HMI design tools to be integrated into systems design processes.

By prioritizing and orienting these tools towards quantifying, supporting, and testing situational awareness – rather than on cognitive load at the expense of situational awareness – EDGE will help create HMI systems that allow operators to not just monitor autonomous systems but also adapt their use to meet the needs of unanticipated situations.

"As highly-automated machines and AI-enabled systems have become more and more complicated, the trend in HMI development has been to reduce cognitive workload on humans as much as possible.

Unfortunately, the easiest way to do this is by limiting information transfer," said Bart Russell, EDGE program manager in DARPA's Defense Sciences Office.

"Reducing workload is important, because an overloaded person cannot make good decisions. But limiting information erodes situational awareness, making it difficult for human operators to know how to adapt when the AI doesn't function as designed. Current AI systems tend to be brittle – they don't handle unexpected situations well – and warfare is defined by the unexpected."

The EDGE design tools will focus on supporting the ability of operators of autonomous systems, who are not necessarily data scientists or AI experts, to understand enough about the abstract functioning of a system that they can adapt with it when they encounter off-nominal situations.

Designers will be able to leverage EDGE design tools to create HMIs that help operators understand an AI system's processes, or how it works; the system's status against its performance envelope (i.e., if it's in its "comfort zone," or near the edges of its speed, range, etc.); and the environmental context, which is often where the most unanticipated elements come in.

"We need HMIs that do a better job of exchanging information between the system and the human," Russell said.

"There's a lot of work right now focused on designing machines to understand human intentions, called AI Theory of Mind. I'm interested in helping humans better understand the complex systems they're teamed with. EDGE is specifically focused on the Observe, Orient, Decide and less on the Act in the OODA loop.

It's not about how fast you press a button, or the ergonomics of your cockpit, it's about how well you perceive the information that's coming to you and does that help you develop sufficient understanding of systems processes, status against the machine's performance envelope, and the context in which it's operating to still complete a mission despite off-nominal conditions."

The suite of EDGE HMI design tools will include models that quantify situational awareness demands to enable detailed co-design between software engineers and HMI designers; composable design methods to speed and mature design implementation; and an HMI breadboard for realistic test and verification early in the design process.

A webinar Proposers Day for interested proposers is scheduled for June 1, 2021. More information and details about registration are available here: https://go.usa.gov/xHSKg

A Broad Agency Announcement (BAA) solicitation is expected be available on beta.SAM.gov in the coming weeks.

Number 16

Targets for Addressing the Four Challenges of Cross-Border Payments: Consultative document

FSB FINANCIAL STABILITY BOARD

The G20 has made enhancing cross-border payments a priority. Faster, cheaper, more transparent and more inclusive cross-border payment services, including remittances, which would have widespread benefits for citizens and economies worldwide, support economic growth, international trade, global development and financial inclusion.

A roadmap was developed by the FSB, in coordination with the Committee on Payments and Market Infrastructures (CPMI) and other relevant international organisations and standard-setting bodies to address these challenges.

Financial innovation is creating opportunities to make payments more efficient. Innovation in technology and business models in payments has put the focus on further enhancements in payments systems.

New technologies have the potential to facilitate fast, low cost, transparent and scalable payments for a broad range of users through the banking system.

Public authorities have an important role to play, working with the private sector to leverage opportunities and address challenges in both existing and new arrangements supporting cross-border payments.

The G20 Leaders endorsed the Roadmap in the form of 19 Building Blocks and related Actions for Enhancing Cross-border Payments1 at their November 2020 Summit.

A foundational step in the Roadmap consists of setting quantitative targets at the global level for addressing the challenges of cost, speed, transparency and access faced by cross-border payments, which will play an important role in defining the ambition of the work and creating accountability.

They are intended to provide a common vision for the improvements that are being sought through the collaborative work of the private and public sectors.

These targets are being set in an inclusive manner, including through this public consultation.

This consultation document:

(i) describes the principles, and key design features underpinning, the targets and target metrics;

(ii) proposes three market segments for which targets be set across the four challenges;

(iii) considers factors in setting the targets; and

(iv) proposes a set of targets that are high-level, simple, small in number and focused on end-users.

The FSB is inviting comments on this consultation document and the questions set out below.

Responses should be sent to fsb@fsb.org by Friday 16 July 2021. Responses will be published on the FSB's website unless respondents expressly request otherwise.

1. What are your comments on the key design features applied in designing the targets (section 1)? Are there any design features that you consider are missing?

2. Do you agree with the market segments as described? Are they sufficiently clear? Do they reflect the diversity of cross-border payments markets, while providing a high-level common vision for addressing the four roadmap challenges?

3. Do you have any comments on the target metrics proposed?

4. Do you agree with the proposal in the definition of the market segments to separate remittance payments from other types of cross-border person-to-person (P2P) payments because of the greater challenges that remittances in some country corridors face? If so, can you suggest data sources that can distinguish between the two types?

5. Are the proposed numerical targets suitable? Are they objective and measurable, so that accountability can be ensured by monitoring progress against them over time?

6. What are your views on the cost target for the retail market segment? Does it reflect an appropriate level of ambition to improve on current costs while taking into consideration the variety of payment types within the segment? Should reference transaction amounts be set for the target (in the same way as $200 has been set for the current UN Sustainable

Development Group targets for remittances) and, if so, what amount would you suggest?

7. What are your views on the speed targets across the three market segments? Are the proposed targets striking the right balance between the ambition of having a large majority of users seeing significant improvements, the recognition that different types of user will have different speed requirements, and the extent of improvements that can be envisaged from the actions planned under the roadmap?

8. Are the dates proposed for achieving the targets (i.e. end-2027 for most targets) appropriately ambitious yet achievable given the overall time horizon for the Actions planned under the Roadmap? Would an alternative and more ambitious target date of end-2026 be feasible?

9. What data sources exist (or would need to be developed) to monitor the progress against the targets over time and to develop and set key performance indicators? Do you have relevant data that you would be willing to share for this purpose either now or during the future monitoring?

10. Do you have further suggestions or questions about the detailed definition and measurement of the targets and their implementation? Which types of averages can be constructed to help to measure progress?

11. Do you have any suggestions for more qualitative targets that could express ambitions for the benefits to be achieved by innovation that would be in addition to the proposed quantitative targets for the payments market as a whole?

Number 17

PUBLIC CONSULTATION ON THE DRAFT CANDIDATE EUCC SCHEME

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act (hereinafter referred to as CSA as indicated in the glossary), ENISA has set up an Ad Hoc Working Group (AHWG) to support the preparation of a candidate EU cybersecurity certification scheme to serve as a successor to the existing ICT products certification schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement).

As stipulated by Article 49.3 of the Cybersecurity Act, "When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process."

ENISA has therefore organised a public consultation from July, 2 to July, 31 2020. This report presents the outcome of this consultation.

1. The contributors

- Important fact is that the contributors represent a broad spectrum of actors involved in ICT products certification ensuring that input is received from all different angles.

- Manufacturers/developers represented 37 % and the conformity assessment bodies (certification bodies and ITSEFs/testing laboratories) 24 % of the total number of respondents.

- 77% of the participants indicated EU/EEA as their country of establishment and 20% as non-EU/EEA. Further to that, 32% indicated that their country of establishment participates in the SOG-IS MRA and 33% that their country of establishment is a member of the Common Criteria Recognition Arrangement (CCRA).

2. The intend to use the draft candidate EUCC scheme: 33% of the respondents indicated to envisage having ICT products certified under the EUCC scheme (manufacturers/producers/developers and trade organisations) and 25% indicated to have their products certified; generating a demand side that is more or less in balance with the activity of contributors.

3. The transition from current scheme (SOG-IS or national schemes) to EUCC scheme; 64% of the survey participants agreed that the choices made in the EUCC scheme will have a positive impact on the transition from current activities. 32% were neutral and only 4% were of the opinion that the impact will not be positive. The need of guidance to support transition was noted.

To read more: https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme

Number 18

How AI Could Alert Firefighters of Imminent Danger

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Firefighting is a race against time. Exactly how much time? For firefighters, that part is often unclear. Building fires can turn from bad to deadly in an instant, and the warning signs are frequently difficult to discern amid the mayhem of an inferno.

Seeking to remove this major blind spot, researchers at the National Institute of Standards and Technology (NIST) have developed P-Flash, or the Prediction Model for Flashover.

The artificial-intelligence-powered tool was designed to predict and warn of a deadly phenomenon in burning buildings known as flashover, when flammable materials in a room ignite almost simultaneously, producing a blaze only limited in size by available oxygen.

The tool's predictions are based on temperature data from a building's heat detectors, and, remarkably, it is designed to operate even after heat detectors begin to fail, making do with the remaining devices.

The team tested P-Flash's ability to predict imminent flashovers in over a thousand simulated fires and more than a dozen real-world fires.

Research, just published in the *Proceedings of the AAAI Conference on Artificial Intelligence*, suggests the model shows promise in anticipating simulated flashovers and shows how real-world data helped the researchers identify an unmodeled physical phenomenon that if addressed could improve the tool's forecasting in actual fires. You may visit: https://ojs.aaai.org/index.php/AAAI/article/view/17736

With further development, P-Flash could enhance the ability of firefighters to hone their real-time tactics, helping them save building occupants as well as themselves.

Flashovers are so dangerous in part because it's challenging to see them coming. There are indicators to watch, such as increasingly intense heat or flames rolling across the ceiling. However, these signs can be easy to miss in many situations, such as when a firefighter is searching for trapped victims with heavy equipment in tow and smoke obscuring the view. And from the outside, as firefighters approach a scene, the conditions inside are even less clear.

“I don't think the fire service has many tools technology-wise that predict flashover at the scene,” said NIST researcher Christopher Brown, who also serves as a volunteer firefighter. “Our biggest tool is just observation, and that can be very deceiving. Things look one way on the outside, and when you get inside, it could be quite different.”

Computer models that predict flashover based on temperature are not entirely new, but until now, they have relied on constant streams of temperature data, which are obtainable in a lab but not guaranteed during a real fire.

Heat detectors, which are commonly installed in commercial buildings and can be used in homes alongside smoke alarms, are for the most part expected to operate only at temperatures up to 150 degrees Celsius (302 degrees Fahrenheit), far below the 600 degrees Celsius (1,100 degrees Fahrenheit) at which a flashover typically begins to occur. To bridge the gap created by lost data, NIST researchers applied a form of artificial intelligence known as machine learning.

“You lose the data, but you’ve got the trend up to where the heat detector fails, and you've got other detectors. With machine learning, you could use that data as a jumping-off point to extrapolate whether flashover is going to occur or already occurred,” said NIST chemical engineer Thomas Cleary, a co-author of the study.

Machine-learning algorithms uncover patterns in large datasets and build models based on their findings. These models can be useful for predicting certain outcomes, such as how much time will pass before a room is engulfed in flames.

To build P-Flash, the authors fed their algorithm temperature data from heat detectors in a burning three-bedroom, one-story ranch-style home — the most common type of home in a majority of states. This building was of a digital rather than brick-and-mortar variety, however.

Because machine learning algorithms require great quantities of data, and conducting hundreds of large-scale fire tests was not feasible, the team burned this virtual building repeatedly using NIST’s Consolidated Model of Fire and Smoke Transport, or CFAST, a fire modeling program validated by real fire experiments, Cleary said.

The authors ran 5,041 simulations, with slight but critical variations between each. Different pieces of furniture throughout the house ignited with every run. Windows and bedroom doors were randomly configured to be open or closed. And the front door, which always started closed, opened up at some point to represent evacuating occupants. Heat detectors placed

in the rooms produced temperature data until they were inevitably disabled by the intense heat.

To learn about P-Flash's ability to predict flashovers after heat detectors fail, the researchers split up the simulated temperature recordings, allowing the algorithm to learn from a set of 4,033 while keeping the others out of sight. Once P-Flash had wrapped up a study session, the team quizzed it on a set of 504 simulations, fine-tuned the model based on its grade and repeated the process. After attaining a desired performance, the researchers put P-Flash up against a final set of 504.

The researchers found that the model correctly predicted flashovers one minute beforehand for about 86% of the simulated fires. Another important aspect of P-Flash's performance was that even when it missed the mark, it mostly did so by producing false positives — predictions that an event would happen earlier than it actually did — which is better than the alternative of giving firefighters a false sense of security.

"You always want to be on the safe side. Even though we can accept a small number of false positives, our model development places a premium on minimizing or, better yet, eliminating false negatives," said NIST mechanical engineer and corresponding author Wai Cheong Tam.

The initial tests were promising, but the team had not grown complacent.

"One very important question remained, which was, can our model be trusted if we only train our model using synthetic data?" Tam said.

Luckily, the researchers came across an opportunity to find answers in real-world data produced by Underwriters Laboratories (UL) in a recent study funded by the National Institute of Justice. UL had carried out 13 experiments in a ranch-style home matching the one P-Flash was trained on, and as with the simulations, ignition sources and ventilation varied between each fire.

The NIST team trained P-Flash on thousands of simulations as before, but this time they swapped in temperature data from the UL experiments as the final test. And this time, the predictions played out a bit differently.

P-Flash, attempting to predict flashovers up to 30 seconds beforehand, performed well when fires started in open areas such the kitchen or living room. But when fires started in a bedroom, behind closed doors, the model could almost never tell when flashover was imminent.

The team identified a phenomenon called the enclosure effect as a possible explanation for the sharp drop-off in accuracy. When fires burn in small,

closed-off spaces, heat has little ability to dissipate, so temperature rises quickly. However, many of the experiments that form the basis of P-Flash's training material were carried out in open lab spaces, Tam said. As such, temperatures from the UL experiments shot up nearly twice as fast as the synthetic data.

Despite revealing a weak spot in the tool, the team finds the results to be encouraging and a step in the right direction. The researchers' next task is to zero in on the enclosure effect and represent it in simulations. To do that they plan on performing more full-scale experiments themselves.

When its weak spots are patched and its predictions sharpened, the researchers envision that their system could be embedded in hand-held devices able to communicate with detectors in a building through the cloud, Tam said.

Firefighters would not only be able to tell their colleagues when it's time to escape, but they would be able to know danger spots in the building before they arrive and adjust their tactics to maximize their chances of saving lives.

Number 19

FBI Targets Encrypted Platforms Used by Criminal Groups

Global Partners Announce Results of Innovative Operation Trojan Shield

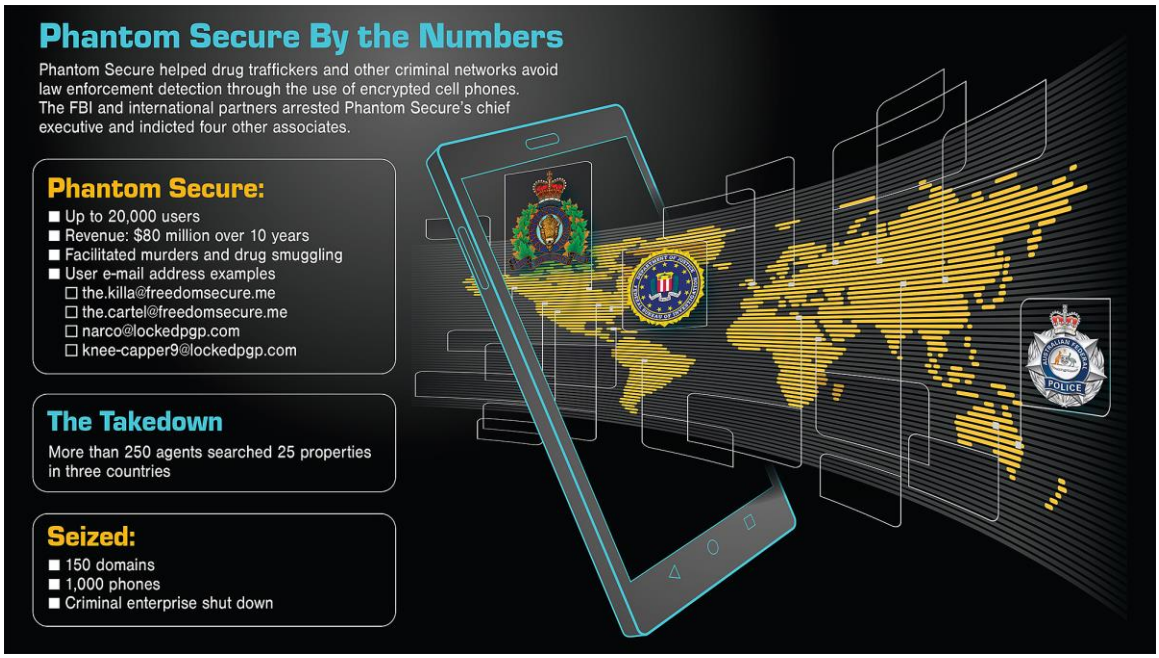
Criminal organizations that rely on hardened, stripped-down devices to send encrypted messages may learn this week they have been using a platform operated by the very investigators they are trying to thwart.

In an innovative effort, the FBI, with the help of the Australian Federal Police, launched their own encrypted communications platform and supplied more than 12,000 devices to hundreds of criminal organizations that operate around the globe.

The FBI, along with the Drug Enforcement Administration, Australian Federal Police, Europol, and law enforcement partners in more than a dozen countries, are announcing the results of that covert effort, known as Operation Trojan Shield.

In recent days and weeks, authorities have carried out hundreds of arrests in Australia and across Europe as a result of intelligence gathered during the operation. Law enforcement has also been able to mitigate direct threat-to-life situations.

The FBI's San Diego Field Office was the hub for the more than 100 agents and analysts and 80 linguists who were pooled together for the operation that began with the takedown of the encrypted phone provider Phantom Secure.



In 2018, the FBI and the U.S. Attorney's Office for the Southern District of California pursued charges against the company's executives for facilitating the transnational importation and distribution of narcotics by providing encrypted devices to criminals.

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular 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 interpretative;

- 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.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.