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

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

Dear readers,

This time they really scared me. But this all takes place in a fictional version of 2039; it's a scenario that was played out in a tabletop exercise (TTX)—a mini-wargame— titled St. Paul Syndrome II.

On August 17, Alaskan officials reported 81 cases of an unidentified hemorrhagic fever, similar to but more contagious than the Ebola or Marburg viruses, on the Alaskan island of St. Paul in the Bering Strait.

Within a day, 24 infected people had died. The outbreak occurred two weeks after the United States was accused of sinking the Russian ship Ulana.

Americans had attempted to search Ulana because they suspected it of carrying biological warfare materials to Russia's recently solidified ally North Korea.

Four U.S. Marines died in the skirmish, as well as almost all of the Russian ship's crew.

In addition, a group of South Korean tourists—one of whom had North Korean ties—visited St. Paul three days before the first infection was discovered.

These combined events have led to an increasingly volatile situation between the United States, Russia, and multiple countries in the Asian-Pacific.

If you're thinking you missed some major breaking news, you can breathe a sigh of relief. This is just a scenario. You can read more at:

- The Los Alamos National Laboratory. It applies scientific and engineering solutions to national security and to many of the world's most difficult challenges.

- The U.S. Naval War College. It supports combat readiness, strengthens global maritime partnerships, and contributes original strategy and legal research to the US and international community.

Simulating complex war situations—from sea to space to cyber—builds analytical, strategic, and decision-making skills. Wargaming programming helps shape defense plans and policies for various commands and agencies.

Read more at Number 8 below.

We have some good news!

There is clear progress in the implementation of the national strategy for protection of Switzerland against cyber-risks (NCS).

We learned at the end of September that during its meeting on 17 August 2021, the Federal Council's Cybercommittee adopted the report on the *progress* made in implementing the 2018-2022 national strategy for the protection of Switzerland against cyber-risks (NCS).

Implementation is proceeding according to plan and is supported by the cantons, the business community and universities.

The National Cybersecurity Centre (NCSC) coordinates the implementation of the NCS and prepares an annual report on the implementation status on behalf of the NCS Steering Committee.

The report covers the current implementation status as of the second quarter of 2021. Of a total of 275 milestones, 154 have been implemented and of the 29 measures, six have already been completed.

Further development of organisational structures

A key element of the NCS implementation is the development of the organisational structures in the Confederation.

The areas of cybersecurity (NCSC), cyberdefence (DDPS) and cyberlaw enforcement (FDJP) have undergone further strategic and organisational development.

The national contact point for cyber incidents became operational on 1 January 2020 and processed 10,834 incidents reported by companies and the general public in its first year.

In line with the overarching NCS, the Federal Department of Defence, Civil Protection and Sport (DDPS) defined the guidelines for the strategic orientation of cyberdefence for the period 2021 to 2024 in the DDPS cyber strategy.

In the area of law enforcement, the organisation and financing of the Network for Investigative Support in the Fight against Cybercrime (NEDIK) was regulated in an administrative agreement.

The network pools specialised resources at the national level to efficiently combat digital crime and makes an important contribution to prevention.

Parallel to this, implementation work is underway in which the cantons, the business community and universities are involved to a significant degree.

Development of vulnerability management and introduction of security labels

One focus of the NCS is the development of vulnerability management at the NCSC. In the future, bug bounty programmes (use of ethical hackers) are to be established for the entire Federal Administration.

In the context of the SwissCovid app and the Covid certificate, the NCSC conducted two public security tests (PSTs) and was thus able to make its expert services available to the Federal Administration.

For the PST related to the Covid certificate, the NCSC collaborated for the first time with the National Test Institute for Cyber Security (NTC), which was founded last year on the initiative of the Canton of Zug.

The reporting period also saw the launch of the initiative to create an independent seal of quality for IT services.

The aim is to increase the level of quality of services and thus the cyber-resilience of companies, and to strengthen confidence in Switzerland's digital security.

In order to promote cybersecurity among communes in particular, the "cyber-safe.ch" pilot project was also launched with the support of the NCS, the Swiss Security Network (SSN) and the Association of Swiss Communes (ASC). Currently, around fifteen Swiss communes are being tested and informed about any measures they may need to take before they could be awarded the "cyber-safe.ch" label.

More (in German) at:
https://www.ncsc.admin.ch/ncsc/de/home/strategie/berichte-und-studien.html

Inhaltsverzeichnis

The emergence of large technology firms (big techs) represents a major source of disruption to the financial system and the economy.

These are the first words in the new paper with title "*Big tech regulation: what is going on?"* (Financial Stability Institute (FSI), Insights on policy implementation No 36).

The FSI is one of the bodies hosted by the Bank of International Settlements at its headquarters in Basel, Switzerland.

The paper continues: "Big techs have expanded the available range of financial products and services, often with enhanced customer experience.

However, the ease and speed with which these companies can scale up their activities and expand into finance may generate pronounced concentration dynamics.

This could significantly affect the adequate functioning of the financial system and may damage market contestability and eventually increase operational vulnerabilities due to the excessive reliance of market players on the services provided by big techs."

The paper continues: "*Different jurisdictions have moved to adjust their policy frameworks to cope with the risks presented by big techs.*

In particular, a number of policy initiatives have emerged in China, the European Union (EU) and the United States over the last few years in the areas of competition, data protection and data-sharing, operational resilience, conduct of business and financial stability.

These initiatives generally seek to achieve a balance between addressing the different risks posed by big techs and preserving the benefits they bring in terms of market efficiency and financial inclusion."

To achieve this balance is not going to be easy, especially when China becomes an example. But as Albert Einstein has said, *life is like riding a bicycle. To keep your balance, you must keep moving*.

There are some interesting parts in the paper, where China looks more advanced than the States. For example, I was surprised (a polite expression) with the following Table, with sources including "authors' compilation":

Data protection and data-sharing approaches in the EU, US and China — Table 2

	EU	US	China
Data protection			
Collection and use of personal data			
Of which: Lawfulness, fairness and transparency	√	√	√
Purpose specification	√	*	√
Security	√	√	√
Users' data rights			
Of which: Consent and access	√	*	√
Rectification and deletion	√	*	√
Data portability	√	*	√
Data-sharing			
Open banking			
*Approach: prescriptive, facilitative**, market-driven****	Prescriptive	Market	Market

Legend: Comprehensive | Partial | Early stages

* While there is no federal law addressing these elements at present, they are subject to ongoing debate.

** Under a facilitative approach, jurisdictions issue guidance and recommended standards, and release open API standards and technical specifications.

*** No explicit rules or guidance that either require banks or prohibit them to share customer-permissioned data with third parties.

Sources: BCBS (2019) and authors' compilation.

According to the paper, the "proposed data protection frameworks in the US and the finalised framework in China show a high degree of alignment with the EU's GDPR".

We also read: "Chinese authorities have engaged in a number of ex post supervisory actions against big techs. The initial public offering (IPO) of Ant Group rapidly unravelled after regulators blocked it for not complying with listing criteria and disclosure requirements.

In April 2021, the group was forced to restructure and its affiliate, Alibaba, was fined RMB 18.23 billion ($2.8 billion) – the biggest antitrust fine levied in China to date. Additionally, regulators ordered 34 Chinese internet companies to undergo rectification of their business models for potential anticompetitive practices.

A week later, the China Securities Regulatory Commission (CSRC) issued new rules aimed at restricting the listing of fintech and "model innovation enterprises" on the Shanghai Stock Exchange Science and Technology Innovation Board."

I am not sure I understand perfectly what is going on. It looks like China is becoming a role model in regulation worthy of imitation. I am surprised, and I disagree.

Read more at number 2 below.

We have *another* definition for the term *vulnerability*.

According to the Financial Stability Board, a vulnerability is a property of the financial system that:

(i) reflects the accumulation of imbalances,

(ii) may increase the likelihood of a shock, and

(iii) when acted upon by a shock, may lead to systemic disruption.

According to the National Institute of Science and Technology (NIST) and the US Committee on National Security Systems (CNSS), *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

According to the National Industrial Security Program (NISP) that was established by Executive Order 12829, *Acute Vulnerability* is the vulnerability that puts classified information at imminent risk of loss or compromise, or that has already resulted in the compromise of classified information. Acute vulnerabilities require immediate corrective action.

Critical Vulnerability is an instance of National Industrial Security Program Operating Manual (NISPOM) non-compliance vulnerability that is serious, or that may foreseeably place classified information at risk or in danger of loss or compromise.

According to the Department of Homeland Security (DHS) Risk Lexicon, *vulnerability* is a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

The DHS Risk Lexicon gives an extended definition too: *Vulnerability* is a characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation.

In all my professional life, I try to build a *culture of vulnerability awareness* for organizations and companies. Every time I find another different definition of the word vulnerability, I know that we fight an uphill battle, and we have to struggle against very unfavourable circumstances.

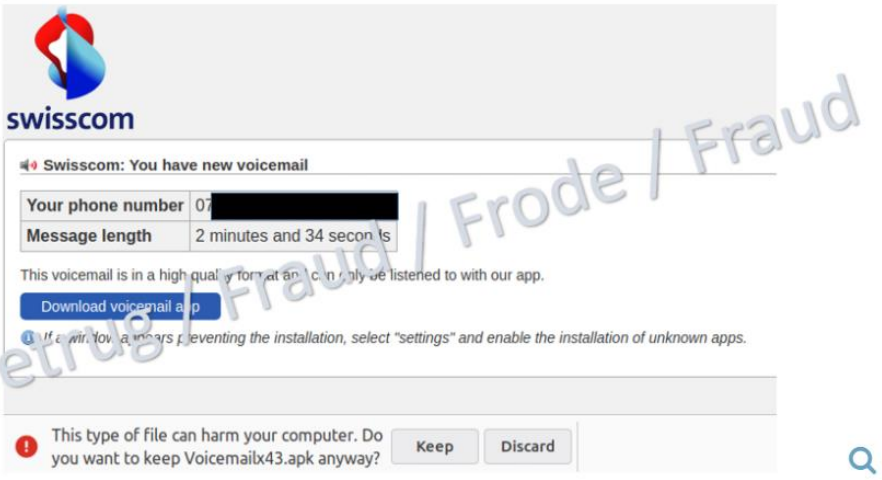
Read more at number 9 below.

Text message with alleged voicemail leads to malware.

The Swiss NCSC has received over a hundred reports of a text message asking the recipient to listen to a voicemail at the link provided.

The website that opened after clicking on the link appeared at first glance to be a page of the corresponding mobile phone provider (in this case, Swisscom or Sunrise) on which the voicemail data could be seen and the voicemail could be downloaded.

At second glance, however, it becomes apparent that an Android app must first be downloaded in order to listen to the voicemail. As could be expected, this was malware, which then infiltrates the mobile phone.



Download page for the Trojan disguised as a voicemail app

The FluBot malware is specialised in stealing text messages from Android mobile phones, among other things. The aim is to find one-time passwords for banking applications in the stolen text messages.

The data thus obtained enables the attackers to also abuse applications with **two-factor** protection in cases where the second factor is sent via text message.

The attackers can log on to the bank with user names and passwords which they have usually stolen beforehand, and can then also use the malware to receive the text message verification code.

The FluBot malware not only steals data; it can also suppress the notification function of the infected smartphone. This means that users do not even notice that the bank has sent them an authentication text message.

This malware first appeared in Switzerland in June 2021 and the NCSC received several reports about it at that time. The malware itself hides deep in the infected operating system and it is almost impossible to uninstall it completely. Restoring the factory settings for the operating system is the only reliable way of getting rid of the malware.

Even though this malware only attacks Android devices, users of devices with the iOS operating system must also be careful and should not click on any links in text messages.

- Do not install any software that is offered outside the operating systems' official stores.

- In particular, you should not install any software received via a link in a text message or other messenger service (WhatsApp, Telegram, etc.).

- If you nevertheless installed such software, you should have the device checked by a specialist and should not carry out any banking transactions or online shopping. Do not enter any passwords either.

- Restoring the factory settings on the infected device is almost the only way to remove the malware.

Online reviews are of interest for blackmailers, too.

Such reviews are very helpful for customers when they want to find out in advance about an online store, a shop or a restaurant.

However, since such reviews also influence customer behaviour, it is clear that there are also individual advertisers who try to manipulate such reviews in their favour or to the competitor's disadvantage.

Companies specialised in "optimising" such reviews also exist.

However, a case that was reported to the Swiss NCSC shows that it is possible to be even bolder. An (unjustified) bad review was posted for a company on a review portal. It was written in such detail that the readers believed it to be authentic. Shortly after the review was published, someone contacted the company and offered a service to remove the bad review.

The chronological sequence would appear to suggest that the two events are connected and that this is a blackmailing scam. Even if this is not the case, such offers are usually fraudulent and promise more than they deliver.

- Be sceptical if someone offers you an unsolicited service by phone or email.

- In such a case, be sure to note down all available information, such as the exact time, the number of the person calling and other details concerning the contact. This information can help you defend yourself against unjustified reviews.

- As soon as you notice a fake review, inform the operators of the review portal.

Welcome to our monthly newsletter.

Best regards,

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

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

Number 1 (Page 14)

Selecting and Hardening Remote Access VPN Solutions

Number 2 (Page 16)

FSI Insights on policy implementation No 36

Big tech regulation: what is going on?

By Juan Carlos Crisanto, Johannes Ehrentraud, Aidan Lawson and Fernando Restoy

Number 3 (Page 19)

Moving forward in securing Online Trust via the Digital Wallets

The 2021 Trust Service Forum allows stakeholder communities to engage in open discussions on securing trust services online and on the future of the EU Digital Identity Framework.

Number 4 (Page 22)

Methodology for a Sectoral Cybersecurity Assessment

Number 5 (Page 26)

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Number 6 (Page 28)

Disrupting Exploitable Patterns in Software to Make Systems Safer

Program pushes secure system design by developing ways to stop cyber attackers' from executing unintended computations on critical systems

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 7 (Page 30)

A Smart Use for Doping: Implanted Atoms Create Unique Electrical IDs That Distinguish Bona Fide Devices From Forgeries

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

Number 8 (Page 34)

Simulating wartime decisions helps prepare for the real thing

Los Alamos NATIONAL LABORATORY

Number 9 (Page 41)

FSB Financial Stability Surveillance Framework

FSB FINANCIAL STABILITY BOARD

Number 10 (Page 44)

Solving Defense Optimization Problems with Increased Computational Efficiency

Program aims to develop Quantum-Inspired solvers to tackle complex defense optimization problems with 500X performance improvements

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 11 (Page 46)

Attackers look to deploy attacks through the software supply chain

National Cyber Security Centre

Number 12 (Page 49)

Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms

cybereason

Number 13 (Page 50)

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

THE UNITED STATES DEPARTMENT of JUSTICE

Number 14 (Page 52)

Agency Actions Needed to Address Foreign Influence

US Government Accountability Office (GAO) - Testimony Before the Subcommittees on Investigations and Oversight and Research and Technology Committee on Science, Space, and Technology House of Representatives, Statement of Candice N. Wright, Director, Science, Technology Assessment, and Analytics.

GAO

Number 15 (Page 56)

New Android malware allows attackers to monitor all user activity on infected devices

National Cyber Security Centre

Number 16 (Page 58)

Episode 50: The Photonicist

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Selecting and Hardening Remote Access VPN Solutions

National Security Agency | Cybersecurity and Infrastructure Security Agency | Cybersecurity Information Sheet

Virtual Private Networks (VPNs) allow users to remotely connect to a corporate network via a secure tunnel.

Through this tunnel, users can take advantage of the internal services and protections normally offered to on-site users, such as email/collaboration tools, sensitive document repositories, and perimeter firewalls and gateways.

Because remote access VPN servers are entry points into protected networks, they are targets for adversaries.

This joint NSA-CISA information sheet provides guidance on:

- Selecting standards-based VPNs from reputable vendors that have a proven track record of quickly remediating known vulnerabilities and following best practices for using strong authentication credentials.

- Hardening the VPN against compromise by reducing the VPN server's attack surface through:

Configuring strong cryptography and authentication

Running only strictly necessary features

Protecting and monitoring access to and from the VPN

Active Exploitation

Multiple nation-state Advanced Persistent Threat (APT) actors have exploited public Common Vulnerabilities and Exposures (CVEs) to compromise vulnerable VPN devices.

In some cases, exploit code is freely available online. Exploitation of these public CVEs can enable a malicious actor to perform:

- Credential harvesting
- Remote code execution of arbitrary code on the VPN device
- Cryptographic weakening of encrypted traffic sessions
- Hijacking of encrypted traffic sessions
- Arbitrary reads of sensitive data (e.g., configurations, credentials, keys) from the device

These effects usually lead to further malicious access through the VPN, resulting in large-scale compromise of the corporate network or identity infrastructure and sometimes of separate services as well.

To read more: https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

Number 2

FSI Insights on policy implementation No 36

Big tech regulation: what is going on?

By Juan Carlos Crisanto, Johannes Ehrentraud, Aidan Lawson and Fernando Restoy

BIS

The emergence of large technology firms (big techs) represents a major source of disruption to the financial system and the economy.

Big techs have expanded the available range of financial products and services, often with enhanced customer experience. However, the ease and speed with which these companies can scale up their activities and expand into finance may generate pronounced concentration dynamics.

This could significantly affect the adequate functioning of the financial system and may damage market contestability and eventually increase operational vulnerabilities due to the excessive reliance of market players on the services provided by big techs.

Different jurisdictions have moved to adjust their policy frameworks to cope with the risks presented by big techs.

In particular, a number of policy initiatives have emerged in China, the European Union (EU) and the United States over the last few years in the areas of competition, data protection and data-sharing, operational resilience, conduct of business and financial stability.

These initiatives generally seek to achieve a balance between addressing the different risks posed by big techs and preserving the benefits they bring in terms of market efficiency and financial inclusion.

Thus far, competition has been the policy area where the most initiatives have been conducted and a paradigm shift is emerging.

Given the large potential for big techs to abuse their technological and data superiority to quickly dominate different market segments and adopt anticompetitive practices, preserving market contestability has become a top priority for authorities in China, the EU and the US.

Competition policy proposals include not only the augmentation of traditional ex post enforcement tools but also the creation of new big tech-specific ex ante regulatory regimes.

A number of data protection and data-sharing initiatives have been proposed.

Policy initiatives across the three jurisdictions place special emphasis on personal data use and data protection.

Moreover, there are relevant initiatives, particularly in China and the EU, with respect to users' data portability.

This, together with emerging policy and market developments on data-sharing, seems to be paving the way to a generalised use of personal data for the provision of financial services by different types of entities.

Policy initiatives are addressing the operational resilience of big tech firms.

These typically apply to big techs either as providers of financial services2 or as third-party service providers of financial firms.

The operational resilience requirements in both cases intend to capture all sources of operational risk (in particular, information and communication technology risks) and expect adoption of sound risk management practices, swift response in case of disruption and continuity of critical services.

Some jurisdictions have taken meaningful policy efforts to address potential conduct issues and financial stability challenges but they do not follow an homogeneous pattern.

A key development in the conduct of business area is the EU's proposed Digital Services Act (DSA). This establishes extensive requirements for very large online platforms connected with the functioning and use of their services.

As such, the DSA represents a comprehensive effort to deal with how big techs treat their customers and the information they receive.

Regarding financial stability, the main regulatory development is the China financial holding company (FHC) regime.

This requires all entities holding two or more types of financial institutions to be structured and licenced as FHCs (if size thresholds or other conditions are met).

This effectively mandated big techs to reorganise their financial business and represents a novel entity-based regulatory approach that entails a comprehensive oversight of the activities performed by big techs through all their financial subsidiaries.

Additional regulatory responses might be needed to comprehensively address big tech risks and achieve policy consistency at the international level.

Recent initiatives in China, the EU and the US constitute important steps in addressing risks posed by big techs. However, if big techs continue to gain prominence in the financial system, additional policy responses might be necessary.

It is also very likely that new policy actions will largely need to follow an entity-based approach and require close cooperation between competition, data and financial authorities. Moreover, given the cross-border scope of big tech activities, enhanced international regulatory cooperation is essential.

To read more: https://www.bis.org/fsi/publ/insights36.pdf

Number 3

Moving forward in securing Online Trust via the Digital Wallets

The 2021 Trust Service Forum allows stakeholder communities to engage in open discussions on securing trust services online and on the future of the EU Digital Identity Framework.

Electronic signatures, electronic seals and other online trust services have become a staple in the life of many Europeans.

In light of the COVID-19 pandemic, a key aspect to ensure a viable business model for qualified trust service providers was an increasing usage of online trusted services among European citizens, businesses and public administrations in an online mode.

This new reality across the EU has highlighted the security concerns of remote identification and authentication processes.

The necessity for a new framework for EU digital identity became apparent.

The European Commission presented last June a new framework for the EU digital identity by offering to citizens and businesses the digital wallets that will allow EU citizens to retain their documents such as national digital identities, licences, diplomas and bank credentials securely in their smartphone.

The wallet should also allow them to log in to online services across the EU and to electronically sign their documents.

On September 21st, the European Union Agency for Cybersecurity (ENISA) in collaboration with the European Commission delivered the 7th consecutive ‘’Trust Service Forum’’.

It attracted over to 1000 participants and brought more than forty experts, service providers, conformity assessment, supervisory bodies and national authorities together, to discuss the online trust market and its emerging issues under the European Commission’s Regulation 910/2014, on electronic identification and trusted services for electronic transactions in the internal market (eIDAS Regulation).

On 22nd September, D-TRUST in cooperation with TÜViT and the European School of Management and Technology (ESMT), held the 13th CA-Day.

Both conferences were held in a hybrid format, with physical presence for the panellists at the ESMT premises in Berlin and virtually for the participants.

The forum was jointly opened by the European Commission's Director of Digital Society, Trust and Cybersecurity Ms. Lorena Boix Alonso and ENISA's Head of Policy Development and Implementation Unit Mr. Evangelos Ouzounis and it was consisted of three main distinct blocks.

In the first one, the panellists discussed the new ''EU Digital Identity Framework- bringing opportunity to wider use of online trust solutions across the EU".

The concept of decentralised online identity, that gives back control to users over their personal data and leverages the use of an identity wallet, was additionally discussed.

Second block focused on certification and standardisation efforts and the third one on the trust service market – current state of play, opportunities and outlook.

Panellists had also the opportunity to further elaborate on the upcoming revisions of the eIDAS Regulation that proposes to further extend its application to the private sector and to promote trusted digital identities across the EU.

Background

The Trust Services Forum acts as a platform for participants to share their good practices on the implementation of trust services; review the standards, implementing acts and technical guidelines within the eIDAS; and discuss strategies to promote the adoption of qualified trust services.

The EU Agency for Cybersecurity supports the Commission on the implementation of the eIDAS by providing security recommendations for the implementation of trust services, mapping technical and regulatory requirements, promoting the deployment of qualified trust services in Europe and raising awareness among users on securing their e-transactions.

Under the EU Cybersecurity Act of 2019, the Agency gained an extended mandate to explore the area of electronic identification (eIDs) included in the regulation.

EU's Digital Wallet's proposal

The Commission on the 3rd June 2021 proposed a framework for a European Digital Identity which will be available to all EU citizens, residents, and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone.

They will be able to access online services with their national digital identification, which will be recognised throughout Europe. Large platforms are proposed to accept the use of European Digital Identity wallets upon request of the user, for example to prove their age. Use of the European Digital Identity wallet will always be at the choice of the user.

The new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share.

Number 4

Methodology for a Sectoral Cybersecurity Assessment

Cybersecurity certification under the European Union Cybersecurity Act (CSA) is intended to increase trust and security for European consumers and businesses and help to achieve a genuine digital single market.

This requires that all relevant levels of the ICT market, from sectoral ICT services and systems via ICT infrastructures to ICT products and ICT processes, will be addressed and that the related cybersecurity certification schemes are well accepted by the market.

The CSA stipulates specific requirements, which target efficiency and coherence between schemes of the CSA's cybersecurity certification framework.

These requirements include:

– The security and assurance requirements for ICT services, ICT processes or ICT products should be defined based on the risk associated with their intended use.

– Assurance levels should be implemented consistently across schemes.

– Support for security-by-design.

The methodology for sectoral cybersecurity assessments described in this document (hereinafter called SCSA Methodology) addresses these objectives in the context of drafting sectoral cybersecurity certification schemes, which address ICT services in individual market sectors.

It is designed to be used as a preparatory step for the definition of a candidate scheme involving sectoral stakeholders.

A basic principle of the proposed methodology is to establish a sound understanding of the sectoral ICT services and system as a foundation for all other functions:

– A cybersecurity assessment at the sectoral level will provide information about the objectives of the sectoral stakeholders and will identify the primary assets and related risks.

As an enhancement of the typical risk assessment procedure, a 'deep dive' to gain detailed information about the intended use of relevant subsystems, products or services will be conducted.

In addition, cyberthreat intelligence (CTI) will be employed to provide information on potential attackers, their motivation and capabilities.

This adds an important parameter to the risk analysis and contributes to the information needed to assign security and assurance requirements to ICT subsystems, ICT products or ICT services based on risk.

– The SCSA Methodology provides the option to integrate sectoral, product, process and potentially also ISMS-based cybersecurity certification schemes.

It offers a concept of internal risk, security and assurance reference levels.

If these are commonly used, they will support consistency in the definition of risk, security and assurance across schemes.

The SCSA Methodology is designed to address a wide range of certification schemes, beyond Common Criteria or other ISO/IEC 15408-based schemes.

Optionally other types of certification schemes can be integrated in order to establish consistency across the various types of schemes that support the proposed methodology.

– A link between the ISO/IEC 270xx series of standards and ISO/IEC 15408 is needed to allow information to be exchanged between the outcome of risk assessment and the specification of security and assurance of products.

The expert team has developed a mapping approach that addresses existing divergences of terminology between these standards and allows the transfer of the information that is required.

– The introduction of a common, scalable approach to risk-based security and assurance supports the definition of scaled controls.

These controls are associated with clear security levels which are defined in accordance with their ability to treat risk and protect against known attack potentials.

The expert team has drafted a sample list of scaled controls and has described how these controls can be used in a coordinated way.

Based on these properties and functions, the SCSA Methodology has the potential to fully support the aforementioned requirements stipulated by the CSA and to promote the market acceptance of cybersecurity certification in the following ways:

– The SCSA Methodology supports the identification of risk associated with the intended use of ICT systems, ICT services and ICT processes at any level of the sectoral architecture.

In applying the methodology, relevant stakeholders will be responsible for the identification of risks and they will be involved in the definition of security and assurance requirements.

This will allow them to balance their view of risks against the investment needed to mitigate these risks by introducing appropriate levels of security and assurance.

It can be expected that this transparent, cooperative approach will contribute significantly to the market acceptance of schemes under the CSA.

– As required by the CSA, consistency in the implementation of assurance levels can be achieved across schemes. This will allow the re-use of certificates issued by one scheme in other schemes, thus providing an important benefit both to the business interests of product and infrastructure service providers and to their customers.

At the same time, the methodology's approach to consistency is also flexible enough to support the integration of new types of cybersecurity certification schemes, which may emerge as a result of specific requirements from different markets.

– Introducing a common concept for security levels facilitates the definition of controls which can be commonly used across participating schemes. This provides a sound basis for the introduction of libraries of such controls.

The availability of those could significantly promote the introduction of security-by-design, as well as the implementation of defined security levels in ICT products, ICT processes and also in ICT systems.

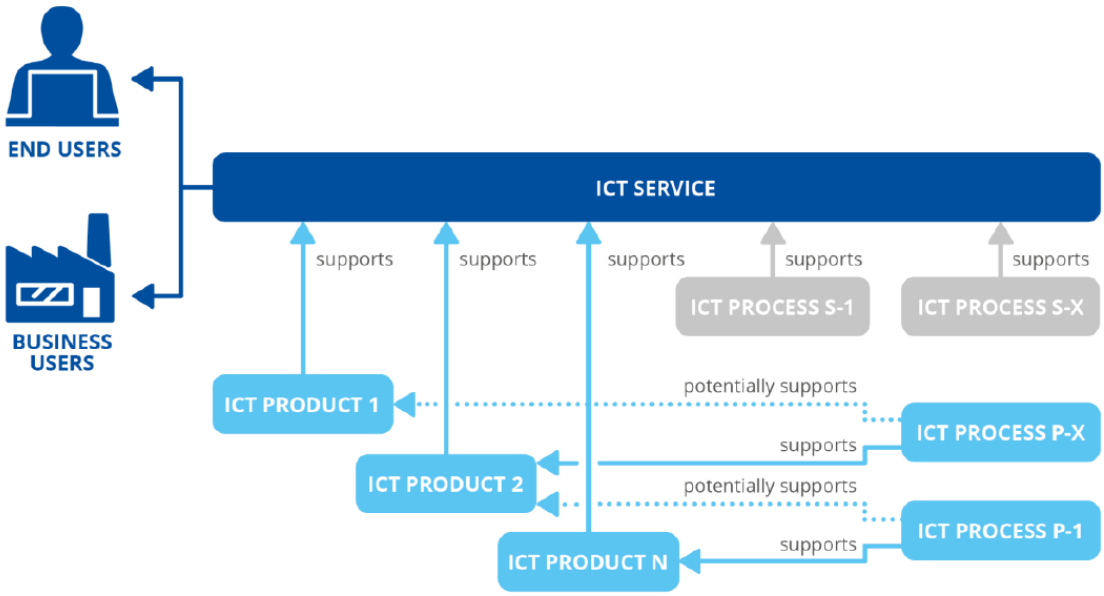
Applying the SCSA Methodology will generate sound information about the sectoral system and defined relationships between the stakeholders involved, which may enable additional tangible benefits, including:

– Product and service providers will benefit from reliable information about the intended use of their products and services, as well as sectoral

security and assurance requirements. This will allow them to optimize their products and their market reach.

– The defined relationships between risk, security and assurance proposed by this methodology support the definition of horizontal products and services, which can serve various sectors.

Figure 1: CSA-defined elements and their relations



To read more: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment

Number 5

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year.

These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim.

The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors.

Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

Cyber attacks targeting networks used by emergency services personnel can delay access to real-time digital information, increasing safety risks to first responders and could endanger the public who rely on calls for service to not be delayed.

Loss of access to law enforcement networks may impede investigative capabilities and create prosecution challenges.

Targeting healthcare networks can delay access to vital information, potentially affecting care and treatment of patients including cancellation of procedures, rerouting to unaffected facilities, and compromise of Protected Health Information.

Technical Details

Conti actors gain unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials. Conti weaponizes Word documents with embedded Powershell scripts, initially staging Cobalt Strike via the Word documents and then dropping Emotet onto the network, giving the actor access to deploy ransomware.

Actors are observed inside the victim network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery.

The actors first use tools already available on the network, and then add tools as needed, such as Windows Sysinternals and Mimikatz to escalate privileges and move laterally through the network before exfiltrating and encrypting data.

In some cases where additional resources are needed, the actors also use Trickbot. Once Conti actors deploy the ransomware, they may stay in the network and beacon out using Anchor DNS.

If the victim does not respond to the ransom demands two to eight days after the ransomware deployment, Conti actors often call the victim using single-use Voice Over Internet Protocol (VOIP) numbers. The actors may also communicate with the victim using ProtonMail, and in some instances victims have negotiated a reduced ransom.

To read more: https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

Number 6

Disrupting Exploitable Patterns in Software to Make Systems Safer

Program pushes secure system design by developing ways to stop cyber attackers' from executing unintended computations on critical systems

While much attention is paid to detecting and remedying flaws or vulnerabilities in software, the way a system is designed can also create large opportunities for attackers.

System designers primarily focus on ensuring a program is adept at executing a specific task, focusing on how a design can best support intended features and behaviors and on how they will be implemented within the design.

Attackers have also discovered that these design structures and implementation behaviors can be repurposed for their own malicious purposes.

Unexpected – or emergent – behaviors that these features could exhibit are not often taken into consideration at the time of design.

As a result, attackers often find that they can generate emergent behaviors by using what's already built into a system, providing a way to exploit flaws that are several layers down.

In other words, systems are unknowingly being designed in ways that support adversarial programmability and combinations of features and unprotected abstractions.

These amount to embedded exploit execution engines – creating what is colloquially known as "weird machines."

"When it comes to exploits, the common thinking is that there is a flaw in the program and then there is a crafted input that can trigger the flaw resulting in the program doing something it shouldn't like crashing or granting privileges to an attacker," said Sergey Bratus, a program manager in DARPA's Information Innovation Office (I2O).

"Today, the reality is somewhat different as those existing flaws aren't immediately exposed, so an attacker needs help getting to them. This help is unwittingly provided by the system's own features and design. Attackers are able to make use of these features and force them to operate in ways they were never intended to."

This challenge becomes increasingly problematic when observing a class of systems that rely on similar features. When an attacker discovers an exploit on one system, this can give a big hint on how to find similar exploits for other systems that have been developed independently by different vendors but make use of similar mechanisms.

This creates persistent exploitable patterns that can be used across a whole host of programs.

The Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program seeks to give developers a way to understand emergent behaviors and thereby create opportunity to choose abstractions and implementations that limit an attacker's ability to reuse them for malicious purposes, thus stopping the unintentional creation of weird machines.

HARDEN will explore novel theories and approaches and develop practical tools to anticipate, isolate, and mitigate emergent behaviors in computing systems throughout the entire software development lifecycle (SDLC).

Notably, the program aims to create mitigation approaches that go well beyond patching. At present, patches tend to only address a particular exploit and do not disrupt the underlying exploit execution engine residing at the design-level.

HARDEN will also focus on validating the generated approaches by applying broad theories and generic tools to concrete technological use cases of general-purpose integrated software systems.

Potential evaluation systems include the Unified Extended Firmware Interface (UEFI) architecture and boot-time chain of trust, as well as integrated software systems from the Air Force and Navy domains, such as pilots' tablets.

"There are many ways to theorize about addressing these challenges, but the test of the theory is how it will apply to an actual integrated system that we base trust on, or want to base trust on. We want to ensure we're creating models that will be of actual use to critical defense systems," noted Bratus.

To learn more:
https://sam.gov/opp/76520ba476714e04a6349578a763120c/view

Number 7

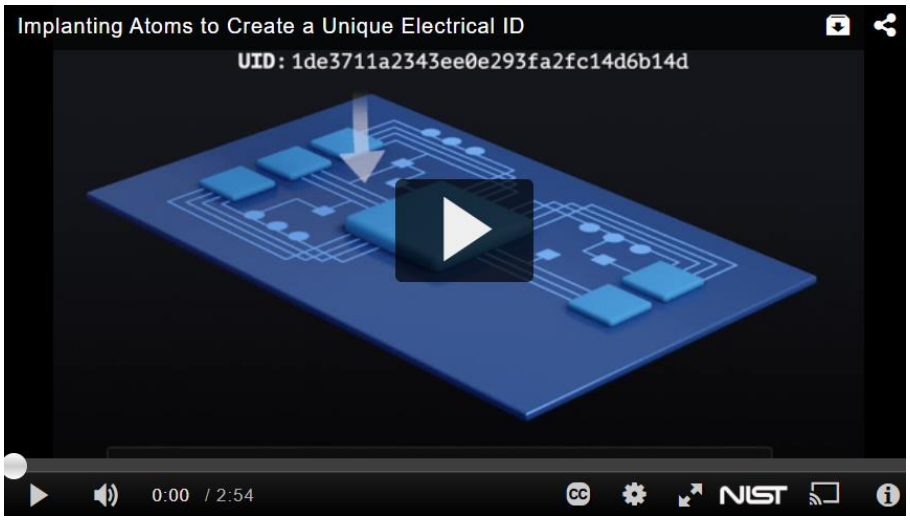
A Smart Use for Doping: Implanted Atoms Create Unique Electrical IDs That Distinguish Bona Fide Devices From Forgeries

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

If someone sells you a luxury handbag from Paris, France, but it turns out be a forgery from Paris, Texas, the counterfeit item might cost you a thousand bucks and the crook could wind up in jail. But if a counterfeit electronic device gets installed in a car, it could cost passengers or the driver their lives.

Without new security measures, the interconnected wireless technologies, digital electronics and micromechanical electronic systems that make up the Internet of Things are vulnerable to forgeries and tampering that could cause entire telecommunication networks to fail. In 2017, sales of counterfeit products of all sorts — from electronics to pharmaceuticals — amounted to an estimated $1.2 trillion worldwide.

To help prevent counterfeit computer chips and other electronic devices from flooding the market, researchers at the National Institute of Standards and Technology (NIST) have demonstrated a method that could electronically authenticate products before they leave the factory.



The video:
https://cdnapisec.kaltura.com/index.php/extwidget/preview/partner_id/684682/uiconf_id/31013851/entry_id/1_kv68s3z0/embed/dynamic

To detect the presence of forged components in a system, you need a way of uniquely identifying and authenticating these components throughout the supply chain.

To achieve this, NIST researchers have developed a new low-cost process for creating unique and non-duplicable ID tags by altering the electronic structure of silicon.

These tags could be embedded into a device during the manufacturing process and easily authenticated by anyone receiving the device, ensuring a secure supply chain for components in critical systems. Credit: Sean Kelley/NIST.

The scientists employed a well-known technique called doping, in which small clusters of "foreign" atoms of a different element from those in the device to be labeled are implanted just beneath the surface.

The implanted atoms alter the electrical properties of the topmost layer without harming it, creating a unique label that can be read by an electronic scanner.

Using doping to create electronic tags for devices is not a new idea. However, the NIST technique, which uses the sharp tip of an atomic force microscope (AFM) probe to implant atoms, is simpler, less costly and requires less equipment than other doping techniques using lasers or a beam of ions, said NIST researcher Yaw Obeng. It is also less damaging than other methods.

"We're putting a sticker on every device, except that the sticker is electronic and no two are identical because in each case the amount and pattern of the dopant atoms is different," said Obeng.

To create the electronic ID, Obeng and his colleagues first deposited a 10-nanometer (billionth of a meter) film of dopant material — in this case aluminum atoms — about 10-centimeter-square silicon wafers that were then broken into postage-stamp-size fragments so that they could fit in the AFM.

The team then used the needle-like tip of the AFM probe to push aluminum atoms a few nanometers into the silicon fragments. The diameter of the implanted regions was tiny, no larger than 200 nm.

The implanted atoms alter the arrangement of silicon atoms just beneath the surface of the wafer.

These silicon atoms, as well as those that reside throughout the wafer, are arranged in a repeating geometric pattern known as a lattice.
Each silicon lattice acts like an electrical circuit with a certain impedance, the AC (alternating current) equivalent of resistance in a DC (direct current) circuit.

When the implanted aluminum atoms were rapidly heated to about 600 degrees Celsius, a few of them acquired enough energy to replace some of the silicon in lattices just beneath the wafer's surface. The random substitution altered the impedance of those lattices.

Each dopant-modified lattice has a unique impedance depending on the amount and type of dopant. As a result, the lattice can serve as a distinctive electronic label — a nanometer-scale version of a QR code for the wafer, Obeng said.

When a scanner directs a beam of radio waves at the device, the electrically altered lattices respond by emitting a unique radio frequency corresponding to their impedance. Counterfeit devices could be easily identified because they would not respond to the scanner in the same way.

"This research is key because it offers a means to uniquely identify components by a secure, unalterable and inexpensive means," said Jon Boyens, a researcher with NIST's Computer Security Division who was not a co-author of the study.

The study, which Obeng presented on Sept. 16 at the International Conference on IC Design and Technology in Dresden, Germany, builds upon earlier work by the same team (https://aip.scitation.org/doi/abs/10.1063/1.5065385?journalCode=jap).

The new study refines the AFM method for inserting dopant atoms, so that the AFM probe can more precisely place the atoms in the silicon wafer. The higher precision will make it easier to test the electronic ID system under real-life conditions.

Obeng and his collaborators, who include Joseph Kopanski of NIST and Jung-Joon Ahn of NIST and George Washington University in Washington, D.C., consider their technique a prototype that will need modification before it can be used in mass production.

One possibility is to use the sharp probes of several AFMs working side by side so that the dopant material could be implanted in many devices at once.

Another strategy would employ high-pressure rollers to rapidly push dopant atoms coating a computer chip or other device a few nanometers into the device.

A pattern stenciled onto the rollers would ensure that the dopant atoms were implanted according to a precise blueprint. Rollers are widely used to smooth paper, textiles and plastics.

To read more: https://www.nist.gov/news-events/news/2021/09/smart-use-doping-implanted-atoms-create-unique-electrical-ids-distinguish

Number 8

Simulating wartime decisions helps prepare for the real thing

Los Alamos NATIONAL LABORATORY

On August 17, Alaskan officials reported 81 cases of an unidentified hemorrhagic fever, similar to but more contagious than the Ebola or Marburg viruses, on the Alaskan island of St. Paul in the Bering Strait.

Within a day, 24 infected people had died. The outbreak occurred two weeks after the United States was accused of sinking the Russian ship Ulana.

Americans had attempted to search Ulana because they suspected it of carrying biological warfare materials to Russia's recently solidified ally North Korea.

Four U.S. Marines died in the skirmish, as well as almost all of the Russian ship's crew.

In addition, a group of South Korean tourists—one of whom had North Korean ties—visited St. Paul three days before the first infection was discovered.

These combined events have led to an increasingly volatile situation between the United States, Russia, and multiple countries in the Asian-Pacific.

If you're thinking you missed some major breaking news, you can breathe a sigh of relief. This all takes place in a *fictional version of 2039*; it's a scenario that was played out in a tabletop exercise (TTX)—a mini-wargame— titled St. Paul Syndrome II, in March of 2021.

Pieces on a board

A wargame, according to deceased wargaming expert Francis J. McHugh of the United States Naval War College, "is a simulation, in accordance with predetermined rules, data, and procedures, of selected aspects of a conflict situation." It's essentially a pretend war.

Wargaming has been around for hundreds of years. "John Clerk, a landsman with no actual experience in the ways of the sea, revolutionized British 18th-century naval tactics by using a tabletop for an ocean and wooden blocks to represent ships," McHugh explained in Fundamentals of War Gaming, which was published in 1960.

The United States has used similar techniques for a long time. According to a 2015 article by then Deputy Secretary of Defense Bob Work and Vice Chairman of the Joint Chiefs of Staff General Paul Selva, during the 1920s and 1930s, "militaries the world over struggled to adapt to new inventions such as radar and sonar, as well as rapid improvements in wireless communications, mechanization, aviation, aircraft carriers, submarines, and a host of other militarily relevant technologies."

During this time, the United States military began to lean heavily on wargaming to play out the possibilities of these new developments and their impact on warfare.

"Wargaming is strategic analysis," says Rich Castro, the retired director of the Strategic Analyses and Assessments Office at Los Alamos National Laboratory. "The Lab's participation is important because wargaming is an analytical tool that brings together many different thoughts, combining the expertise of the Department of Defense, Department of Energy, and the national laboratories."

Wargames help leaders consider different scenarios and think about how they might play out so they can prepare to make quick decisions in the event that a similar scenario actually takes place. "Things are moving so fast, technology moves so fast, you have to think faster," Castro says.

"We don't have the luxury of thinking about these problems in the long-term. There are a lot of changes in our adversaries—cyber, space, nuclear, conventional—that didn't exist during the Cold War. They all come together now in an escalation ladder. You have to play this out or you're caught completely off guard."

Full-scale wargames are played at different locations in the United States, often at the Naval War College in Rhode Island, with hundreds of participants present from all across the country.

The basic structure is that a group of analysts from the organization running the game write a scenario— usually focused on a particular region, technology, or situation that is pertinent to current concerns—to be played out over the course of one or two weeks. Preparation for the game usually takes several months.

Players are assigned to teams that represent countries; a control group determines the outcome of team decisions, actions, and interactions with other country teams. The control group also represents countries that do not have assigned teams. More than 30 large-scale wargames are held annually across the nation, and players from Los Alamos are invited for a particularly important reason—their nuclear expertise.

The nuclear niche

According to Tim Goorley, Los Alamos' lead wargaming consultant for nuclear effects, Los Alamos provides expertise on what happens to people, aircraft, sea vessels, and satellites, for example, in the event of a nuclear detonation. That information is then fed into the game to help the players on both sides understand what possible actions they could take next.

Laboratory personnel provide expertise in person at wargames, and they're consulted ahead of the games during the long, complicated process of scenario creation. For example, one game incorporated whether it was possible to have a new weapon, and, if such a weapon existed, how many the United States might own. Goorley called some Los Alamos engineers to see whether such a weapon could be produced in the timeframe required by the game and whether it could be deployed and used in the way the game planners wanted.

The Los Alamos scrimmage

Another way in which wargames are useful is that they help debunk commonly believed myths about nuclear weapons.

Many wargames end with the detonation of a nuclear weapon, assuming that's a game-over event.

But, according to Goorley, that's not true at all; things are just getting started.

"People don't realize how much you can still do just a few miles or days out from ground zero," he says. "You need to keep going through the game for about a week or two after the detonation to fully understand the effects."

Although many films show city blocks being instantly vaporized by a nuclear weapon, or show an electromagnetic pulse sending a huge part of the country back to the dark ages, those scenarios are not realistic, and realism is vital to productive wargames.

As Goorley puts it, the Laboratory "takes the falling sky and puts it back up."

Experts from Los Alamos are also able to give particular insight into adversaries' policy and technical capabilities. "It takes a nuclear weapons designer to catch a nuclear weapons designer," Goorley explains.

Although full-scale wargames are the longest and most detailed versions, smaller versions referred to as tabletop exercises exist, in which fewer people play out a scenario in a shorter timeframe.

Los Alamos has been conducting tabletop exercises for several years, the most recent being the St. Paul Syndrome II scenario.

St. Paul Syndrome II was a collaboration between the Laboratory's Office of National Security and International Studies (NSIS) and the Center for Strategies and International Studies (CSIS), a Washington, D.C., think tank with whom the Lab has partnered. In fact, the most recent TTX was a replay of a scenario (St. Paul Syndrome I) that different participants played out in the summer of 2020.

By keeping that scenario secret, Los Alamos and CSIS were able to use it again with new players who, through their different decisions, revealed entirely new options and pathways for the unfolding events. "I have learned never to expect particular outcomes," says Ian Williams, an International Security Program fellow and deputy director for the CSIS Missile Defense Project. "Even when running the same scenario with participants of similar professional backgrounds, we see teams take a wide variety of strategies and actions."

St. Paul Syndrome I and II were developed "to explore how decision makers respond to a multi-domain national security conflict," says Paula Knepper, an NSIS program manager. "In this case, we have nuclear and bioweapons as well as an issue related to the Arctic."

The scenario was "the most complex one that we have done so far," Williams says. "Rather than have one major crisis that all the teams were focused on, the scenario had each team facing a different issue that overlapped with the vital interests of the other country teams. This dramatically increased the potential friction points between countries."

NSIS is in charge of choosing Laboratory participants and filling each team roster. An invitation is quite desirable at Los Alamos; for St. Paul Syndrome II, the rosters were filled in less than 24 hours. "One of our objectives is staff development," Knepper says.

"We keep in mind creating opportunities for Laboratory staff to extend their professional networks. We also look for team diversity—experiences, organizations, technical backgrounds, etc. We find that diverse teams have the most insightful and creative outcomes."

Wargames are as realistic as possible and are based on current intelligence, so most are conducted at top secret levels so real intelligence agents can attend and contribute what they know.

The recent TTX between Los Alamos and CSIS, however, was not classified, so the lessons learned from it can be put to broader use. TTXs can be unclassified because they focus on scenarios that take place years in the future, in a world that is only a possibility.

Los Alamos is a particularly useful ecosystem for wargames and small-scale exercises alike because of the close proximity and working relationships of people from many areas of expertise, including engineers, infrastructure experts, policy experts, and scientists from myriad fields.

“The Laboratory is a unique place,” Castro says, “in that it can pull together a team to quickly address multi-domain issues, and everyone can be sequestered in an area just to concentrate on one problem. I don’t know other places that you can do that.”

The coronavirus pandemic threw a wrench into that unique capability in that teams were not able to sequester in person for the past two TTXs, but CSIS and NSIS quickly adapted to build a virtual game space.

Personnel from CSIS ran the game and were assigned to help the country teams, but all of the players were Lab employees.

Some were scientists from fields including nuclear engineering, astrophysics, geophysics, and biosecurity and public health. Others were from intelligence systems, international studies, and international threat reduction.

Most Los Alamos players had never participated in a wargame before. “It was really neat hearing how people with different academic and professional backgrounds approached problems,” says Caleb Schelle, a shock and vibration testing engineer. “I was one of the younger members on the team, and I appreciated learning how more experienced scientists and engineers chose their words and actions thoughtfully.”

Amanda Evans, a scientist in chemical and biological threats, also valued the insight of her colleagues during the TTX. “Building our team’s interactions was a very positive experience,” she says, “as was learning from more experienced colleagues.”

Kickoff

Before the TTX began, participants were divided into teams, each team representing a country—the United States, Russia, China, and Japan. Team

members prepared by reading historical background information that was available to all teams plus some country-specific information provided by their countries' intelligence services.

Teams also received information about their own countries' military capabilities and strategic positions, along with information about that of other countries—to the best of their intelligence agencies' knowledge. They then began to make decisions to play out the scenario, all over the course of just four days.

On the first day of the TTX, after meeting all together, the country teams broke into separate groups and got to work examining the current state of the scenario and determining their main objectives.

At the end of each day, each team must submit its "turn," which includes its objectives and actions—both public and covert.

The time spent in groups is used to discuss how to make those decisions, to read and discuss new information as it comes in throughout the day from the control group, and, at times, to communicate with other countries.

Early in the day, the United States team learned from the Centers for Disease Control and Prevention that the St. Paul virus was a form of Marburg virus that had been developed in a Soviet laboratory in the 1980s, meaning that the outbreak was a bio-attack made by either Russia or Russian-aided North Korea.

The American team's response to this news was much more peaceful than many might have guessed. "It was interesting to see how the U.S. team did not really view it as an attack," observes NSIS Director John Scott. "They appeared to be most concerned about containing the outbreak on the island."

Meanwhile, the Russian team began to launch misinformation campaigns to place blame on the United States for the Ulana sinking, China worked to disrupt American power in the Pacific, and Japan, faced with growing anti-American sentiment among its citizens, strategized the best ways to restore peace to both the region and its own people.

Over the next four days, teams worked to destabilize relationships between other countries, solidify their allies, secure military positions, avoid war, gather and decipher intelligence, get their political parties re-elected, and stop an outbreak of a disease with a 99 percent fatality rate. They moved their military ships around, demanded that each other remove ships from certain areas, and communicated with each other via confidential channels. They issued public statements to each other and to their own citizens.

Teams also received a great deal of information that threw them for loops. For example, uncovered intelligence determined that the Russians had scuttled the Ulana (sunk their own ship) and blamed it on the Americans. Information was also revealed that the Ulana was carrying equipment for bioweapons, yet it seemed that Russia was not directly involved in releasing Marburg on St. Paul Island.

To read more: https://discover.lanl.gov/publications/national-security-science/2021-summer/wargames

Number 9

FSB Financial Stability Surveillance Framework

The assessment of vulnerabilities affecting the global financial system is a core mandate of the FSB. Identifying material vulnerabilities facilitates monitoring by relevant public authorities and the preparation of policy actions to mitigate the financial stability risks posed by the vulnerabilities.

This report describes the framework used by the FSB to identify and assess global financial system vulnerabilities.

The framework has recently been revised following the conclusion of work to enhance the FSB's financial stability surveillance.

The purpose of the new framework is to increase the effectiveness of the FSB's vulnerabilities discussions, and improve the timeliness with which the discussions identify challenges to global financial stability.

The new surveillance framework aims to identify vulnerabilities in a proactive and forward-looking manner. It is based on systematic analysis that spans all parts of the global financial system.

To serve the international remit of the FSB, the new framework provides a global, cross-border, and cross-sectoral perspective on current vulnerabilities that draws on the collective perspective of the FSB's broad membership.

At the same time, the framework aims to capture new and emerging vulnerabilities in an evolving global financial system.

The framework embodies four key principles: focus on vulnerabilities that may have implications for global financial stability; scan vulnerabilities systematically and with a forward-looking perspective, while preserving flexibility; recognise differences among countries; and leverage the comparative advantages of the FSB while avoiding duplication of work.

The framework includes a common terminology – which defines key concepts such as vulnerabilities, shocks and resilience – as well as a common taxonomy of vulnerabilities.

Providing a common basis for discussion, these elements aid shared understanding and consensus building around the identification and assessment of vulnerabilities in the FSB.

The framework focuses on vulnerabilities, the accumulation of imbalances in the financial system, as opposed to the shocks that may trigger those vulnerabilities.

The framework also emphasises vulnerabilities that are common across countries or that may engender cross-border spillovers, which could interact with other vulnerabilities. However, in the event of a material shock, the approach has the flexibility to respond to the stress at hand while maintaining the surveillance of vulnerabilities.

The time horizon over which vulnerabilities materialise is important for policy, and therefore the framework also explicitly identifies global vulnerabilities that are currently material, those that may become material in the next 2 to 3 years, and those that may become material over a longer horizon.

The framework places particular emphasis on bringing multiple perspectives to bear in the assessment of current and emerging vulnerabilities.

Accordingly, the framework draws on the collective perspective of the FSB's broad membership and utilises several different sources to build a picture of vulnerabilities.

These sources include: analysis of surveillance indicators; regular surveys of FSB members and regional bodies; ongoing analysis by relevant FSB working groups; and periodic outreach to private sector participants. Drawing conclusions from these key inputs necessarily requires considered judgment.

Resilience, the capacity of the financial system to absorb shocks, is a vital concept for assessing vulnerability.

Gauging resilience enables the picture of gross vulnerabilities to develop into a view on material net vulnerabilities, and on the stability of the financial system.

Enhancing resilience assessments will be an ongoing priority of the FSB. Once identified, material global net vulnerabilities should be subject to more intensive monitoring and analysis, and, as appropriate, policy dialogue among FSB committees.

In addition, communication with the public about identified vulnerabilities offers important benefits. However, the FSB relies on a frank and open exchange among its members to fulfil its mandate and the external communication should not inhibit this.

Therefore, the external communication will focus on the key messages from the internal vulnerabilities assessment.

These messages will be included in future FSB Annual Reports and could also be communicated in other formats, for example in notes to the G20.

Glossary of Terms

The **global financial system** consists of financial intermediaries, markets, and instruments as well as infrastructure that supports their activities. It also includes participants such as central banks and regulatory authorities, as well as providers of services that support financial activities.

Financial stability is the capacity of the global financial system to withstand shocks, containing the risk of disruptions in the financial intermediation process and other financial system functions that are severe enough to adversely impact the real economy.

A **shock** is an event that may lead to disruption or failure in part of the financial system.

A **vulnerability** is a property of the financial system that:
(i) reflects the accumulation of imbalances,
(ii) may increase the likelihood of a shock, and
(iii) when acted upon by a shock, may lead to systemic disruption.

Propagation mechanisms are the channels through which financial vulnerabilities cause disruption, given the occurrence of a shock.

Resilience is the capacity of a financial system to absorb shocks and prevent them from leading to an unravelling of the accumulated imbalances.

To read more: https://www.fsb.org/wp-content/uploads/P300921.pdf

Number 10

Solving Defense Optimization Problems with Increased Computational Efficiency

Program aims to develop Quantum-Inspired solvers to tackle complex defense optimization problems with 500X performance improvements

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Department of Defense (DOD) must solve many complex optimization problems to enable mission capabilities - from determining the most efficient way to distribute supplies to minimizing warfighters' exposure to hostile forces.

Solving these intricate scenarios is difficult, largely owing to the limitations of existing computing resources.

Today, many optimization problems are solved on conventional computers running both heuristic and approximate algorithms, extracting the best solutions allowed by the limited time and energy that is available.

Many believe quantum computing could be the answer. While there are potential advantages to quantum information processing, there is not enough supporting evidence to show that a quantum solution would be suitable for the size, weight, and power limits of many DOD mission-relevant applications.

"That does not mean that valuable lessons cannot be learned from quantum techniques, and applied to classical computing," said Bryan Jacobs, a program manager in the Microsystems Technology Office. "DARPA seeks to do just that with a new program to develop Quantum-Inspired (QI) classical solvers. QI solvers are mixed-signal systems that use classical analog components and digital logic to emulate the physics of dynamic systems." These systems are projected to outperform both conventional and quantum computers by over a factor of 10,000.i

DARPA's Quantum-Inspired Classical Computing (QuICC) program seeks to leverage lessons learned from benchmarking quantum algorithms to develop QI solvers for a range of complex DOD optimization problems, and demonstrate the feasibility of reducing the required computational energy by at least two orders of magnitude over existing techniques.

To date, prototype QI solvers have been demonstrated using small, "boutique" problems tailored to existing architectures. To tackle larger scale, more DOD-relevant problem classes, the QuICC program must address multiple technical obstacles. These include analog hardware

challenges that restrict connectivity between dynamic systems, as well as the prohibitive growth in digital resources with problem size.

To overcome the challenges, the QuICC program seeks innovative solutions with algorithmic and analog hardware co-design, and application-scale benchmarking techniques. Researchers will work across two technical areas to achieve the target objectives.

The first area focuses on developing solver algorithms and creating a framework for assessing the potential performance of QI solvers. The second aims to develop QI dynamical system hardware as well as validated models of their performance.

Progress on QuICC will be measured against a set of key metrics, including computational efficiency, which is characterized by the energy expended to obtain a high-quality solution to a given problem.

QuICC prototype systems will target a 50X reduction in energy for intermediate problem sizes, and show the feasibility of a 500X reduction for mission-scale problem sizes.

“With QuICC, we want to create a fundamentally new way of doing classical computing that takes inspiration from the algorithmic advances happening in quantum computing. The goal is to enable a 500X performance improvement in the energy required to solve complex, DOD-relevant optimization problems.

If we’re successful in generalizing and scaling QI solvers for DOD-relevant applications, we could see a quantum leap in computational efficiency for a broad range of optimization challenges,” said Jacobs.

To learn more about the QuICC program and its objectives, please visit the Broad Agency Announcement published on SAM.gov

Number II

Attackers look to deploy attacks through the software supply chain

Cloud services can be more secure than in-house solutions, but they aren't always without their own flaws.

An unnamed software-as-a-service (SaaS) provider invited researchers from Unit 42 at Palo Alto Networks to identity vulnerabilities in the supply chain. You may visit: https://unit42.paloaltonetworks.com/cloud-threat-report-2h-2021/

The exercise uncovered critical software development flaws leaving customers potentially vulnerable to attacks similar to those on SolarWinds and Kaseya VSA.

The researchers were able to escalate their privileges from the limited access a contractor might be given, all the way to administrator access. From this position a real attacker would be able to compromise the system, with the company realising too late to take effective action.

Nathaniel Quist, principle researcher at Unit 42, said "Role-based access controls within the developer roles would have prevented the Unit 42 researchers from accessing all of the developer repositories".

In his blog post, There's a hole in my bucket, Nigel C talks about ways to secure data in the cloud, including the importance of setting identity (e.g. role) or resource-based policies for access. You may visit: https://www.ncsc.gov.uk/blog-post/theres-hole-my-bucket

There's a hole in my bucket

...or 'Why do people leave sensitive data in unprotected AWS S3 buckets?'

In his 'My cloud isn't a castle' blog, Andrew A discussed the general challenge of preventing leaks from misconfigured cloud services. Here we look at a specific service which we've been asked about: Amazon Web Services (AWS).

It seems like every month there's a new announcement about an organisation suffering a data leak from an improperly-secured Amazon S3 bucket. Either the bucket was made public (exposing sensitive files to

anyone on the Internet), or was left open to any authenticated AWS user (anyone can sign up to AWS to become an authenticated AWS user).

However, there's not much public discussion about why so many buckets end up exposed. A first thought might be 'someone forgot to lock down the access'. However, S3 buckets - by default - can only be accessed by the bucket owner.

The owner must decide to make the bucket accessible, meaning data leaks are not due to users forgetting to lock them down. Something else must be going on....

It's not always good to share

While some data leaks may simply be a case of storing sensitive data in the wrong bucket, I suspect that many of these leaks are a consequence of S3 buckets being used as 'just another file storage system'.

Despite some superficial similarities, S3 is not a POSIX file system like Windows or UNIX, and assumptions based on POSIX file systems can mislead. Working with S3 without understanding how AWS works will lead to frustration and/or insecure data.

Access control for S3 buckets can be complex as it is implemented through two different systems: the older coarse-grained ACLs (Access Control Lists), and the newer 'IAM Policies'.

IAM policies are powerful and fine-grained (perhaps too fine-grained for purposes like simple file-sharing). For users unfamiliar with IAM (and its use of JSON) there's a steep learning curve, so it's perhaps not surprising when people on a tight timescale simply make the bucket public. Do any of these justifications sound familiar?

- 'It's only for a little while.'

- 'It's only for the demo. I'll look up the proper way to do it later.'

- 'Nobody will find it anyway.'

Unfortunately for these people:

- It's easy to forget to remove temporary permissions.
- It's easy to forget to implement correct protections when the demo transitions to a live system.

- People will find it: there are lots of people hunting for open buckets. It's sensible to assume that if a bucket is public, its contents have already been copied.

And, while 'world-readable' with local files really translates to 'readable by anyone on the system', with S3 buckets it's literal.

To read more: https://www.ncsc.gov.uk/blog-post/theres-hole-my-bucket

Number 12

Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms

cybereason

In July 2021, the Cybereason Nocturnus and Incident Response Teams responded to Operation GhostShell, a highly-targeted cyber espionage campaign targeting the Aerospace and Telecommunications industries mainly in the Middle East, with additional victims in the U.S., Russia and Europe.

The Operation GhostShell campaign aims to steal sensitive information about critical assets, organizations' infrastructure and technology.

During the investigation, the Nocturnus Team uncovered a previously undocumented and stealthy RAT (Remote Access Trojan) dubbed ShellClient which was employed as the primary espionage tool.

The Nocturnus Team found evidence that the ShellClient RAT has been under ongoing development since at least 2018, with several iterations that introduced new functionalities, while it evaded antivirus tools and managed to remain undetected and publicly unknown.

Assessments as to the identity of the operators and authors of ShellClient resulted in the identification of a new Iranian threat actor dubbed MalKamak that has operated since at least 2018 and remained publicly unknown thus far.

In addition, our research points out possible connections to other Iranian state-sponsored APT threat actors such as Chafer APT (APT39) and Agrius APT. However, we assess that MalKamak has distinct features that separate it from the other Iranian groups.

To read more: https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms

Number 13

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced the launch of the department's *Civil Cyber-Fraud Initiative*, which will combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco.

"Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

The creation of the Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is a direct result of the department's ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May.

The review is aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats.

Civil Cyber-Fraud Initiative Details

The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.

The False Claims Act is the government's primary civil tool to redress false claims for federal funds and property involving government programs and operations.

The act includes a unique *whistleblower* provision, which allows private parties to assist the government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.

The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

The benefits of the initiative will include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.

- Holding contractors and grantees to their commitments to protect government information and infrastructure.

- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.

- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.

- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.

- Improving overall cybersecurity practices that will benefit the government, private users and the American public.

The department will work closely on the Initiative with other federal agencies, subject matter experts and its law enforcement partners throughout the government.

Report Cyber-Fraud

Tips and complaints from all sources about potential cyber-related fraud, waste, abuse and mismanagement can be reported by accessing the webpage of the Civil Division's Fraud Section, which can be found at: https://www.justice.gov/civil/report-fraud

Number 14

Agency Actions Needed to Address Foreign Influence

US Government Accountability Office (GAO) - Testimony Before the Subcommittees on Investigations and Oversight and Research and Technology Committee on Science, Space, and Technology House of Representatives, Statement of Candice N. Wright, Director, Science, Technology Assessment, and Analytics.

What GAO Found

U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest (COI).

Federal grant-making agencies such as the National Science Foundation (NSF) can address this threat through COI policies and requiring the disclosure of information that may indicate conflicts.

In a December 2020 report, GAO reviewed five agencies, including NSF, which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018.

GAO found that three of the agencies it reviewed have agency-wide COI policies and two do not.

The three agencies with existing COI policies focus on financial interests and do not specifically address or define non-financial interests, which may include multiple professional appointments.

In the absence of agency-wide COI policies and definitions for non-financial interests, researchers may not fully understand what they need to report on their grant proposals, leaving agencies with incomplete information to assess the risk of foreign influence.

Elements of Conflict of Interest (COI) Policies at Selected Agencies

	National Science Foundation	National Institutes of Health	National Aeronautics and Space Administration	Department of Defense	Department of Energy
Agency-wide COI policy	✓	✓	✓	No Agency-wide COI Policy	
Addresses financial COI	✓	✓	✓		
Addresses non-financial COI	—	—	—		

Source: GAO analysis of agency documents. | GAO-22-105434

In the report, GAO found that agencies were working with the Office of Science and Technology Policy (OSTP) on efforts to protect federally funded research and were waiting for OSTP to issue guidance on addressing foreign influence before updating their policies.

In January 2021, the White House and OSTP issued documents for agencies and research organizations, respectively, on actions to strengthen protections for federally funded research against foreign influence.

As of September 2021, OSTP is working on implementation guidance for agencies, due to be issued in November 2021.

All five agencies have mechanisms to monitor and enforce COI policies and requirements. While most agencies collect non-financial information, such as details of foreign collaborations, agencies rely on universities to monitor financial conflicts.

All five agencies have enforcement mechanisms for responding to an alleged failure to disclose required information, however, only NSF and the National Institutes of Health have written procedures for such allegations.

In addition, agencies have referred cases for criminal investigation, among other enforcement actions, where they identified researchers who failed to disclose required information.

Chairman Foster, Chairwoman Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees:

Thank you for the opportunity to discuss our December 2020 report on foreign influence in federally funded research.

The federal government reportedly expended about $44.5 billion on university science and engineering research in fiscal year 2019.

Safeguarding U.S. taxpayers' investment in federally funded research from undue foreign influence is of critical importance.

Recent reports by GAO and others have noted challenges faced by the research community to combat undue foreign influence, while maintaining an open research environment that fosters collaboration, transparency, and the free exchange of ideas.

For example, we recently reported on the risk foreign students working at U.S. research universities may pose by transferring sensitive knowledge they gain to their home countries.

In August 2018, the Director of the National Institutes of Health (NIH) sent a letter to over 10,000 universities highlighting concerns over foreign government talent recruitment programs, noting that these programs can influence researchers receiving federal funding to divert intellectual property and federally funded research to other countries.

The letter also highlighted concerns that some researchers who receive federally funded grants did not disclose financial and other resources provided by foreign governments.

For example, in May 2020, a former researcher at one U.S. university pleaded guilty for not reporting hundreds of thousands of dollars in foreign income on his federal tax returns, in relation to his involvement in the Thousand Talents Program, a Chinese-government talent recruitment program.

This case came to light after the agency reviewed the researcher's grant proposals and became concerned that he had failed to disclose, among other things, foreign research activity.

My testimony today summarizes the findings in our December 2020 report on foreign influence in federally funded research.

Specifically, it discusses

(1) the extent to which selected agencies and universities have conflict of interest policies and disclosure requirements that address potential foreign influence,

(2) the extent to which selected agencies have mechanisms to monitor and enforce policies and requirements, and

(3) the views of selected stakeholders on how to better address foreign threats to federally funded research.

For the report, we reviewed relevant laws, regulations, federal guidance, conflict of interest policies and requirements, and interviewed agency officials, university officials, and researchers about agency and university conflict of interest policies and disclosure requirements.

For this testimony, we asked the agencies we reviewed to provide updates on any steps taken to address the recommendations in our December 2020 report, and updated the recommendation status of selected agency activities, as appropriate.

This testimony, as well as the report, focuses on the top five agencies with the largest amount of funding for federal research, and which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018—the Department of Defense (DOD), the Department of Energy (DOE), the National Aeronautics and Space Administration (NASA), NIH, and the National Science Foundation (NSF).

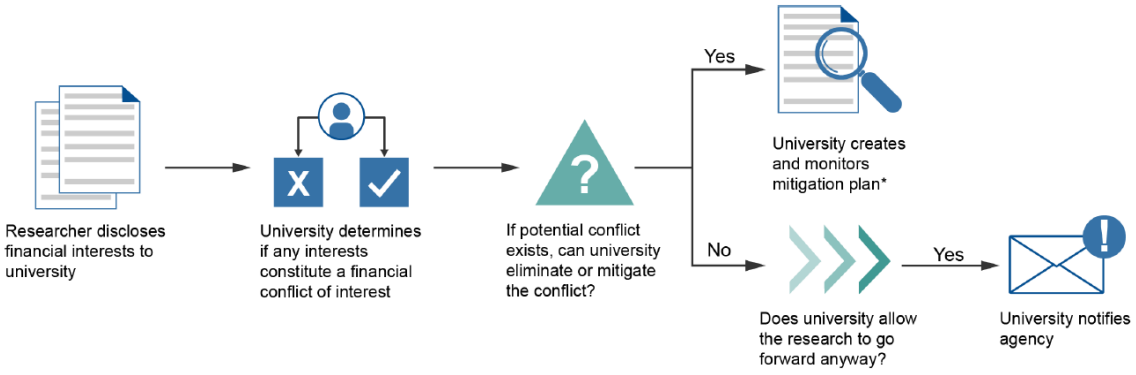
We also selected 11 universities, each of which received over $500 million in combined research grant funding in fiscal years 2018 and 2019 from two or more of the five selected agencies.

Additional information on our scope and methodology is available in our December 2020 report.

Our work was performed in accordance with generally accepted government auditing standards.

To read more: https://www.gao.gov/assets/gao-22-105434.pdf

Figure 1: Generalized University Processes for Identifying and Mitigating Potential Financial Conflicts of Interest



Source: GAO analysis of university and agency policies. | GAO-22-105434

*NIH regulations require universities to submit financial conflict of interest reports, including a description of the key elements of the university's mitigation plans. 42 C.F.R. § 50.605(b)(1)-(3). In addition, DOE officials told us that some of their components also require universities to submit mitigation plans. DOD noted that they may require such information in certain circumstances.

Number 15

New Android malware allows attackers to monitor all user activity on infected devices

National Cyber Security Centre

The malware, first seen last month in Canada and the US, has been named "Tanglebot" and allows attackers to gain access to all user activity via the *camera and microphone*, monitor the user's location and *steal any data* on the device, including messages and stored files.

The malware is spread via malicious text message, this is a form of phishing called smishing, which is an increasingly common method of spreading malware. Both phishing emails and smishing texts work by persuading victims to click on a link.

In this case, once the link is clicked "Tanglebot" victims are informed that Adobe Flash Player needs to be updated - Adobe stopped supporting Flash in December 2020 – and are led through a series of dialogue boxes which will allow the attackers to install and configure the malware. *Attackers then have full access to the device.*

The NCSC has published advice on how to deal with suspicious emails and messages such as this. You may visit:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

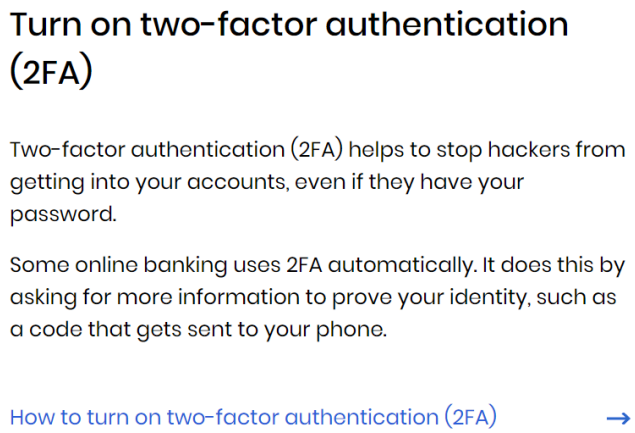
Spotting suspicious messages

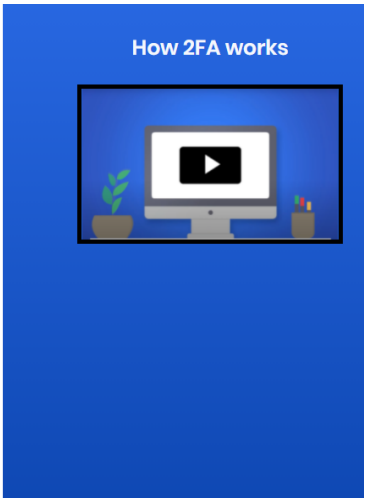
Spotting scam messages and phone calls is becoming increasingly difficult. Many scams will even fool the experts. However, there are some tricks that criminals will use to try and get you to respond without thinking. Things to look out for are:

- **Authority** - Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

Specifically, when receiving a scam text message, forward it to 7726. This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.

The Cyber Aware website and our Individuals and Families page has additional advice to help you protect yourself online. You may visit: https://www.ncsc.gov.uk/cyberaware/home





Number 16

Episode 50: The Photonicist

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this episode of the Voices from DARPA podcast, Gordon Keeler, a program manager since 2017 in the agency's Microsystems Technology Office, takes listeners on a scenic tour of his efforts to integrate electrons and photons in ways that do more computing, more sensing, more decision-making, and more artificial intelligence in cheaper, smaller, lighter, and more energy-efficient packages than has been possible previously.

His work is a showcase of what technology insiders refer to as SWaP-C, which stands for Size, Weight and Power, and Cost.

Innovations that shrink one or all of those aspects of a technology can be far more important to realizing practical, affordable technologies and capabilities than the invention itself.

As Keeler explains how these and other technology drivers unfold in the half-dozen electronic, photonic, and optoelectronic programs he oversees, he also reveals what inspired him to give up the stable and secure job he held for 14 years before arriving at DARPA.

"I had no doubt really in my mind, DARPA clearly was the pinnacle of doing really innovative scientific research and development and leading the community to go do new things," Keeler tells listeners.

"I wanted to make an impact and DARPA was clearly a way to do that."

In that spirit, the Microsystems Technology Office will be running the 2021 ERI Summit, which from October 19-21 brings together leaders from across the electronics ecosystem to showcase technical achievements from DARPA's five-year, $1.5B investment in the advancement of the U.S. semiconductor industry.

This year's Electronics Resurgence Initiative Summit will also celebrate MTO's 30th anniversary, recognizing the many contributions the office has made to the microsystems field throughout its history.

YouTube: https://youtu.be/8f5y1jD7_No

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

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.