July 2020, cyber risk and compliance in Switzerland

Top cyber risk and compliance related local news stories and world events

Dear readers,

On Thursday 9 July 2020, Switzerland and the USA met for the first bilateral cyber dialogue. Together, the two countries are committed to an open and secure digital space.

In addition to the FDFA, the FDF with the Federal Delegate for Cyber Security, the DDPS, OFCOM and Fedpol are involved in the digital exchange. According to the Federal Department of Defence, Civil Protection and Sport (DDPS), in light of the ongoing COVID-19 pandemic, the SwissCovid tracing app attracted particular interest.

In keeping with the topic and taking into account the current COVID 19 regulations, some of the exchange took place digitally - the US Embassy in Bern organized a video exchange with Washington.

For Switzerland, the US is a key dialogue partner on cyber-related issues. The two countries are working together to create a free, open and secure digital space.

Digitalisation knows no national or departmental boundaries

Neither COVID-19 nor digitalisation know national borders and has long since ceased to be able to be processed within the department, as the establishment of the National Centre for Cyber Security NCSC underlines.

Inter-departmental and international cooperation is central to making Switzerland's cyberspace more secure, preserving the openness of the Internet and exploiting the economic potential for Switzerland. The first digital and cyber dialogue between Switzerland and the US accordingly drew a diverse mix of participants.

The Federal Department of Foreign Affairs FDFA is responsible for implementation within the framework of the National Strategy for the

Protection of Switzerland against Cyber Risks (NCS).

In addition, the Swiss delegation was represented by the Federal Delegate for Cyber Security and representatives of the Federal Department of Defence, Civil Protection and Sports (DDPS), the Federal Office of Communications (OFCOM) and the Federal Office of Police (Fedpol).

On the US side, representatives of the National Security Council, the Ministry of Homeland Security, the Ministry of Defence, the Ministry of Justice, the FBI and the Ministry of Foreign Affairs took part in the bilateral dialogue.

Swiss tracing app as an exemplary project

The diverse field of participants is a reflection of the multifaceted range of topics addressed at the cyber dialogue. Digitalisation is not an independent phenomenon but rather a development that impacts all areas of daily life and the way people interact with each other.

In addition to mobile communications security and better protection of communications infrastructure, the delegations also focused on law enforcement cooperation in the area of cybercrime and cybersecurity.

The technological implementation of the Swiss tracing app SwissCovid also met with great interest. The SwissCovid app for mobile phones is a digital application that complements the contact tracing already being carried out by the cantons. The aim is to help contain the coronavirus and prevent it from spreading uncontrollably.

While the main focus of discussions was on COVID-19-related issues and the possibilities offered by digitalisation in stemming the spread of the pandemic, Switzerland and the US plan to use the cyber dialogue as a long-term platform for exchanges.

Bilateral cyber dialogues are an integral part of Switzerland's National Strategy for Protection against Cyber Risks, which was adopted by the Federal Council in 2018.

Further information

Switzerland and the US join forces for an open and secure digital space
Address for further inquiries
FDFA Communication
Federal Palace West Wing
CH-3003 Bern, Switzerland
Tel.: +41 58 462 31 53

E-mail: kommunikation@eda.admin.ch
Twitter: @SwissMFA

On Wednesday 8 July 2020, the Swiss Federal Office of Civil Aviation FOCA and the US Federal Aviation Administration FAA have signed a declaration of intent to strengthen collaboration in the area of Unmanned Aircraft Systems (UAS).

Collaboration will focus on research and development and on the exchange of ideas, personnel and information to better respond to present and future challenges related to UAS operations and their safe integration into airspace.

The declaration establishes a framework under which the FAA and the FOCA will cooperate in advancing domestic and international UAS safety standards and their harmonisation.

The two civil aviation authorities will collaborate on initiatives and projects of mutual interest and benefit in relation to UAS operations.

Even though the two countries are rather different, the challenges the USA and Switzerland are facing in the fastest growing segment of civil aviation are very similar.

Both countries are highly innovative, with stakeholders demanding new ways to access airspace in order to perform unprecedented operations. Exchanging viewpoints on and approaches to mutual challenges will be of real benefit to both sides.

The cooperation will allow valuable steps forward such as implementing remote identification, the ability of a UAS in flight to provide identification information that can be received by other parties. This capability will help to increase the effectiveness of airspace control, oversight and law enforcement, therefore improving the safety of UAS operations.

With its Innovation and Digitalisation Unit, the FOCA leads Switzerland's efforts on UAS and is the designated authority in charge of facilitating the integration of drones into Swiss airspace.

The FAA's UAS Integration Office coordinates across the FAA for the development of drone-centric operating concepts, policies, requirements, criteria, and procedures for both existing and new system evaluations.

In *traditional identity payments fraud*, a fraudster pretends to be another real person and uses his or her credit. The victim is directly affected financially, so this type of fraud is typically detected and reported relatively quickly.

In *synthetic identity payments fraud*, a fraudster creates a new identity to commit fraud in one of several ways. Methods include *identity fabrication* (a completely fictitious identity without any real PII), *identity manipulation* (using slightly modified real PII to create a new identity), or *identity compilation* (a combination of real and fake PII, such as a false driver's license, to form a new identity).

The Federal Reserve has published a new paper with title *Mitigating Synthetic Identity Fraud in the U.S. Payment System*. It is highly recommended to read it.

Synthetic identity accounts behave more like normal customers – building credit over a period of time – than *conventional* identity fraudsters, who must rapidly cash in before the victim notices and reports the theft.

Organizations that have the most success are those that look beyond basic PII elements (such as name, SSN, date of birth and address) and use additional data sources to gain reasonable assurance of the applicant's identity.

There are benefits to use robust *link analysis processes* – processes that look across various banking instruments (such as checking accounts, lending accounts and other financial instruments) to identify relationships or common characteristics of synthetic identities.

Examples include screening for multiple account applications originating from the same IP address or device and detecting potential fraud networks by linking identities that appear as authorized users on multiple accounts.

Link analysis also can be conducted across multiple banks from service providers that have multiple financial institutions as clients. We see increased use of *artificial intelligence (AI) and machine learning* – the use of technology to perform tasks that normally require human intelligence – to detect and mitigate synthetic identity fraud.

While the technological capabilities of these models are developing rapidly, the industry must collect more and better data in order for these AI and machine learning solutions to improve their sensitivity and more successfully mitigate fraud.

There is no single solution to completely mitigate synthetic identity payments fraud. Factors such as the regulatory environment, technological advancement and shifts in fraudster tactics create a constantly evolving payments fraud landscape.

Information sharing within – and between – organizations can help the industry draw connections between datasets to better identify potential synthetic identities.

Read more at number 8 below.

Marcus Aurelius believed that loss is nothing else but *change,* and change is nature's delight.

In financial stress testing, we are not filled with delight when we make assumptions about *change*. For example, *climate change* stress tests are very challenging, as we need *realistic assumptions* approved by the board and the supervisors.

I have just studied a very interesting paper, the *"Second Discussion Paper on Methodological principles of insurance stress testing"* from the European Insurance and Occupational Pensions Authority (EIOPA), the European Union's regulatory institution. In 40 pages, it covers:

- Climate Change Stress Tests,
- Climate Change risk and transmission channels,
- Elements of a Climate Change Stress Test exercise,
- Objective of Climate Change stress test,
- Scenario design, scenario narratives, and much more.

A problem is that Climate Change Stress Tests have to deal with the uncertainty, nature and time horizon of any climate change scenario, as the impact of climate change can be structural, irreversible, and non-linear, but the impacts may only manifest themselves beyond the typical short-term time horizon of the stress test.

The structural, non-linear and irreversible impact of climate change in the long run has also been referred to as the *Tragedy of the Horizons* (Mark Carney, Breaking the Tragedy of the Horizon – Climate Change and Financial Stability, 2015). The physical impacts of climate change will be felt over a long-term horizon, but the time horizon in which financial, economic and political players plan and act is much shorter.

These are some key assumptions and uncertainties surrounding climate change scenarios:

Key assumptions and uncertainties	Macroeconomic physical	Macroeconomic transition	Financial stability physical	Financial stability transition
Future climate policy	Determine the extent of warming	Determine the speed and timing of transition	Determine the extent of warming	Determines the speed and timing of transition, and also may have diffuse impacts on different sectors (for example, a widespread carbon tax)
Rate of progress in carbon-neutral technology	Determine the extent of warming	Could reduce costs or actually result in an increase in GDP	Determine the extent of warming	Key technologies (for example carbon capture and storage) will be particularly important for some sectors, and result in less disruption to existing business models
Feedback loops within the model	Key assumptions (e.g. about GDP) are often taken as external in the model	Economy may be affected indirectly through second-round effects	Financial stability risks could be exacerbated by second-round impacts	Financial stability risks could be exacerbated by second-round impacts
Level of adaption and adaptive capacity	Higher level of adaption could lower the long-term physical damages but might entail higher adaption costs in the short-term	More diversified economies, adaptive firms, and resilient financial systems could reduce transition costs	Higher level of adaption could lower the long-term physical damages but might entail higher adaption costs in the short-term	More diversified economies, adaptive firms, and resilient financial systems could reduce transition costs
Non-linear impacts / uncertainties in climate modelling	Damages may be higher than expected, either through direct losses to particular sectors or through general macroeconomic channels	Higher-than-expected damages could impacts the speed and timing of climate policy	Damages may be higher than expected, either through direct losses to particular sectors or through general macroeconomic channels	Higher-than-expected damages could impacts the speed and timing of climate policy

Read more at Number 5 below.

This is interesting. Face coverings made from layered cotton fabric is likely to slow the spread of COVID-19 better than synthetics.

Researchers have completed a new study of how well a variety of natural and synthetic fabrics filter particles of a similar size to the virus that causes COVID-19.

Of the 32 cloth materials tested, three of the five most effective at blocking particles were 100% cotton and had a visible raised fiber or nap, such as found on flannels.

Four of the five lowest performers were synthetic materials.

The testing also showed that multiple fabric layers could improve cotton's effectiveness even further.

None of the materials came close to the efficiency of N95 masks.

Although the sample size was relatively small, the researchers noticed that

tighter woven fabrics generally filtered better than knits and loosely woven fabrics.

The 100% cotton fabrics with many raised fibers also appeared to filter better than cotton fabrics that lacked this feature.

The raised fibers often form web-like structures similar to those in medical grade masks.

Three researchers from the National Institute of Standards and Technology (NIST) — Christopher Zangmeister, James Radney and Jamie Weaver — teamed up with Edward Vicenzi of the Smithsonian Institution's Museum Conservation Institute to evaluate materials and determine both their ability to filter particles and their breathability.

Their results appear in the journal ACS Nano (at https://pubs.acs.org/doi/10.1021/acsnano.0c05025).

The U.S. Centers for Disease Control and Prevention (CDC) recommends that people wear cloth face coverings in public settings (you may visit https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/diy-cloth-face-coverings.html where social distancing is difficult, primarily to prevent a person who doesn't know they're infected from spreading the virus.

The virus that causes COVID-19 is primarily spread through respiratory droplets that are expelled when a person sneezes, coughs or even talks. However, some research also suggests the virus can spread through much smaller aerosols — smaller than 1/100th the width of a human hair — that are also expelled, and which can linger in air much longer than droplets.

"It turns out that off-the-shelf materials provide some protection from aerosols if you use multiple layers of cloth and a face covering fits snugly," said Zangmeister. "But none are as good as an N95 mask."

The project measured a common way to determine how well a material captures particles, called filtration efficiency. Zangmeister and Radney, who are experts at measuring aerosols, set up a relatively simple experiment that relied on extremely sensitive equipment for sizing and counting aerosol particles.

The experiments used fabric samples, or swatches, rather than complete masks. "Basically, we take a swatch of material and flow a stream of particles of a known size at it," said Zangmeister. "We count the number of particles in the air before and after it's passed through the fabric. That tells us how effective the material is at capturing particles."

Instead of real (and dangerous) samples of the SARS-CoV-2 virus, the team used table salt, or sodium chloride (NaCl), the recommended stand-in for virus particles by the CDC's National Institute for Occupational Safety and Health (NIOSH), which establishes testing standards for N95 and other masks. The airflow rates used in the experiments were also from NIOSH test recommendations.

The researchers tested each material against particles ranging from 50 to 825 nanometers (nm) to chart its relative performance.

Meanwhile, Weaver, a materials chemist with a background in textiles, and Vicenzi, an expert in microscopy, studied each piece of fabric to determine its yarn count, weave and mass in the hopes of establishing a relationship between these characteristics and the fabric's ability to filter particles.

The SARS-CoV-2 virus particles are about 110 nm in diameter. N95 masks are rigorously tested to ensure they block at least 95% of particles in this size range.

A HEPA (high-efficiency particulate air) filter such as those you might find in an air purifier blocks 99.97% of particles that are about 300 nm in size, and an even higher percentage of smaller particles.
Of the fabrics tested in the NIST study, the best-performing single fabric layer blocked 20% of particles in the size range of the virus.

While Zangmeister and Radney conducted the aerosol experiments at NIST's Gaithersburg, Maryland, campus, Weaver and Vicenzi were able to conduct their imaging work at home where they have been working since mid-March.

"We intentionally used inexpensive digital microscopes and freeware to do our part of the research from home," said Weaver. "One motivation for this was to develop imaging methods that would allow citizen scientists to better study fabrics for relatively little startup costs."

In addition to the fabrics, the team looked at materials including a HEPA filter, N95 mask, a surgical mask and even coffee filters, which have been suggested for use in homemade face coverings, for comparison. The team also tested combinations of fabrics (a cotton and a synthetic layer), which did not show increased effectiveness.

By combining imaging and aerosol measurements, the team found that some fabrics that filter the most particles are also the hardest to breathe through, and some even fail to meet health and safety recommendations for breathability.

"The texture turned out to be one of the more useful parameters to look at because we found that most of the cotton fabrics with raised threads tended to filter best," said Weaver. "Our findings suggest that a fabric's ability to filter particles is based on a complex interplay between material type, fiber and weave structures, and yarn count."

This research adds to the body of knowledge on fabrics and filtration that dates back to the 1918 flu pandemic that killed an estimated 20 to 50 million people worldwide and prompted the first research into fabric masks and their potential to protect against viruses. It also supports subsequent research suggesting that cloth filters would not be suitable for health-care settings.

But despite decades of research on the topic, the team found that a lack of standard test methods and the broad range of materials tested made it difficult to directly compare the results of previously published studies. They hope their work will provide a method for rapidly screening materials.

"We didn't know the answer when we started this project," said Zangmeister. "But the bottom line is that none of these fabrics are as good as an N95 mask. Still, cloth face coverings can help slow the spread of coronavirus. We hope this research will help manufacturers and DIYers determine the best fabrics for the job and serve as a basis for additional research."

The team plans to begin another round of testing on a new set of materials in the near future. Weaver and Vicenzi have upgraded their imaging hardware and plan to employ more sophisticated textural analysis for the next round of fabrics.

Adagia is the title of the collection of ancient Greek and Latin proverbs compiled by Desiderius Erasmus Roterodamus. I like the proverb *Non semper erit aestas* (it will not always be summer … it also means be prepared for hard times).

Seneca has said something very similar, *non semper Saturnalia erunt* (Saturnalia will not last forever). The Saturnalia was a principal festival of the Romans.

For those in the northern hemisphere, this is a time of year to visit a relaxing location *not for business*. There is no better way to relax than to get outside, unplug and just enjoy nature and life.

I never completely shut off, but I always find time to read interesting papers. Yes, papers, not novels. Why should I read a spy novel, when I can read a declassified paper (records under the Freedom of Information Act or Mandatory Declassification Review, available at the NSA website).

Which is first in the list? The paper with title "*Reading Between the Lines: Methods of Analysis of Soviet Military Literature*".

We read: "Probably since the first hieroglyphics were linked onto papyrus, military authors have been beset by a fundamentally unresolvable conflict.

On the one hand, propaganda and indoctrination ask that military information be spread widely to persuade and instruct.

On the other hand, security demands strict controls on the spread of that same information to protect what are deemed vital state secrets.

The Soviets, well aware of the problem, prefer to stress security. That presents a dilemma to Soviet officers, especially those with sensitive areas of expertise, who wish to advance their careers by publishing books or articles."

"Language can either throw up barriers or pave the way to understanding. This article has already considered one limited use of language, terminology, as a finite set of fixed expressions. The scope can also be widened for a look at the entire spectrum of word usage.

In the broadest sense, all researchers must grapple with linguistic nuances to obtain the data they are seeking.

More specifically, however, there are certain uses of language which can be exploited in their own right, regardless of the basic meaning being conveyed, to discover interesting facts about the user.

Translation from one language into another presents a specific case where meaning can be either obscured or clarified, depending on the circumstances.

Glaring and embarrassing errors in translation, such as Jimmy Carter's English "love" for the people of Poland turning into "carnal desire" with interpretation into Polish, make great reading in newspapers.

They merit no further attention for practical study of Soviet military literature. Instead, greater profit can be gained by exploiting the helpful clues to be found in Soviet translations, especially those from English to Russian.

Words chosen for translation, and those omitted, can tell a great deal about the state of an author's knowledge and mental processes.

For instance, this author, while gaining some valuable new knowledge, got much less than he expected from a recently published Soviet dictionary on military electronic terminology (Nikolay Nikolaevich Novichkov and German Semenovich Pimenov, English-Russian Military Dictionary of Radioelectronics, Laser, and Infrared Engineering, Military Publishing House, 1984).

Instead, what the dictionary contained were a number of significant omissions and a hodgepodge of entries of doubtful validity.

It omitted avionics, a contraction for aviation electronics in common usage in American aviation publications for a generation or more.

The closest equivalent for the term in the dictionary was an entry for aerospace electronics.

Then it devoted seven pages to mostly useless word associations with device, such as lasing device (i.e., a laser).

Taken at face value, the work shows that some Soviets who should be better informed demonstrate a serious lack of understanding of an important sector of Western technical terminology.

At the same time, the book proved its worth by showing how firmly entrenched the new vocabulary associated with radioelectronic combat has become."

Interesting.

May you and your family have a happy and healthy summer!

Welcome to our monthly newsletter.

Best regards,

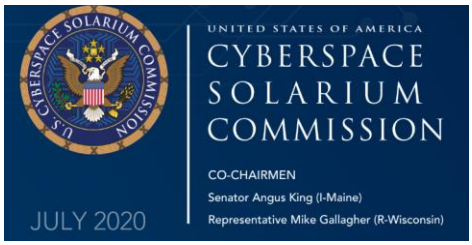
George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

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

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein and Germany:
https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2020.pdf

Number 1 (Page 17)

The Cyberspace Solarium Commission report consists of over 80 recommendations which are organized into 6 pillars.



Number 2 (Page 20)

ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme

The EUCC Candidate Scheme for ICT Products, set to replace the SOG-IS, is released today for public feedback.

Number 3 (Page 22)

EINSTEIN Data Trends – 30-day Lookback

Number 4 (Page 24)

NIST Kick-Starts 'Threshold Cryptography' Development Effort

Number 5 (Page 27)

EIOPA publishes its second Discussion Paper on Methodological Principles of Insurance Stress Testing

Number 6 (Page 29)

Risk Dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

Number 7 (Page 32)

NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation

NCA
National Crime Agency

Number 8 (Page 36)

Mitigating Synthetic Identity Fraud in the U.S. Payment System

THE FEDERAL RESERVE
FedPayments Improvement
COLLABORATE. ENGAGE. TRANSFORM.

Number 9 (Page 39)

Episode 29: The Light and Matter Maestro

DARPA
DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Number 10 (Page 40)

Attackers Cryptojacking Docker Images to Mine for Monero

paloalto NETWORKS | UNIT 42

Number 11 (Page 41)

GCHQ to help firms use cutting edge tech to keep citizens safe

GCHQ

Number 12 (Page 43)

Washington Man Sentenced for Role in Developing "Mirai" Successor Botnets

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of ALASKA

Number 13 (Page 45)

Securing Industrial Control Systems: A Unified Initiative

Number 14 (Page 47)

HMRC phishing scam targets passport information

National Cyber Security Centre

Number 15 (Page 48)

DHS, DOT, and HHS Issue New Guidance for Airline Industry Partners to Facilitate Safe Air Travel

Homeland Security

Number 16 (Page 51)

Understanding fake news: A bibliographic perspective. Andrew Park, Matteo Montecchi, Cai 'Mitsu' Feng, Kirk Plangger, and Leyland Pitt

Number 17 (Page 53)

Priorities for the Financial Action Task Force (FATF) under the German Presidency, Objectives for 2020-2022

FATF Financial Action Task Force

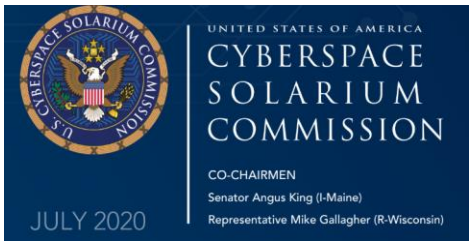
Number 18 (Page 55)

Annual Report on Trust Services Security Incidents in 2019

enisa European Network and Information Security Agency

Number 1

The Cyberspace Solarium Commission report consists of over 80 recommendations which are organized into 6 pillars.



These 6 pillars are as follows:

1. Reform the U.S. Government's Structure and Organization for Cyberspace.

While cyberspace has transformed the American economy and society, the government has not kept up.

Existing government structures and jurisdictional boundaries fracture cyber policymaking processes, limit opportunities for government action, and impede cyber operations.

Rapid, comprehensive improvements at all levels of government are necessary to change these dynamics and ensure that the U.S. government can protect the American people, their way of life, and America's status as a global leader.

2. Strengthen Norms and Non-Military Tools.

A system of norms, built through international engagement and cooperation, promotes responsible behavior and dissuades adversaries from using cyber operations to undermine American interests.

The United States and others have agreed to norms of responsible behavior for cyberspace, but they go largely unenforced.

The United States can strengthen the current system of cyber norms by using non-military tools, including law enforcement actions, sanctions, diplomacy, and information sharing, to more effectively persuade states to conform to these norms and punish those who defect from them.

A coalition of like-minded allies and partners willing to collectively support a rules-based international order in cyberspace will better hold malign actors accountable.

3. Promote National Resilience.

Resilience, the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior, is key to denying adversaries the benefits of their operations and reducing confidence in their ability to achieve their strategic ends.

National resilience efforts rely on the ability of both the United States public and private sectors to accurately identify, assess, and mitigate risk across all elements of critical infrastructure.

The nation must be sufficiently prepared to respond to and recover from an attack, sustain critical functions even under degraded conditions, and, in some cases, restart critical functionality after disruption.

4. Reshape the Cyber Ecosystem.

Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries' activities. Over time, this will reduce the frequency, scope, and scale of their cyber operations.

Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes. In some cases, that requires aligning market forces.

In other cases, where those forces either are not present or do not adequately address risk, the U.S. government must explore legislation, regulation, executive action, and public-as well as private-sector investments.

5. Operationalize Cybersecurity Collaboration with the Private Sector.

Unlike in other physical domains, in cyberspace the government is often not the primary actor. It must support and enable the private sector.

The government must build and communicate a better understanding of threats, with the specific aim of informing private-sector security operations, directing government operational efforts to counter malicious cyber activities, and ensuring better common situational awareness for collaborative action with the private sector.

While recognizing that private-sector entities have primary responsibility for the defense and security of their networks, the U.S. government must bring to bear its unique authorities, resources, and intelligence capabilities to support these actors in their defensive efforts.

6. Preserve and Employ the Military Instrument of National Power.

Future crises and conflicts will almost certainly contain a cyber component. In this environment, the United States must defend forward to limit malign adversary behavior below the level of armed attack, deter conflict, and, if necessary, prevail employing the full spectrum of its capabilities.

Conventional weapons and nuclear capabilities require cybersecurity and resilience to ensure that the United States preserves credible deterrence and the full range of military response options.

Across the spectrum from competition to crisis and conflict, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives through cyberspace.

Note: The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The finished report was presented to the public on March 11, 2020.

To read more:
https://drive.google.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view

Number 2

ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme

The EUCC Candidate Scheme for ICT Products, set to replace the SOG-IS, is released today for public feedback.

The European Union Agency for Cybersecurity, ENISA, is launching a month-long public consultation for the first candidate cybersecurity certification scheme, the Common Criteria based European cybersecurity certification scheme (EUCC).

The scheme aims to replace the existing schemes operating under the SOG-IS MRA for ICT products, to add new elements and to extend the scope to cover all EU Member States.

The public consultation allows interested parties to provide feedback on the draft of the EUCC candidate scheme and the outcome will be processed and shared. The consultation will remain open for contributions until July 31st, 12:00 CET.

Over the past two decades, the Common Criteria have proven efficient for the certification of chips and smartcards across Europe, and have enhanced the level of security of electronic signature devices, for means of identification such as passports, banking cards and tachographs for lorries. More recently, the criteria have been used intensively to certify the cybersecurity of ICT software products.

This new candidate scheme aims to further improve the Union's internal market conditions for ICT products, and positively affects the ICT services and ICT processes relying on such products.

About the EUCC candidate scheme:

- Built on the current SOG-IS MRA and Common Criteria with rules included for transition;
- Applicable to ICT products;
- Covers assurance levels 'Substantial' and 'High';
- Certificate validity for five years, can be renewed;

- Allows for composite certification;
- Recognition in all EU Member States;
- Voluntary scheme;
- Harmonised conditions for vulnerability handling and disclosure;
- Clearly defined rules on monitoring and handling non-compliance and non-conformity;
- Introduces a new patch management mechanism to support vulnerability handling;
- Use of a framework-based label and a QR code to ensure easy access to accurate certification information.

The EU Cybersecurity Act of 2019 (CSA) lays down an EU cybersecurity certification framework for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as of avoiding fragmentation of the internal market.

ENISA's task under the CSA is to prepare and develop candidate cybersecurity certification schemes with the involvement and support of stakeholders and a working group.

The first ad hoc working group for this scheme, the EUCC AHWG, was set up late last year by ENISA, and is chaired by the Agency.

The group is composed of 20 appointed members representing industry (developers, evaluators), and 12 participants from Member States and accreditation bodies.

The EUCC AHWG has been working in close collaboration with the Commission and with the European Cybersecurity Certification Group (ECCG). The EUCC is the first candidate scheme in the framework.
A second candidate scheme is currently in preparation and relates to the certification of cloud services.

More information at:
https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes

https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/

Number 3

EINSTEIN Data Trends – 30-day Lookback

Cybersecurity and Infrastructure Security Agency (CISA) analysts have compiled the top detection signatures that have been the most active over the month of May in our national Intrusion Detection System (IDS), known as EINSTEIN.

This information is meant to give the reader a closer look into what analysts are seeing at the national level and provide technical details on some of the most active threats.

IDS is a network tool that uses sensors to monitor inbound and outbound traffic to search for any type of suspicious activity or known threats, alerting analysts when a specific traffic pattern matches with an associated threat.

IDS allows users to deploy signatures on these boundary sensors to look for the specific pattern, or network indicator, associated with a known threat.

The EINSTEIN Program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the federal civilian departments and agencies.

By collecting information from participating federal departments and agencies, CISA builds and enhances our Nation's cyber-related situational awareness.

The signatures CISA created have been included below for analysts across various organizations to use in enhancing their own network defenses.

Note: CISA has created and tested these signatures in an environment that might not be the same for all organizations, so administrators may need to make changes or updates before using in the following signatures in their local environments.

1. NetSupport Manager RAT

The NetSupport Manager Remote Access Tool (RAT) is a legitimate program that, once installed on a victim's machine, allows remote administrative control.

In a malicious context, it can—among many other functions—be used to steal information.

Malicious RATs can be difficult to detect because they do not normally appear in lists of running programs, and they can mimic the behavior of legitimate applications.

In January 2020, Palo Alto researchers observed the abuse of NetSupport in targeted phishing email campaigns.

In November 2019, Zscaler researchers observed "software update-themed" campaigns tricking users into installing a malicious NetSupport Manager RAT.

The earliest malicious use of NetSupport was seen in a phishing email campaign—reported by FireEye researchers in April 2018.

To read more: https://www.us-cert.gov/ncas/alerts/aa20-182a

Number 4

NIST Kick-Starts 'Threshold Cryptography' Development Effort

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

A new publication by cryptography experts at the National Institute of Standards and Technology (NIST) proposes the direction the technical agency will take to develop a more secure approach to encryption. This approach, called threshold cryptography, could overcome some of the limitations of conventional methods for protecting sensitive transactions and data.

The document, released today in a final version as NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives (NISTIR 8214A), offers an outline for developing a new way to implement the cryptographic tools that developers use to secure their systems.

Its authors are inviting the cryptography community to collaborate with them on NIST's budding Threshold Cryptography project, which in part seeks to ensure that threshold implementations are interoperable.

"We are kicking the threshold cryptography development effort into high gear," said Apostol Vassilev, a NIST computer scientist. "Over the coming months, the Threshold Cryptography project will be engaging with the public to define criteria for this work. We want to get feedback from the community so we can consider a variety of threshold schemes and standardization paths."

Threshold cryptography takes its name from the idea that individual keyholders cannot open a lock on their own, as is common in conventional cryptography. Instead, out of a group of keyholders, there must be a minimum number of them — a "threshold" number — working together to open the lock.

In practice, this lock is an electronic cryptosystem that protects confidential information, such as a bank account number or an authorization to transfer money from that account.

A threshold system is complicated because the keyholders must be able to collaborate on a task without seeing one another's parts of the key. But a successful system might address some of the weak spots in conventional cryptography, because a threshold system would be safe even if some of the keyholders get hacked.

In conventional cryptosystems, “the main problem is the single point of failure,” Vassilev said. “If you give all your authority to a single individual, you’ve given them a lot of trust and responsibility. Not only can single individuals get corrupted, but they also get sick or go on vacation. If they’re unavailable, it can cause bottlenecks.”

Another vulnerability of conventional systems is the “side-channel attack,” in which an adversary monitors a computer performing an encryption operation in order to obtain details such as the power the chip consumes or the time it takes to produce a key.

These details give insights about the key, eventually permitting attacks such as the recent Spectre and Meltdown hacks on widely available computer processors. Threshold systems might address this and other weaknesses as well, said Vassilev’s colleague Luís Brandão.

“The threshold paradigm can prevent the computer itself from becoming the single point of failure,” said Brandão, a coauthor of the report. “The computer never has the key in the first place.”

The idea of threshold cryptography is not new in and of itself, but some of the algorithms needed to effectively carry out a threshold scheme have only recently become mature enough to consider developing standards, Vassilev said.

The new NIST publication and its previously released companion, NISTIR 8214, are an initial step toward those standards, with the aim of gathering a solid rationale to devise criteria for standards.

“The first one, NISTIR 8214, describes what it is we want to work on,” he said, “while NISTIR 8214A outlines a road map for how to get there. Those two things are what we’re trying to clarify with the help of the cryptography community.”

A near-term goal will be to develop ways to apply threshold schemes to what are known as “cryptographic primitives” — the fundamental building blocks of logic that can be combined to make software for cryptography systems.

A primitive handles a specific task like creating a digital signature, but it must be combined with others to do complex jobs such as maintaining a secure internet connection. A well-considered set of primitives could form the basis of effective threshold cryptography systems.

The larger goal is to enhance the security of the implementation and operations of standardized cryptographic primitives. The Threshold

Cryptography project will explore what threshold schemes have the best potential for interoperability and effectiveness when applied to NIST-approved primitives.

The end results may span a variety of formats, including guidance, recommendations and reference definitions. The integration with existing standards will become more clear as the project moves along.

The NIST team has organized the development effort into two tracks. One will focus on threshold cryptography for single-device hardware, such as computer processors, which are particularly vulnerable to side-channel attacks.

The other will focus on multiparty devices, which typically consist of several computers connected over a network collaborating in a threshold computation. These devices bring their own challenges, such as performing tasks when the parts of the secret key are distributed among devices spread across several locations.

The single-device track is the subject of a July 7-9 webinar hosted by the Belgian university KU Leuven — an event that will help NIST continue to work with the international community on technical advancements in cryptography.

The NIST webinar presentation slides are available online, and the NIST Threshold Cryptography project page contains more information on collaborating with the team. This collaboration will be crucial to the long-term development effort, Vassilev said.

“It is quite important to have feedback and contributions from the community,” he said. “Some of the additional concrete ways in which we will advance will become clear as we work together. Join the party if you want to influence the direction the effort goes.”
To read more:
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8214A.pdf

https://csrc.nist.gov/Projects/threshold-cryptography

Number 5

EIOPA publishes its second Discussion Paper on Methodological Principles of Insurance Stress Testing

The European Insurance and Occupational Pensions Authority (EIOPA) published its second Discussion Paper on Methodological Principles of Insurance Stress Testing. You may visit: https://www.eiopa.europa.eu/content/second-discussion-paper-methodological-principles-insurance-stress-testing_en

In 2019 EIOPA initiated a process of enhancing its methodology for bottom-up stress testing which resulted in the first Methodological Paper setting out the methodological principles of insurance stress testing. You may visit: https://www.eiopa.europa.eu/content/methodological-principles-insurance-stress-testing_en

Based on a constructive dialogue and feedback received from stakeholders in the preparation of the first Methodological Paper, EIOPA follows the same approach and is now engaging with stakeholders to further enrich the stress test toolbox with additional elements to be potentially applied in future exercises.

The second Discussion Paper is structured in three sections addressing the following topics:

- Stress test framework on climate change
- Approach to liquidity stress testing
- Multi-period framework for the bottom-up insurance stress testing

EIOPA invites stakeholders to provide feedback to be considered in the final Paper. To this aim, it contains a series of questions to collect feedback particularly on technical topics linked to key elements of insurance stress testing.

The Discussion Paper is part of a broader process to enhance EIOPA's stress testing framework.

In this context, EIOPA will work on specific stress testing related topics such as the assessment of liquidity positions under adverse scenarios, assessment of the vulnerabilities towards climate-related risks and potential approaches to multi-period stress tests.

The Discussion Paper is open for comments until Friday, *2 October 2020*. Stakeholders are invited to submit their feedback via email by using the provided template. Contributions should be sent to the following email address: eiopa.stress.test@eiopa.europa.eu

Contributions either not provided via the template, sent to a different email address or sent after the deadline will not be considered.

Unless requested otherwise, all contributions received will be published after the deadline for submission.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/consultations/eiopa-bos-20-341_second-discussion_paper-methodological-principles-for-stress-testing.pdf

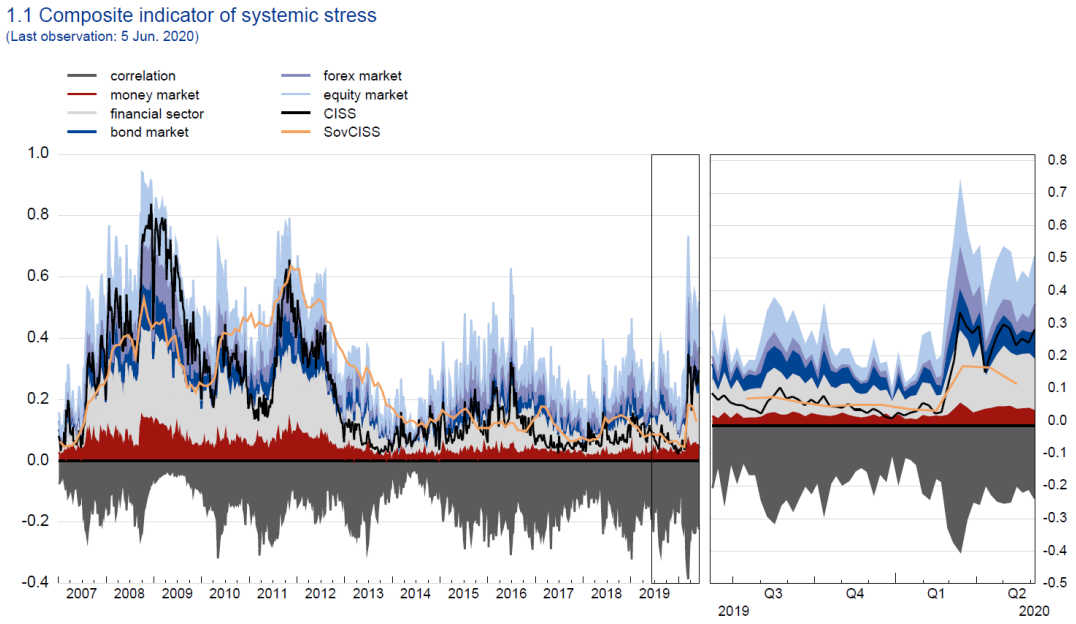
Number 6

Risk Dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

The ESRB risk dashboard is a set of quantitative and qualitative indicators of systemic risk in the EU financial system. It is published quarterly, one week after its adoption by the General Board, and is accompanied by an overview note that explains the recent development of the indicators, and two annexes that explain the methodology and describe the indicators.

The risk dashboard should not be considered to be a policy statement on systemic risks. Additional indicators that support systemic risk assessment in the EU financial system are available in the Macro-prudential database maintained by the ECB.



Market-based indicators of systemic stress in the European Union (EU) showed positive signs of recovery from the economic shock caused by the outbreak of the coronavirus (COVID-19).

During the second quarter of 2020 the indicators of systemic stress gradually decreased and stabilised at a lower level.

Similarly, indicators of implied volatility, which measure market uncertainty, decreased notably across various market segments and the probability of the simultaneous default of large and complex banking groups and EU sovereigns also fell.

Instead, there was some variation in the implied volatility of short-term interest rates, as the level of volatility of interest rates denominated in pound sterling continued to rise while the volatility for US dollar interest rate decreased, with large fluctuations.

EU equity indices and price/earnings ratios recovered most of their losses.

However, equity prices of financials, particularly banks and insurance companies, recovered only moderately and did not return to their pre-COVID-19 levels.

Regarding macroeconomic developments, euro area monetary financial institution (MFI) credits and deposits rose significantly in the first quarter of 2020.

The total amount of four-quarter cumulated credit flows increased by around €600 billion owing mainly to a large increase in credit to non-euro area residents and somewhat smaller increases in credit to non-financial corporations (NFCs) and to the general government.

Total deposits soared by approximately the same amount as credits because of the positive contribution of the deposits of the Eurosystem, NFCs, and other financial institutions.

There were no significant changes in the domestic credit-to-GDP gap in the fourth quarter of 2019.

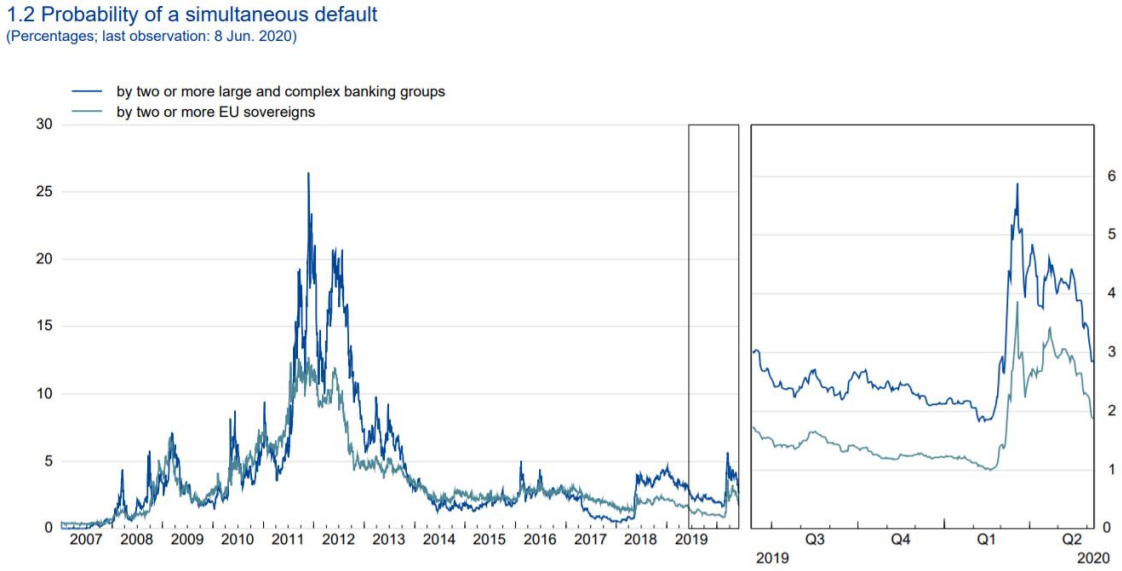
A deep economic contraction prevailed in the EU and the euro area throughout the first quarter of 2020 as a result of the stringent lockdown measures implemented in most the Member States, a collapse of global trade and the confidence shock affecting the economy.

In the first quarter of 2020, EU GDP and euro area GDP plummeted by 2.6% and 3.1% year on year respectively.

More than half of EU Member States suffered an economic slump, with Italy, France and Spain being the most severely hit countries (recording falls in GDP of 5.4%, 5.1%, and 4.1% respectively in the first quarter of 2020).

The outlook for the EU economy is surrounded by considerable uncertainty with regard to the depth and length of the coronavirus pandemic and its ultimate economic implications.

Even larger impacts on production and unemployment are expected in the second quarter of 2020, while the European Commission and the ECB forecasts do not anticipate a sustained recovery before 2021.



To read more: https://www.esrb.europa.eu/pub/rd/html/index.en.html

Number 7

NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation

NCA
National Crime Agency

Entire organised crime groups dismantled during Operation Venetic with 746 arrests, and £54m criminal cash, 77 firearms and over two tons of drugs seized so far.

UK law enforcement has made a massive breakthrough in the fight against serious and organised crime after the takedown of a bespoke encrypted global communication service used exclusively by criminals.

EncroChat was one of the largest providers of encrypted communications and offered a secure mobile phone instant messaging service, but an international law enforcement team cracked the company's encryption.

There were 60,000 users worldwide and around 10,000 users in the UK – the sole use was for coordinating and planning the distribution of illicit commodities, money laundering and plotting to kill rival criminals.

Since 2016, the National Crime Agency has been working with international law enforcement agencies to target EncroChat and other encrypted criminal communication platforms by sharing technical expertise and intelligence.

Two months ago this collaboration resulted in partners in France and the Netherlands infiltrating the platform. The data harvested was shared via Europol.

Unbeknown to users the NCA and the police have been monitoring their every move since then under Operation Venetic – the UK law enforcement response.

Simultaneously, European law enforcement agencies have also been targeting organised crime groups.

The EncroChat servers have now been shut down.

Operation Venetic is the biggest and most significant operation of its kind in the UK.

The NCA, Regional Organised Crime Units (ROCUs) and police forces have punched huge holes in the UK organised crime network so far by arresting 746 suspects and seizing:

- Over £54million in criminal cash
- 77 firearms, including an AK47 assault rifle, sub machine guns, handguns, four grenades, and over 1,800 rounds of ammunition
- More than two tonnes of Class A and B drugs
- Over 28 million Etizolam pills (street Valium) from an illicit laboratory
- 55 high value cars, and 73 luxury watches

In addition, a specialist NCA team, working closely with policing partners, has prevented rival gangs carrying out kidnappings and executions on the UK's streets by successfully mitigating over 200 threats to life.

Organised crime groups in the UK have been using EncroChat, communicating freely believing the technology made them secure. The criminal group behind EncroChat operated from outside the UK.

On 13 June EncroChat realised the platform had been penetrated and sent a message to its users urging them to throw away their handsets.

The phones – which have pre-loaded apps for instant messaging, the ability to make VOIP calls and a kill code which wipes them remotely – have no other conventional smart phone functionality and cost around £1,500 for a six-month contract.

And recent messages from some of the UK handsets included:

- "This year the police are winning."
- "NCA as u know well are sophisticated and relentless."
- "If NCA then we have a big problem."
- "The police are having a field day."

The NCA created the technology and specialist data exploitation capabilities required to process the EncroChat data, and help identify and locate offenders by analysing millions of messages and hundreds of thousands of images.

Intelligence packages were disseminated to NCA operational teams, ROCUs, Police Service of Northern Ireland, Police Scotland, Metropolitan Police, Border Force, the Prison Service, and HMRC to develop and launch investigations.

The highest-harm organised crime groups were prioritised, with officers working tirelessly to attribute the handles to real world identities.

The Crown Prosecution Service is leading all the Operation Venetic prosecutions.

NCA Director of Investigations Nikki Holland, said:

“The infiltration of this command and control communication platform for the UK’s criminal marketplace is like having an inside person in every top organised crime group in the country.

“This is the broadest and deepest ever UK operation into serious organised crime.

“The NCA is proud to have led the UK part of this operation, working in partnership with policing and other agencies. The results have been outstanding but this is just the start.

“A dedicated team of over 500 NCA officers has been working on Operation Venetic night and day, and thousands more across policing. And it’s all been made possible because of superb work with our international partners.

“Together we’ve protected the public by arresting middle-tier criminals and the kingpins, the so-called iconic untouchables who have evaded law enforcement for years, and now we have the evidence to prosecute them.

“The NCA plays a key role in international efforts to combat encrypted comms. I’d say to any criminal who uses an encrypted phone, you should be very, very worried.”

National Police Chiefs’ Council lead for serious organised crime, Chief Constable Steve Jupp, said:

“This unique operation has specifically focussed on those thought to be involved in the highest levels of organised crime and drugs supply across the UK.

“I want to emphasise that this work is the culmination of meticulous planning to tackle the most serious and organised crimes groups that have been working in our communities.

“Serious organised crime is complex but working together with our Regional Organised Crimes Units and the National Crime Agency we have achieved an unparalleled victory against the kingpin criminals whose criminal activity and violence intimidates and exploits the most vulnerable.

“By dismantling these groups, we have saved countless lives and protected communities across the UK.

“Every UK police force has worked together to carry out these warrants, and I’m extremely proud of their hard work and determination which doesn’t stop here.

“This sort of activity is just one aspect of our continued fight to tackle serious and organised crime. I hope this sends a clear message to the public of our determination to rid communities of this sort of criminalisation.”

Home Secretary Priti Patel said:

“This operation demonstrates that criminals will not get away with using encrypted devices to plot vile crimes under the radar.

“The NCA’s relentless targeting of these gangs has helped to keep us all safe. I congratulate them and law enforcement partners on this significant achievement.

“I will continue working closely with the NCA and others to tackle the use of such devices – giving them the resources, powers and tools they need to keep our country safe.”

Number 8

Mitigating Synthetic Identity Fraud in the U.S. Payment System

In 2019, the Federal Reserve published two white papers as part of our Payments Fraud Insights series.

Our goal was to raise awareness and encourage industry action against synthetic identity fraud, reportedly the fastest-growing type of financial crime facing the United States.

The first paper focused on causes and contributing factors of synthetic identity fraud and its impact on the U.S. payment system, while the second focused on detecting synthetics and examples of sharing information across the industry.

This white paper picks up where our last one left off. It highlights different ways that organizations – both individually and collectively – can work to mitigate synthetic identity fraud.

Additionally, we summarize a number of external factors that impact mitigation, such as the regulatory environment.

Synthetic identity fraud is not a problem that any one organization or industry can tackle independently, given its far-reaching effects on the U.S. financial system, private industries – such as healthcare, automotive and insurance – government entities and consumers.

The Federal Reserve recognizes the need for collaboration as we work with a wide array of payments industry stakeholders to advance U.S. payments security, which is consistent with the approaches described in our paper, Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey.

Our Payments Fraud Insights white papers were made possible by the contributions of many industry and government subject matter experts and Federal Reserve colleagues.

We appreciate your shared insights and look forward to continued dialogue and collaboration in reducing synthetic identity payments fraud.

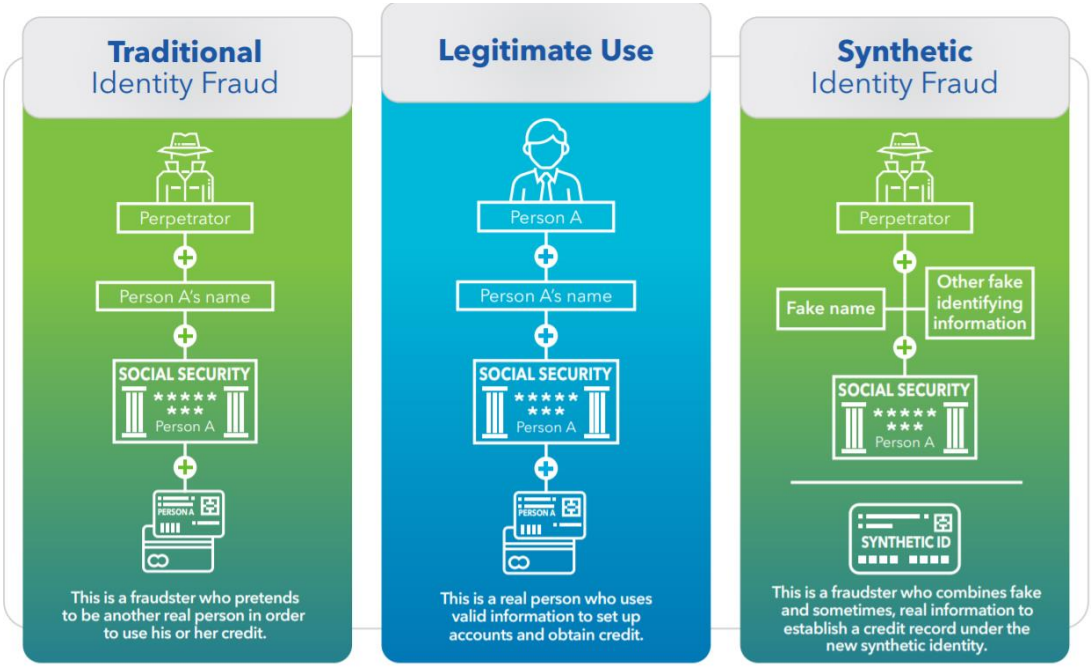
Synthetic identity fraud occurs when perpetrators combine fictitious and sometimes, real information, such as names and Social Security numbers (SSNs), to create new identities.

These identities may then be used to defraud financial institutions, private industry, government agencies or individuals.

Differing definitions and approaches to detection make it difficult to quantify the impact on the U.S. financial system.

One widely reported analysis by Auriemma Group suggested that synthetic identity fraud cost U.S. lenders $6 billion and accounted for 20% of credit losses in 2016.

Our first white paper, Synthetic Identity Fraud in the U.S. Payment System, described key characteristics of this type of fraud. You can find it at:
https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf



Fraudsters leverage the personally identifiable information (PII) of individuals – frequently children, the elderly or homeless – who are less likely to access their credit information and thus, discover the fraud.

Synthetic identities can behave like legitimate accounts and may not be flagged as suspicious using conventional fraud detection models. This affords perpetrators the time to cultivate these identities, build positive credit histories, and increase their borrowing or spending power before

"busting out" – the process of maxing out a line of credit with no intention to repay.

The ease and low cost of creating synthetic identities contributes to the widespread impact of this type of fraud on financial institutions, private industry, government agencies and individuals.

Sophisticated crime rings can leverage multiple tactics at scale to cultivate synthetic identities, including using fake addresses, creating sham businesses and forming relationships with collusive merchants to cash in.

To read more:
http://www.fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf

https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/

Number 9

Episode 29: The Light and Matter Maestro

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this episode of the Voices from DARPA podcast, Dr. Michael Fiddy, a program manager since 2016 in the agency's Defense Sciences Office (DSO), takes listeners on a whirlwind tour of his programs.

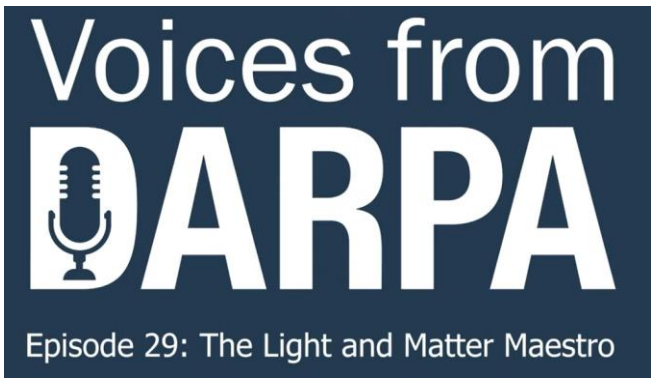
They all share a common thread, which stems from Fiddy's lifelong interest in how light — electromagnetic (EM) energy, more generally — interacts with matter.

At DARPA, he has expressed that interest by challenging researchers to investigate whether biological cells interact with one another via EM signals; how it might be possible to use low-frequency EM radiation to see through just about anything (including metal); and how precisely engineered surfaces might tap into quantum mechanical phenomena (Casimir forces) in the vacuum of space in a quest for fuel-less propulsion technology.

As Fiddy points out in the podcast, "We have been doing science for a few hundred years and there still is an awful lot that we don't know."

YouTube: https://www.youtube.com/watch?v=_bfb5w5h9xk

iTunes: https://itunes.apple.com/us/podcast/voices-from-darpa/id1163190520



Number 10

Attackers Cryptojacking Docker Images to Mine for Monero

Docker containers have been gaining popularity over the past few years as an effective way of packaging software applications.

Docker Hub provides a strong community-based model for users and companies to share their software applications.

This is also attracting the attention of malicious actors intending to make money by cryptojacking within Docker containers and using Docker Hub to distribute these images.

We identified a malicious Docker Hub account, azurenql, active since October 2019 that was hosting six malicious images intended to mine the cryptocurrency, Monero.

The coin mining code within the image intends to evade network detection by using network anonymizing tools such as ProxyChains and Tor.

The images hosted on this account have been collectively pulled more than two million times.

For context, there are legitimate Azure related images under the official Microsoft Docker Hub account that have anywhere from a few thousand to 100 million+ pulls.

One of the wallet IDs identified has been used to earn more than 525.38 XMR, which roughly translates to $36,000 USD. Additionally, when we last checked minexmr.com for this wallet ID, we saw recent activity indicating that it's still being used.

We would like to give a shout out to the awesome security team at Docker Hub. They were very responsive and were able to take down this malicious Docker Hub account quickly in response to our notification.

Palo Alto Networks customers are protected by this threat through Threat Prevention signatures on the Next-Generation Firewall. Prisma Cloud customers are protected by this through the Trusted Images feature.

To read more: https://unit42.paloaltonetworks.com/cryptojacking-docker-images-for-mining-monero/

Number 11

GCHQ to help firms use cutting edge tech to keep citizens safe

The mentorship scheme – called the GCHQ Innovation Co-Lab - is being run from our new Manchester offices, and will see a drive to find innovative start-ups and small to medium sized businesses based in the North West.

Companies taking part in the 12-week programme will work with GCHQ technologists and industry experts to improve their products using data science, artificial intelligence and machine learning.

The aim is to support the development of innovative products in health, education and other sectors including those that tackle the long-term effects of organized crime.

Gav Smith, GCHQ Director General for Technology, said:

“As we increasingly live more of our lives online there is a greater risk data can be manipulated to commit crimes and take advantage of the most vulnerable members of our society.

With GCHQ’s mentorship and support these businesses will have the potential to use the latest technology to improve people’s safety online.”

GCHQ helps keep the UK safe, using cutting-edge technology, technical ingenuity and world leading partnerships to identify, analyse and disrupt threats in an increasingly complex world.

Last year we announced the opening of a new Manchester city centre hub in Albert Square. The hi-tech premises is now at the heart of the nation’s security.

Mr Smith added: “We’re excited to be supporting the thriving technology ecosystem in Greater Manchester, connecting ingenious entrepreneurs and creative technologists with the mission of GCHQ to help tackle some of our hardest challenges.”

A previous mentorship scheme run by our Manchester office supported a range of companies to develop innovative products including software to identify illegal online pharmacies, smart home monitoring for assisted living, and an augmented reality app for suicide prevention.

The GCHQ Innovation Co-Lab is a joint venture with The Landing, a tech mentorship hub based in MediaCityUK, and global tech accelerator UP Ventures.

Emer Coleman, Project Director at Up Accelerator said:

"The GCHQ Innovation Co-Lab will focus on enabling cutting-edge technologies based around data science, artificial intelligence and machine learning. Critical sectors such as, health, education, emergency services and
communications rely heavily on data integrity on which increasingly, vital machine learning is based.

This will only become more important in the future as citizens and businesses across the globe adjust to living with COVID19. Our goal is to help emerging businesses make technical and commercial breakthroughs with their ingenious products and services by giving them access to world-class GCHQ technologists as well as industry experts and dedicated coaches."

Jon Corner, Chief Digital Officer at City of Salford said:

"The GCHQ Innovation Co-Lab at The Landing resonates with our ambitions in Salford and Greater Manchester to build products and solutions that work for all citizens.

I'm delighted that The Landing MediaCityUK is a key part of an evolving and growing partnership with GCHQ, which itself is contributing to the strength of the Greater Manchester digital eco-system

To read more:
https://www.gchq.gov.uk/news/innov-co-lab

https://www.thelanding.org.uk/gchq-innovation-co-lab/

Number 12

Washington Man Sentenced for Role in Developing "Mirai" Successor Botnets

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of ALASKA

U.S. Attorney Bryan Schroder announced that a Washington man has been sentenced to federal prison for his role in a long-running scheme in which he and his criminal associates developed distributed denial-of-service (DDoS) botnets.

The defendant used the botnets to facilitate DDoS attacks, which occur when multiple computers acting in unison flood targeted computers with information to prevent them from being able to access the internet.

Kenneth Currin Schuchman, 22, of Vancouver, WA, was sentenced by Chief U.S. District Judge Timothy M. Burgess to serve 13 months in prison, after previously pleading guilty to one count of fraud and related activity in connection with computers, in violation of the Computer Fraud & Abuse Act.

As part of his sentence, Schuchman was also ordered to serve a term of 18 months of community confinement following his release from prison and a three year term of supervised release.

According to court documents, the botnets were initially based largely on the source code previously developed by other individuals to create the Mirai botnet; however, Schuchman and his criminal associates "Vamp" and "Drake" added additional features over time, so that the botnets grew more complex and effective.

At various times, these successor botnets were known as "Satori," "Okiru," "Masuta," and "Tsunami"/"Fbot." While Schuchman and his criminal associates utilized these successor botnets to conduct DDoS attacks themselves, their primary focus was selling access to paying customers in order to generate illicit proceeds.

The investigation revealed that Schuchman had been engaging in criminal botnet activity since at least August 2017, ultimately compromising hundreds of thousands of devices worldwide, including devices in the District of Alaska.

Schuchman continued to engage in criminal botnet activity, and violated several other conditions of his pretrial release, following his arrest in August 2018.

The three defendants responsible for creating the Mirai botnet, the computer attack platform that inspired the successor botnets, were previously sentenced in September 2018.

“Cybercriminals depend on anonymity, but remain visible in the eyes of justice,” said U.S. Attorney Schroder. “Today’s sentencing should serve as a reminder that together with our law enforcement and private sector partners, we have the ability and resolve to find and bring to justice those that prey on Alaskans and victims across the United States.”

“Cyber-attacks pose serious harm to Alaskans, especially those in our more remote communities,” said Special Agent in Charge Robert W. Britt of the FBI's Anchorage Field Office. “The increasing number of Internet - connected devices presents challenges to our network security and our daily lives.

The FBI Anchorage Field Office will continue to work tirelessly alongside our partners to combat those criminals who use these devices to cause damage globally, as well as right here in our own neighborhoods.”

In a recently unsealed indictment, Schuchman’s criminal associates Aaron Sterritt, a/k/a “Vamp,” or “Viktor” a national of the United Kingdom; and Logan Shwydiuk, a/k/a “Drake,” a Canadian national, have also been charged for their roles in developing and operating these botnets to conduct DDoS attacks, following an investigation by the FBI with the assistance of other law enforcement partners.

To read more: https://www.justice.gov/usao-ak/pr/washington-man-sentenced-role-developing-mirai-successor-botnets

Number 13

Securing Industrial Control Systems: A Unified Initiative

The security of ICS and other operational technologies is essential to achieving CISA's vision of secure and resilient infrastructure for the American people.

Through implementation of this initiative, CISA and our partners will help the ICS community reach the following critical end-state conditions.

- ICS performs within thresholds under duress. ICS networks are resilient to cyberattacks and continue to perform within operational parameters in support of NCFs, despite malicious actions by adversaries in the control systems environment.

- The ICS security community is faster and smarter than its adversaries. Collaborating across industries and national borders, the ICS community raises the cost, time, and complexity thresholds for successful ICS attacks to the point that they exceed the capabilities of even the most advanced threat actors.

- OT devices and networks are secure by design. New OT products, from industrial scale control systems and networks to Internet of Things (IoT) devices, are secure by design. Cybersecurity becomes a preeminent consideration in the development and design of new OT products, and operators can apply security updates without operational disruption.

- Risk drives ICS security priorities. CI asset owners and operators distribute ICS security resources based on a clearly defined risk posture and risk tolerances, and the Federal Government invests resources based on ICS risks to the security and resilience of the NCFs.

- Security resources are readily accessible to all. Using broadly available and easily implemented ICS cybersecurity tools and services, CI asset owners radically increase their baseline ICS cybersecurity capabilities.

CISA pursues this vision by executing our mission to partner with industry and government to understand and manage risk to our Nation's critical infrastructure. CISA will work with our partners in the ICS community toward four enduring and cross-cutting pillars that together drive

sustainable and measurable change to the Nation's ICS security risk posture:

To read more:
https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

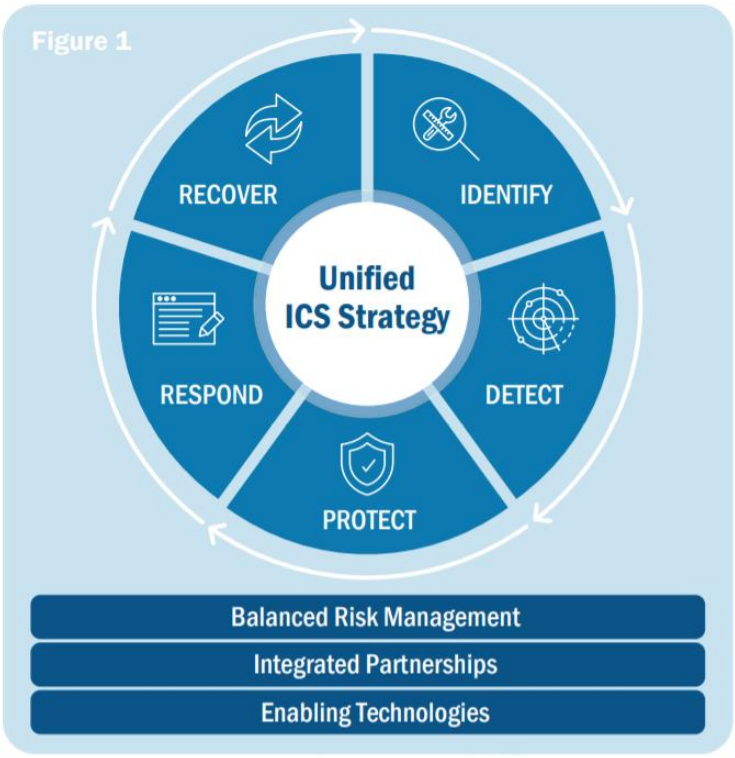


Figure 1: CISA provides full-spectrum ICS security capabilities to CI owners and operators.

Number 14

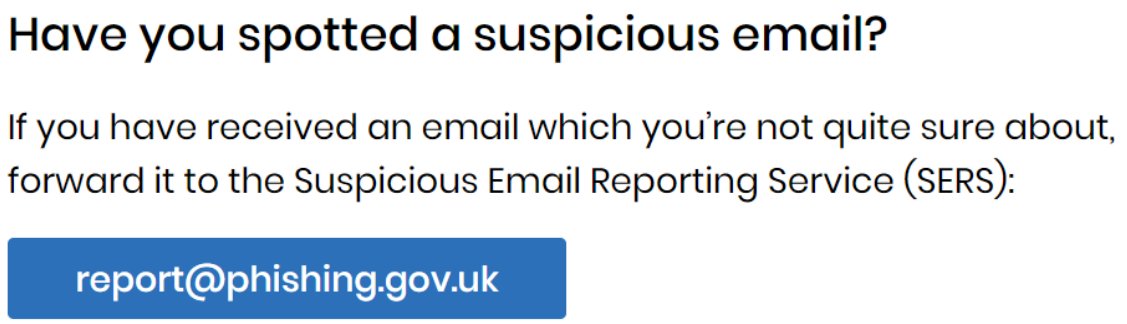
HMRC phishing scam targets passport information

A phishing scam designed to steal personal and financial details from self-employed workers is now trying to capture passport information from victims.

Details from a threat report in June explain how people are informed via SMS that they may be eligible for a tax refund. They are then redirected to a fake web page that looks like the official HMRC site (at: https://www.ncsc.gov.uk/report/weekly-threat-report-12th-june-2020)

The recent addition to this scam includes requesting passport information as part of a 'verification' process.

HMRC will never send notifications of a tax rebate or ask that personal or payment information, including passport information, be disclosed by email or text message.



You should forward any suspicious emails and details of suspicious phone calls purporting to be from HMRC to phishing@hmrc.gov.uk and any suspicious text messages to 60599.

Number 15

DHS, DOT, and HHS Issue New Guidance for Airline Industry Partners to Facilitate Safe Air Travel

The U.S. Departments of Homeland Security, Transportation, and Health and Human Services has issued joint guidance specifically for the air travel industry to better protect passengers, crew, and other airport workers from the COVID-19 pandemic during our economic recovery.

This guidance, the "Runway to Recovery: The United States Framework for Airlines and Airports to Mitigate the Public Health Risks of Coronavirus," lays out a framework for implementing public health measures in the aviation sector to minimize the risk of COVID-19 transmission.

The guidance: https://www.transportation.gov/sites/dot.gov/files/2020-07/Runway_to_Recovery_07022020.pdf

"As we reopen the economy under President Trump's Opening Up America Again guidelines, we are taking aggressive measures to protect the American people from COVID-19 as they reengage their travel plans," said Acting Secretary of Homeland Security Chad F. Wolf.

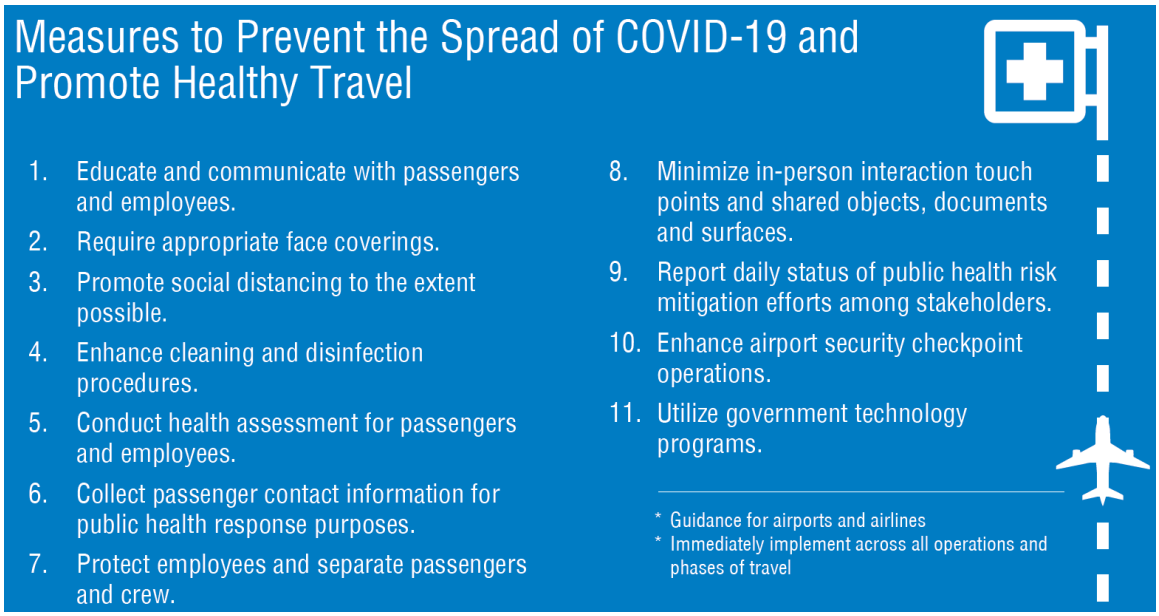
"Air travel is critical to our economic recovery and DHS has been working closely with our partners in the aviation industry throughout every step of our response to this pandemic to ensure that we are facilitating travel in a safe and secure manner."

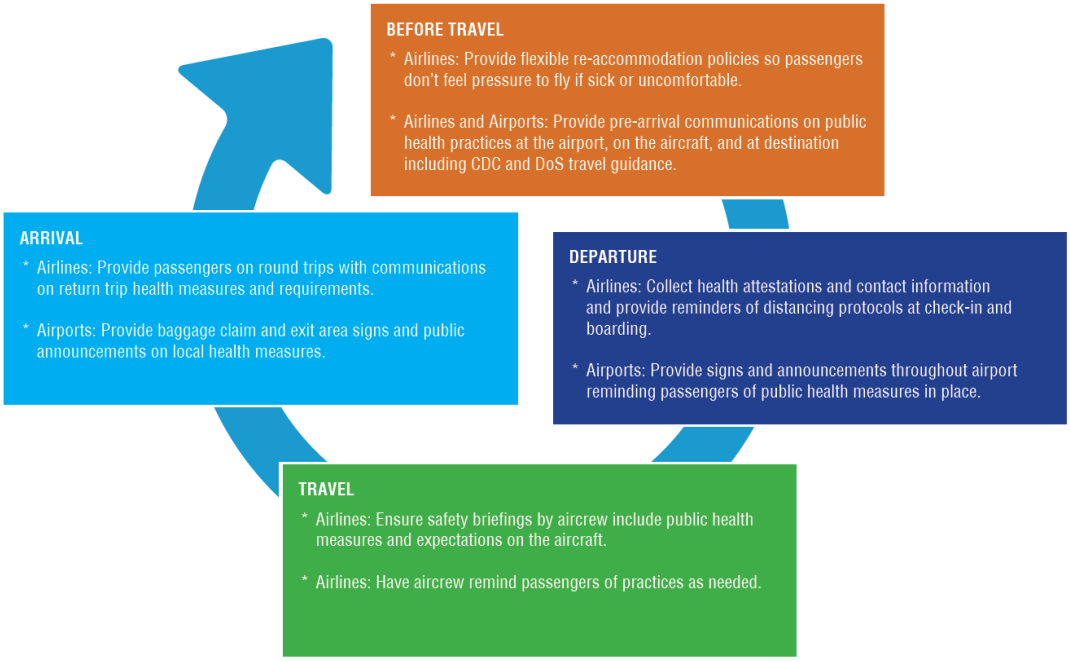
The guidelines call for public health measures to be implemented at each step in the air travel process, including before, during, and after the flight to minimize the chance for transmission of the virus. Some of the recommendations for airlines and airports include:

- Create barriers to disease transmission;
- Increase social distancing measures;
- Minimize points of contact with surfaces and people;
- Ensure cleanliness of all areas with potential for human contact;
- Know how passengers arriving on international flights can be reached if exposed to COVID 19; and
- Specialized training for aviation workers, especially airline crew.

The industry guidelines combine the expertise of three federal agencies, DHS, HHS, and DOT, each of which contributed specialized expertise on infectious diseases, public safety, and transportation operations into these guidelines.

It is important to note that the Transportation Security Administration (TSA) has already implemented many of the guidelines being proposed for the airline industry through their "Stay Healthy. Stay Secure." campaign (https://www.tsa.gov/news/press/releases/2020/06/30/tsa-administrator-pekoske-announces-stay-healthy-stay-secure). The U.S. Government will continually assess these measures, in close consultation with airlines and airports, as Americans begin to travel again.




BEFORE TRAVEL
* Airlines: Provide flexible re-accommodation policies so passengers don't feel pressure to fly if sick or uncomfortable.
* Airlines and Airports: Provide pre-arrival communications on public health practices at the airport, on the aircraft, and at destination including CDC and DoS travel guidance.
DEPARTURE
* Airlines: Collect health attestations and contact information and provide reminders of distancing protocols at check-in and boarding.
* Airports: Provide signs and announcements throughout airport reminding passengers of public health measures in place.
TRAVEL
* Airlines: Ensure safety briefings by aircrew include public health measures and expectations on the aircraft.
* Airlines: Have aircrew remind passengers of practices as needed.
ARRIVAL
* Airlines: Provide passengers on round trips with communications on return trip health measures and requirements.
* Airports: Provide baggage claim and exit area signs and public announcements on local health measures.

Number 16

Understanding fake news: A bibliographic perspective. Andrew Park, Matteo Montecchi, Cai 'Mitsu' Feng, Kirk Plangger, and Leyland Pitt

False information that appears similar to trustworthy media content, or what is commonly referred to as 'fake news', is pervasive in both traditional and digital strategic communication channels.

This paper presents a comprehensive bibliographic analysis of published academic articles related to fake news and the related concepts of 'truthiness', 'post-factuality', and 'deepfakes'.

Using the Web of Science database and VOSViewer software, papers published on these topics were extracted and analysed to identify and visualise key trends, influential authors, and journals focusing on these topics.

Articles in our dataset tend to cite authors, papers, and journals that are also within the dataset, suggesting that the conversation surrounding fake news is still relatively centralised.

Based on our findings, this paper develops a conceptual fake-news framework—derived from variations of the intention to deceive and/or harm—classifying fake news into four subtypes: mis-information, dis-information, mal-information, and non-information.

We conclude that most existing studies of fake news investigate mis-information and dis-information, thus we suggest further study of mal-information and noninformation.

This paper helps scholars, practitioners, and global policy makers who wish to understand the current state of the academic conversation related to fake news, and to determine important areas for further research.

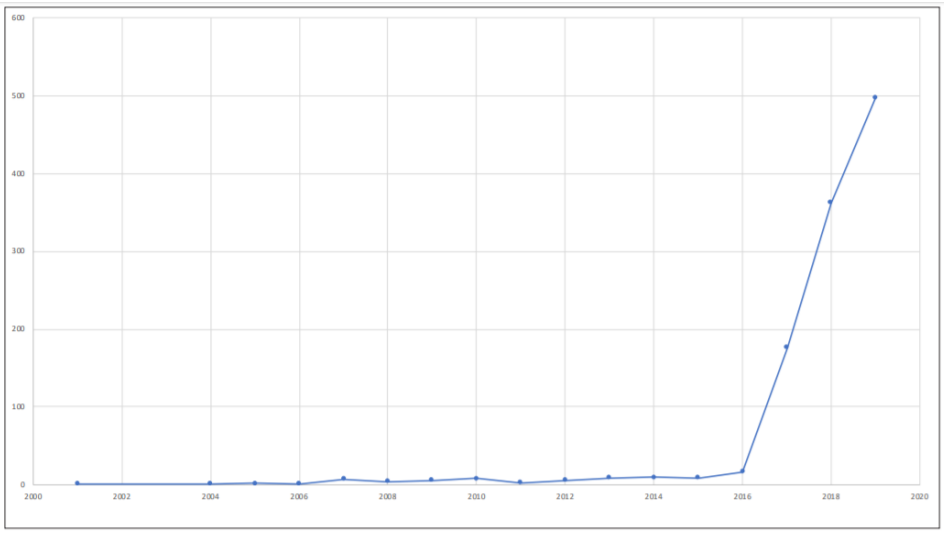


Figure 1. Number of documents feature search terms related only to fake news published – 2001 to October 2019

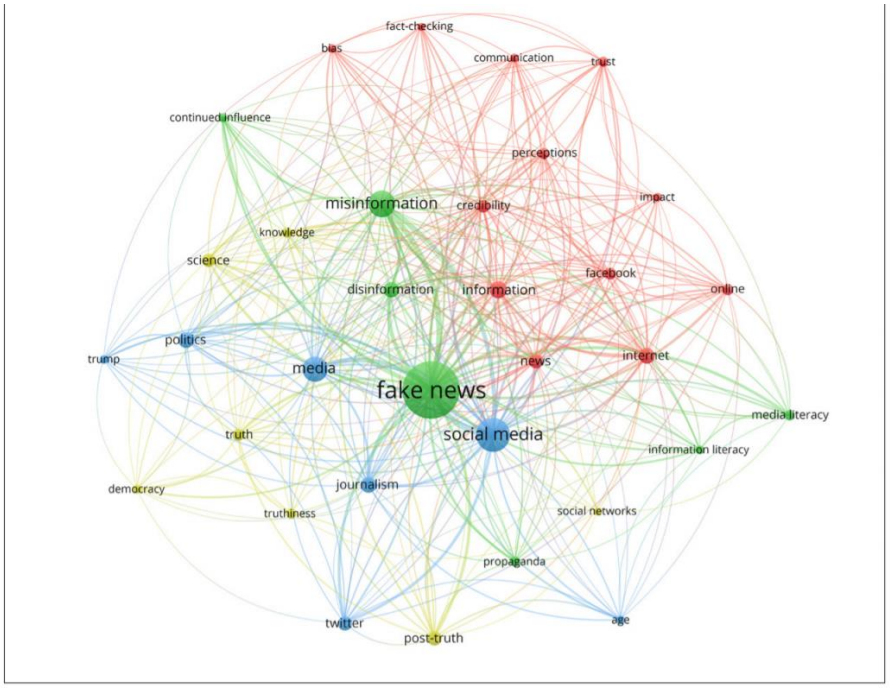


Figure 4. Map of co-occurrence of keywords (Created by VOSviewer)

You can read more at page 142/217, *Academic journal "Defence Strategic Communications" Vol 8:* https://www.stratcomcoe.org/academic-journal-defence-strategic-communications-vol-8-0

Number 17

Priorities for the Financial Action Task Force (FATF) under the German Presidency, Objectives for 2020-2022

Financial Action Task Force

It is with a profound sense of honour and responsibility that Germany takes on the first two-year Presidency of the Financial Action Task Force (FATF).

Working closely with Members and the FATF Secretariat over the next two years, the German Presidency will continue to strengthen the FATF's governance, enhance its strategic focus, increase its public visibility and reinforce its fight against money laundering, terrorist financing and the financing of weapons of mass destruction (proliferation financing).

The FATF will also prioritise work to tackle some of the great challenges facing societies around the world including the opportunities that new technology offers to strengthen AML/CFT systems through digital transformation; ethnically or racially motivated terrorism; migrant smuggling; environmental crime and illicit arms trafficking.

This will be in addition to the FATF's core work of continuing to identify and analyse money laundering and terrorist financing methods and trends, developing and refining the FATF Standards and evaluating and supporting the evaluations of countries globally.

DIGITAL TRANSFORMATION OF AML/CFT

For many years, the FATF has monitored technological developments in the financial services arena and taken action to address emerging risks, most recently by introducing new standards on virtual assets.

The German Presidency intends to build on this work, focusing on the opportunities that technology can offer, by launching an initiative to monitor risks and explore opportunities that the digital transformation of our economies and societies brings to anti-money laundering (AML) and counter-terrorist financing (CFT) efforts.

This initiative includes the following projects:

- A study of opportunities and challenges of new technology to make the implementation of AML/CFT measures by private sector and supervisors more efficient.

- A study of opportunities and challenges for operational agencies, aimed at making systems to detect and investigate money laundering (ML) and terrorist financing (TF) and understanding ML/TF risks, more efficient.

- A stocktake on data pooling and analysis, aimed at helping private sector making better use of artificial intelligence and big data analytics for AML/CFT, and increasing the efficiency of regulatory compliance, while ensuring a high level of data protection.

To accompany and guide this work on digital transformation, the FATF will create a high-level roundtable at which it aims to enter into an open - minded and informed dialogue with key groups such as data protection authorities and technology developers.

To read more:
https://www.fatf-gafi.org/publications/fatfgeneral/documents/objectives-2020-2022.html

Number 18

Annual Report on Trust Services Security Incidents in 2019

Electronic trust services are a range of services around digital signatures, digital certificates, electronic seals, timestamps, etc. which are used in electronic transactions, to make them secure.

eIDAS, an EU regulation, is the EU wide legal framework ensuring interoperability and security of these electronic trust services across the EU. One of the goals of eIDAS is to ensure that electronic transactions can have the same legal standing as traditional paper based transactions.

eIDAS is important for the European digital market because it allows businesses and citizens to work and use services across the EU. The eIDAS regulation was adopted in July 2014 and came into force in 2016.

Article 19 of eIDAS introduces mandatory security breach notification requirements for TSPs in the EU:

- Trust service providers notify the national supervisory body about security breaches with significant impact.

- National supervisory bodies inform each other and ENISA if there is cross-border impact.

- Every year national supervisory bodies send annual summary reports about the notified breaches to ENISA and the Commission.

This document, the Annual Report Trust Services Security Incidents 2019 gives an aggregated overview of these breaches, showing root causes, statistics and trends. It marks the fourth round of security incident reporting for the EU's trust services sector.

The annual summary reporting for 2019 totalled 32 incident reports. A total of 27 EU countries and 2 EFTA countries take part in annual summary reporting.

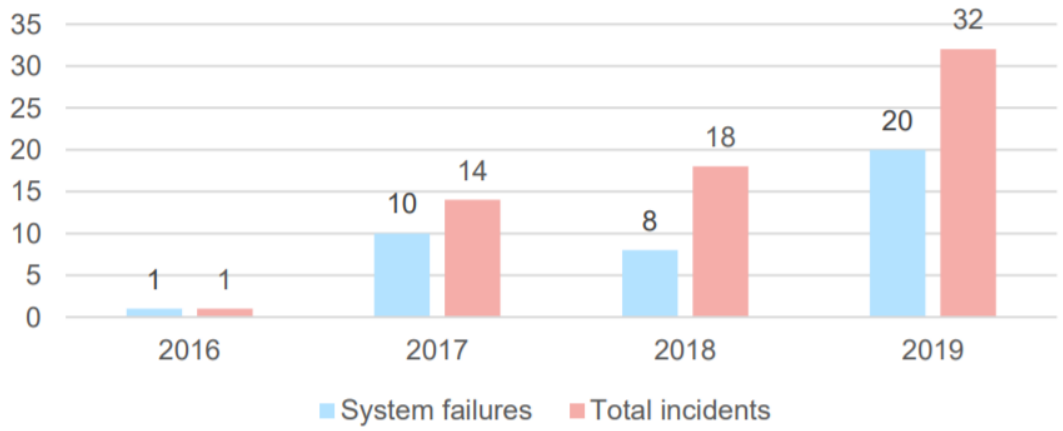
The key statistics relating to the 2019 incidents are:

- *A significant increase in notified incidents:* In 2019 the notified incidents almost doubled with respect to last year, increasing by nearly 80%. This is not necessarily a sign of security getting worse. From discussions with supervisory bodies we conclude that this increase in

notifications is a sign that trust service providers are becoming more familiar with the breach reporting process and their obligations.

- *System failures is the dominant root cause:* Most incidents (63%, 20 incidents) are caused by system failures. Over the last 4 years of annual incident reporting in this sector, system failures have consistently been the most common root cause of reported incidents. Typically, these cases are hardware failures and software bugs. Human errors account for almost 30% of incidents reported in 2019 while only 9% of incidents were flagged as malicious actions.

Figure 1: Total reported incidents vs system failures



- *Most reported incidents concerned qualified trust services:* More than three quarters of total incidents (78%) had an impact on qualified trust services. In general, non-qualified trust services are widely used. However in the set of all reported incidents, only a small number of security breaches concerns a non-qualified trust service (20%, 13 incidents). In most cases (80%, 52 incidents) the notification is done by a TSP also offering qualified services, reporting an incident which has affected both their qualified and non-qualified services

- Most of the incidents were minor. Almost a third had large impact: 31% of incidents reported in 2019 were rated as having large impact. In contrast to the two previous years, there was no incident with “very large” (disastrous) impact. We also observe a significant increase of the “minor” incidents. This is another indication that the incident reporting mechanism has become more familiar to the providers; they are reporting more incident regardless of their severity.

Figure 2: Severity of impact Trust services incidents in the EU - reported over 2016-2019

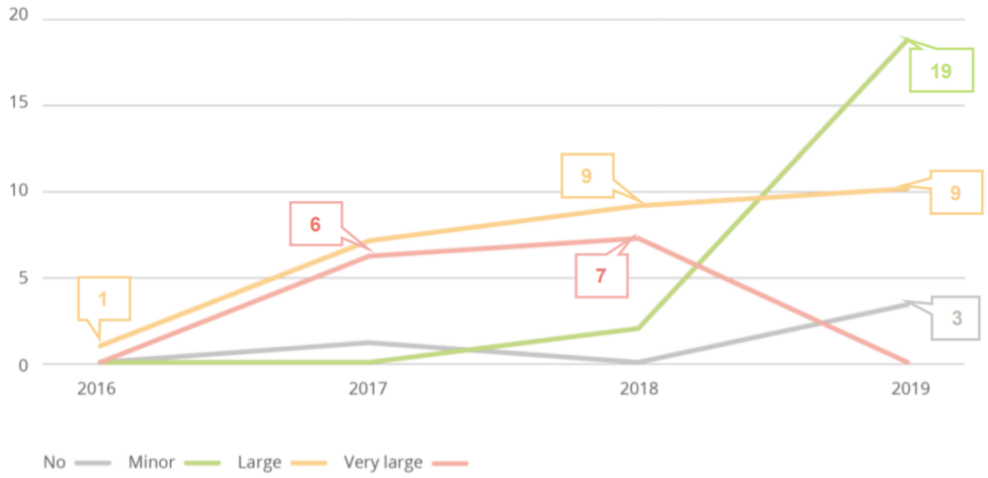
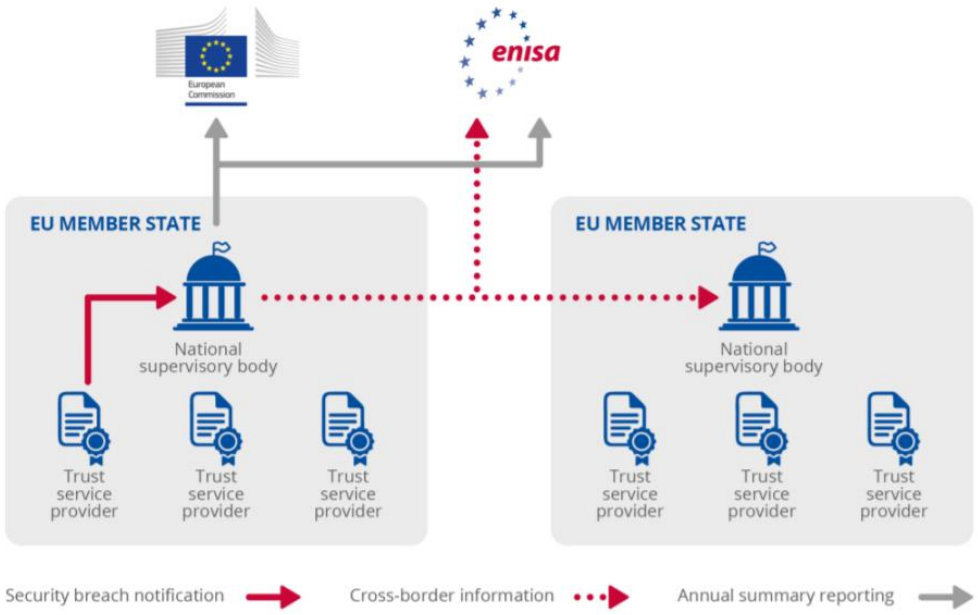


Figure 3: Incident Reporting Framework for Trust Services



To read more:
https://www.enisa.europa.eu/publications/trust-services-security-incidents-2019-annual-analysis-report

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.