March 2019, cyber risk and compliance in Switzerland

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

Dear readers,

I have just read the concluding remarks of Gabriel Bernardino's keynote speech, at the 3rd Annual FinTech and Regulation Conference on "Taking innovation to the next level" in Brussels. Bernardino is the Chairman of the European Insurance and Occupational Pensions Authority (EIOPA).

He said: "As cyber-insurance markets mature, we should start to discuss if cyber insurance should also be mandatory. This would provide a further level of security for companies and consumers in the digital world."

I checked my files, and I saw that the above remarks come just one year after the OECD Conference on Unleashing the Potential of the Cyber Insurance Market (Paris, 22-23 February 2018), and the OECD's Bill Below and Leigh Wolfrom that looked at some of the challenges to insuring cyber risk:

"The evolving nature of cybercrime means risk models may have to look beyond historical data. With new forms of malware and other technologies targeting ubiquitous operating systems, common applications, cloud services and hardware platforms, a single criminal act can potentially scale to global dimensions.

Last year's WannaCry ransomware attack may be a harbinger of things to come. Propagating through legacy Windows systems, Wannacry infected over 200,000 computers in 150 countries. Indeed, the potential for accumulation risks may discourage some insurers and reinsurers from entering the cyber insurance market at all. The bottom line: uncertainty and correlated risks lead to higher prices and limited coverage levels."

To read the excellent paper you may visit:
https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf

I also remembered another excellent paper from the university of St. Gallen, "Insurability of Cyber risk: An empirical analysis", by Christian Biener, Martin Eling, Jan Hendrik Wirfs, that can be found at:

https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

We read: “There is a great need for more research on cyber insurance. Lack of data is a problem, however. For example, according to ENISA, there is a lack of empirical evidence as to the strength and maturity of the cyber insurance market.

Modelling cyber risk holds a great deal of promise, especially if data become available against which to test the models.

Another interesting topic for future research would be discovering approaches that can alleviate the substantial information asymmetry present with cyber risk. Both hidden actions and hidden information will play a role in developing the market further, but exactly how is worth discovering.”

According to the Swiss Reporting and Analysis Centre for Information Assurance (MELANI), numerous people in Switzerland have been affected by sextortion, and the Swiss authorities launch a great web site:
https://www.stop-sextortion.ch/en/index.html (in English)

According to MELANI: “Blackmailers claim in an email to have access to computers and webcams and threaten to publish pictures and videos with sexual content if no ransom is paid.

This scam is called fake sextortion and typically requires payment in bitcoins.

With the help of this fraud method, over the past six months criminals have obtained bitcoins worth approximately CHF 360,000 in spite of the small sums demanded. As long as the victims pay the ransom, this procedure will be invigorated and will continue to be used.”

MELANI continues: “The "fake sextortion" scam consists of making the victim believe that criminals have access to his/her webcam and that they were filmed while looking at pornography.

A threat is then made that the videos will be sent to all the contacts of the recipient if a specific amount in bitcoins is not paid within a certain period of time.

Usually a password from a data leak is given as proof that the computer has been compromised. However, in the majority of cases, this password is outdated and is no longer in use.

Meanwhile, a number of other variants have been observed: mobile phone numbers are also used to convince the victim that the mobile phone has also been compromised.

In another variant, as proof that the email account has been compromised, the

message is apparently sent with the user's own email address. In fact, the sender is bogus, which can be done very easily and without much knowledge.

A subtype of this phenomenon is fake blackmail with threats of an acid attack or a bomb attack. With both types, bitcoins should be paid to halt the attack.

Blackmail emails are sent in several languages, including German, French, Italian and English. Although their modus operandi remained broadly the same, criminals have constantly sought to modify their attempts at extortion, to increase pressure on victims and force them to pay."

To read more:
https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/fake-sextortion.html

---

According to the Bank for International Settlements (BIS), "crypto-assets present a number of risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks." *If you think it looks like a Basel iii nightmare, you are right*.

According to the BIS: "Before acquiring exposures to crypto-assets or providing related services, a bank should conduct comprehensive analyses of the risks noted above. The bank should ensure that it has the relevant and requisite technical expertise to adequately assess the risks stemming from crypto-assets.

The bank should have a clear and robust risk management framework that is appropriate for the risks of its crypto-asset exposures and related services.

Given the anonymity and limited regulatory oversight of many crypto-assets, a bank's risk management framework for crypto-assets should be fully integrated into the overall risk management processes, including those related to anti-money laundering and combating the financing of terrorism and the evasion of sanctions, and heightened fraud monitoring.

Given the risk associated with such exposures and services, banks are expected to implement risk management processes that are consistent with the high degree of risk of crypto-assets. Its relevant senior management functions are expected to be involved in overseeing the risk assessment framework.

Board and senior management should be provided with timely and relevant information related to the bank's crypto-asset risk profile.

An assessment of the risks described above related to direct and indirect crypto-asset exposures and other services should be incorporated into the bank's internal capital and liquidity adequacy assessment processes.

A bank should publicly disclose any material crypto-asset exposures or related services as part of its regular financial disclosures and specify the accounting

treatment for such exposures, consistent with domestic laws and regulations.

The bank should inform its supervisory authority of actual and planned crypto-asset exposure or activity in a timely manner and provide assurance that it has fully assessed the permissibility of the activity and the risks associated with the intended exposures and services, and how it has mitigated these risks."

We also read: "While crypto-assets are at times referred to as "crypto - currencies", the Committee is of the view that such assets do not reliably provide the standard functions of money and are unsafe to rely on as a medium of exchange or store of value." (emphasis added).

I have just read the European Cybersecurity Deployment Report that summarises the activities carried out by ENISA and the participating Member States for the European Cybersecurity Month 2018 and presents the evaluation and conclusions of the campaign.

Humans are the weakest link in information security. The first words of the *Introduction* are:

"With some 95 % of incidents said to be enabled by "some type of human error – intentional or not", there is a strong human factor at play, making cybersecurity everyone's responsibility.

This means personal, corporate and public administration behaviour must change to ensure everybody understands the threat and is equipped with the tools and skills necessary to quickly detect and actively protect themselves against attacks.

People need to develop cyber hygiene habits and businesses and organisations must adopt appropriate risk-based cybersecurity programmes and update them regularly to reflect the evolving risk landscape."

The European Cyber Security Month (ECSM) under the coordination of ENISA is one of the mechanisms by which cyber hygiene and awareness is promoted to the citizens of Europe.

ECSM runs for the entire month of October, with ENISA publishing new material and focusing on a different topic each week.

The report summarises the activities carried out by ENISA and the participating MS for the 2018 campaign and presents the evaluation and conclusions of the campaign.

More importantly, it seeks to trigger a discussion among partners with respect to improvements that can be made in the future.

Week 1 – Theme 1: Practice basic cyber hygiene

ENISA and APWG designed a phishing poster for the first week of the campaign. The phishing poster provided information about the scale of the phishing problem by numbers, tips on how to avoid phishing and what to do if one becomes a victim of phishing.

Week 2 – Theme 2: Expand your Digital Skills and Education

The Get Cyber Skills campaign was launched on Monday 8th October.

ECSM learning modules were created for the campaign with European Schoolnet (under a service contract with the EC for delivering the Better Internet for Kids core service platform and coordination of the Insafe network of Safer Internet Centres in Europe); and as part of the #SaferInternet4EU campaign launched on Safer Internet Day (SID) 2018 by Commissioner Mariya Gabriel to promote online safety, media literacy and cyber hygiene.

This initiative stems from the Digital Education Action Plan and sets out a series of initiatives to support citizens, educational institutions and education systems to better adapt for life and work in an age of rapid digital change.

Key message of the campaign:

Advancing cybersecurity skills and education of younger generations as an important means for keeping themselves and others safe.

Just like the physical world there are threats online that could pose a danger to children and young adults physically, emotionally and financially.

Building cybersecurity skills and competences helps the younger generation to develop routine cyber hygiene practices which they can then transfer to others and help protect society.

The target audience for Get Cyber Skilled campaign were parents, teachers, guardians, role models and community leaders responsible for developing cybersecurity education and skills in young people.

As part of the campaign, four ECSM learning modules were developed to help you create a study plan for your class. Topics include:

- Password management
- Backing up data
- Privacy settings
- Protecting against social engineering

The campaign included a toolkit to help partners and Member States support with the outreach of the campaign.

Week 3 – Theme 3: Recognize Cyber Scams

The theme aimed at educating the general public on how to identify deceiving

content in order to keep both themselves and their finances safe online.

The internet has become very attractive for cybercriminals. Attackers are using sophisticated tricks and promises to wrench money or valuable financial information out of users.

Scams featuring a long-lost deceased relative or Nigerian princes are not the only tricks in the book anymore.

The tactics used by cybercriminals are becoming increasingly innovative and harder to detect.

From pretending to be the CEO of your organisation to impersonating a romantic interest, the online scammers of today will do what it takes to get what they want –money and/or banking credentials.

As such, Europol and the European Banking Federation launched an awareness campaign on the 7 most common online financial scams.

Europol's European Cybercrime Centre (EC3), the European Banking Federation and their partners from the public and private sector participated in the campaign and included the #CyberScams awareness campaign as part of the European Cyber Security Month.

Law enforcement agencies from all 28 EU Member States, 5 non- EU Member States, 24 national banking associations and banks and many other cybercrime fighters raised awareness about this criminal phenomenon.

This pan-European endeavour was driven by a communication campaign and national law enforcement, bank associations and financial institutions that was communicated via social media channels.

For this campaign, awareness-raising material was developed in 27 languages, available for public download, which includes information on the 7 most common online financial scams, and how to avoid them:

- CEO fraud: scammers pretend to be your CEO or senior representative in the organisation and trick you into paying a fake invoice or making an unauthorised transfer out of the business account.

- Invoice fraud: they pretend to be one of your clients/suppliers and trick you into paying future invoices into a different bank account.

- Phishing/Smishing/Vishing: they call you, send you a text message or an email to trick you into sharing your personal, financial or security information.

- Spoofed bank website fraud: they use bank phishing emails with a link to the spoofed website.

Once you click on the link, various methods are used to collect your financial and personal information.

The site will look like its legitimate counterpart, with small differences.

- Romance scam: they pretend to be interested in a romantic relationship. It commonly takes place on online dating websites, but scammers often use social media or email to make contact.

- Personal data theft: they harvest your personal information via social media channels.

- Investment and online shopping scams: they make you think you are on a smart investment… or present you with a great fake online offer.

Week 4 – Theme 4: Emerging Technologies and Privacy

Stay tech wise and safe with the latest emerging technologies.

The plan for week 4 of the campaign included a live webinar by ENISA experts and external experts from Industry with the purpose of discussing the importance of having an "Emerging Technologies Horizon Scanning and Research Process", however the activity was postponed to a later date.

Read more at: https://www.enisa.europa.eu/publications/ecsm-2018-deployment-report

Albert Einstein believed that *games* are the most elevated form of investigation.

Winston Churchill has said: “Play the *game* for more than you can afford to lose… only then will you learn the game.”

I have just read the remarks of *Commissioner Hester M. Peirce* (Securities and Exchange Commission) at the Council of Institutional Investors (Spring Conference).

You may wonder, which is the connection between institutional investors and games?

Well, this is what Hester M. Peirce has said:

“What then do I have to complain about? My concerns are mainly ones of focus. I recently had a conversation with a boy who shares an obsession with many other children his age—the video game Fortnite.

He described to me how much he enjoyed long stretches of playing the game, which I found surprising given that he is a great athlete and generally one of the most active boys I have ever met.

Indeed, if I had just a tenth of his energy, I would be champing at the bit to reverse every last delegation of authority to the SEC staff just so I would have enough to do.

How is it, then, that a boy who has so much energy can sit still in the virtual world of Fortnite? How is it that this simulated environment can drown out the real distractions around him?

Clearly, the designers of that game and others like it have figured out how to concentrate the mind on objects of their own making.

Indeed, as a child, I whiled away many hours playing the flat, unsophisticated videogames of that era, so I can certainly see how inviting today’s games, with their fascinating, multidimensional worlds—and, incidentally, expenditure of real dollars to get a leg-up on competitors—must be.

I see a parallel in today’s investment world. Many investors these days seem focused on non-investment matters at the expense of concentration on a sound allocation of resources to their highest and best use.

Real dollars are being poured into adhering to an amorphous and shifting set of virtue markers.” (emphasis added).

Wow, the word amorphous in a presentation given to institutional investors is unexpected, to say the least.

Francoise Sagan has said: "The illusion of art is to make one believe that great

literature is very close to life, but exactly the opposite is true. Life is amorphous, literature is formal."

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

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

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein and Germany:
https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2019.pdf

Number 1 (Page 15)

How Equifax neglected cybersecurity and suffered a devastating data breach

United States Senate, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, Committee on Homeland Security and Governmental Affairs

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Rob Portman, Chairman
Tom Carper, Ranking Member

HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

Number 2 (Page 21)

Think Global, Act Global: cyberspace and emerging technology

Ciaran Martin, CEO of the NCSC, speaking at CyberSec in Brussels

“More practically, within the cyber security sphere, it is objectively true that nearly all of the functions of the UK’s National Cyber Security Centre fall outside the scope of EU competence.

It follows that our enhanced cooperation with European partners, and the EU as a whole, in cyber security over recent years is not automatically affected by the UK’s changing relationship with the EU.”

Number 3 (Page 30)

Smart Home devices vulnerable to remote attacks due to weak credentials

National Cyber Security Centre
a part of GCHQ

It is no secret that the number of connected devices in the average home is rising. However the Internet of Things (IoT), which is likely to be the norm in the next couple of years, can also contain vulnerabilities and security issues.

Number 4 (Page 32)

Better security measures for smartphones, ENISA has created a SMAShiNG new tool!

ENISA releases SMAShiNG – SMArtphone Secure developmeNt Guidelines – an online tool that maps security measures for smartphone guidelines. The tool supports developers to build secure mobile applications.

enisa European Union Agency for Network and Information Security

The SMAShiNG tool supports developers to build secure mobile applications. It is technologically agnostic, hence can be applied to all mobile applications developed for any operating system on the market nowadays.

Number 5 (Page 34)

Patient calls to Swedish healthcare hotline left unprotected online

National Cyber Security Centre
a part of GCHQ

A server that was used to store recordings of phone calls made to a Swedish "healthcare hotline" has reportedly been found exposed online without password protection. The service provided medical advice via a national health service telephone line.

170,000 hours of calls containing highly personal information were reportedly stored on an open web server without any encryption or authentication. The server contained recordings of conversations going back to 2013.

Number 6 (Page 35)

Public intrusion test

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Post is making its future e-voting system available for a public intrusion test from 25 February to 24 March 2019.

The e-voting system is the first Swiss system that can be completely verified. The complete verifiability makes e-voting available to a broader public, and ensures that systematic malfunction resulting from software errors, human errors or attempted manipulations is detected.

Number 7 (Page 37)

ENISA makes recommendations on EU-wide election cybersecurity

In the context of the upcoming elections for the European Parliament, ENISA has published an opinion paper on the cybersecurity of elections and provides concrete and forward-looking recommendations to improve the cybersecurity of electoral processes in the EU.

enisa European Union Agency for Network and Information Security

ENISA explores cyber-enabled threats, which have the potential to undermine the EU democratic process.

Of particular significance is the possibility of interference in elections by cyber means, due to the widespread use of digital technology to support electoral processes in activities such as confidential communications of politicians and political parties, political campaigns, the electoral register, the counting of votes, and the dissemination of the results.

Number 8 (Page 40)

Written testimony of CISA Director Christopher Krebs for a House Committee on Homeland Security hearing titled "Defending Our Democracy: Building Partnerships to Protect America's Elections"

"Leading up to the 2018 midterms, DHS worked hand in hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle."

Number 9 (Page 49)

Record fine handed to TikTok following data privacy issues

National Cyber Security Centre
a part of GCHQ

The video sharing app, TikTok, has received the largest ever fine recorded in a US case following issues with its management of children's data privacy. Musical.ly app, which was later acquired and incorporated into TikTok, was handed a $5.7m fine because it was knowingly hosting content that had been published by underage users.

Number 10 (Page 51)

A Privacy-Focused Vision for Social Networking

Number 11 (Page 54)

Cybersecurity Disclosure Act of 2019?

Will publicly traded companies be required to disclose to investors whether any members of their board of directors have cybersecurity expertise?

A BILL

To amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Disclosure Act of 2019".

Number 12 (Page 55)

Progress on Lifelong Learning Machines Shows Potential for Bio-Inspired Algorithms

USC milestone on L2M program shows how machines could be capable of learning through experience

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Today's machine learning systems are restricted by their inability to continuously learn or adapt as they encounter new situations; their programs are fixed after training, leaving them unable to react to new, unforeseen circumstances once they are fielded.

Adding new information to cover programming deficits overwrites the existing training set.

With current technology, this requires taking the system offline and retraining it on a dataset that incorporates the new information.

It is a long and arduous process that DARPA's Lifelong Learning Machines (L2M) program is working to overcome.

Number 1

How Equifax neglected cybersecurity and suffered a devastating data breach

United States Senate, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, Committee on Homeland Security and Governmental Affairs

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Rob Portman, Chairman
Tom Carper, Ranking Member

HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

The effects of data breaches are often long-lasting and challenging to reverse. Victims who have had their sensitive personal or financial information stolen by hackers can be left with years of expense and hassle.

No type of entity or sector of the economy has been immune to data breaches. In 2018 alone, Google+, Facebook, Ticketfly, T-Mobile, Orbitz, Saks, Lord & Taylor, and Marriott all announced significant breaches.

The importance of protecting personally identifiable information ("PII") grows with every successive data breach.

Consumers and businesses are well aware of the need to safeguard items like driver's licenses, credit cards, and financial records that criminals can use to their advantage.

Consumers also understand the need to protect information like online passwords, pin numbers, and Social Security numbers.

But a consumer taking appropriate care of this information may not be enough to keep PII out of the hands of criminal hackers.

In the modern world, businesses collect and compile data about their customers and potential customers.

Without proper precautions, this information can be stored or transmitted in ways that leave it vulnerable to theft.

The information collected by consumer reporting agencies ("CRAs") to compile credit reports is one example of PII that must be protected.

This information includes a consumer's name, nicknames, date of birth, Social Security number, telephone numbers, and current and former addresses.

Credit reports also typically include a list of all open and closed credit accounts, account balances, account payment histories, and the names of creditors.

The information tells the story of a consumer's financial life and can determine whether they can rent an apartment, buy a car, or qualify for a home loan. If stolen, criminals can use it to do significant financial harm.

The steps CRAs take to safeguard consumers' credit histories are extremely important. If that information is compromised, consumers should know to be on heightened alert to monitor their finances and mitigate any potential damage.

In 2017, one of the largest CRAs, Equifax Inc. ("Equifax") announced that it had suffered a data breach that involved the PII of over 145 million Americans.

The Subcommittee investigated the causes of this breach to identify ways to prevent future incidents of this scope.

The Subcommittee also reviewed the efforts of Equifax's two largest competitors, Experian plc ("Experian") and TransUnion LLC ("TransUnion"), in responding to the vulnerability that ultimately led to the Equifax data breach.

Highlights of the Subcommittee's investigative results, including findings and recommendations, are provided below.

Equifax Failed to Prioritize Cybersecurity. Equifax had no standalone written corporate policy governing the patching of known cyber vulnerabilities until 2015.

After implementing this policy, Equifax conducted an audit of its patch management efforts, which identified a backlog of over 8,500 known vulnerabilities that had not been patched.

This included more than 1,000 vulnerabilities the auditors deemed critical, high, or medium risks that were found on systems that could be accessed by individuals from outside of Equifax's information technology ("IT") networks.

The audit report concluded, among other things, that Equifax did not abide by the schedule for addressing vulnerabilities mandated by its own patching policy.

It also found that the company had a reactive approach to installing patches and used what the auditors called an "honor system" for patching that failed to ensure that patches were installed.

The audit report also noted that Equifax lacked a comprehensive IT asset inventory, meaning it lacked a complete understanding of the assets it owned.

This made it difficult, if not impossible, for Equifax to know if vulnerabilities existed on its networks. If a vulnerability cannot be found, it cannot be patched.

Equifax never conducted another audit after the 2015 audit and left several of the issues identified in the 2015 audit report unaddressed in the months leading up to the 2017 data breach.

Equifax Could Not Follow Its Own Policies in Patching the Vulnerability That Ultimately Caused the Breach. Equifax's patching policy required the company's IT department to patch critical vulnerabilities within 48 hours.

The company's security staff learned of a critical vulnerability in certain versions of Apache Struts – a widely-used piece of web application software – on March 8, 2017, from the U.S. Computer Emergency Readiness Team at the U.S. Department of Homeland Security.

The National Institute of Standards and Technology gave the vulnerability the highest criticality score possible; it was widely known that the vulnerability was easy to exploit.

Equifax employees circulated news of the vulnerability through an internal alert the next day that went to a list of more than 400 company employees.

Equifax held monthly meetings to discuss cyber threats and vulnerabilities, but senior managers did not routinely attend these meetings and follow-up was limited.

The Apache Struts vulnerability was discussed during the March 2017 and April 2017 meetings, but not discussed at any subsequent monthly meetings.

The Subcommittee interviewed the leadership of the Equifax IT and security staffs and learned that none of them regularly attended these monthly meetings or specifically recalled attending the March 2017 meeting.

In addition, the Chief Information Officer ("CIO"), who oversaw the IT department during 2017, referred to patching as a "lower level responsibility that was six levels down" from him.

Equifax Failed to Locate and Patch Apache Struts. The Equifax developer who was aware of Equifax's use of Apache Struts software was not included in the 400-person email distribution list used to circulate information on the vulnerability.

The developer's manager, however, was on the distribution list and received the alert, but failed to forward it to the developer or anyone on the developer's team. As a result, the key developer never received the alert. Equifax added application owners to the list after the breach.

The Subcommittee also learned that Equifax developers were individually responsible for subscribing to push notifications from software vendors about security vulnerabilities.

The developer who knew of the company's use of Apache Struts software was not subscribed to notifications from Apache and did not receive any alerts about the vulnerability.

On March 14, 2017 – nearly a week after the Apache Struts vulnerability was disclosed – Equifax added new rules to the company's intrusion prevention system intended to help it thwart efforts to exploit the vulnerability.

With these new protections in place, Equifax believed it had the ability to identify and block exploit attempts and did block several attempts the same day the rules were installed.

None of Equifax's subsequent scans identified the vulnerable version of Apache Struts running on Equifax's network. And since Equifax lacked a

comprehensive inventory of its IT assets, it did not know that the vulnerable version of Apache Struts remained on its system.

The Damage Done by the Hackers Could Have Been Minimized. Equifax was unable to detect attackers entering its networks because it failed to take the steps necessary to see incoming malicious traffic online.

Website owners install Secure Sockets Layer ("SSL") certificates to protect and encrypt online interactions with their servers. If an SSL certificate expires, transactions are no longer protected.

As part of an IT management effort unrelated to the Apache Struts vulnerability, Equifax installed dozens of new SSL certificates on the night of July 29, 2017, to replace certificates that had expired.

This included a new certificate for the expired SSL certificate for its online dispute portal. The SSL certificate needed to be up-to-date to properly monitor the online dispute portal, but had expired eight months earlier in November 2016.

Almost immediately after updating the SSL certificate, company employees observed suspicious internet traffic from its online dispute portal that they were able to trace to an IP address in China, a country where Equifax does not operate.

After blocking the IP address, Equifax observed similar traffic the following day to another IP address that appeared to be connected to a Chinese entity and decided to take the online dispute portal offline.

Equifax later determined that the hackers first gained access to Equifax's system through the online dispute portal on May 13, 2017, meaning the hackers had 78 days to maneuver undetected. Equifax confirmed to the Subcommittee that the Apache Struts vulnerability facilitated the data breach that began in May 2017.

Equifax Waited Six Weeks Before Notifying. Once inside Equifax's online dispute portal, the hackers also accessed other Equifax databases as they searched for other systems containing PII.

They eventually found a data repository that also contained unencrypted usernames and passwords that allowed the hackers to access additional Equifax databases.

The information accessed primarily included names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license

and credit card numbers. The usernames and passwords the hackers found were saved on a file share by Equifax employees.

Equifax told the Subcommittee that it decided to structure its networks this way due to its effort to support efficient business operations rather than security protocols.

In addition, Equifax did not have basic tools in place to detect and identify changes to files, a protection which would have generated real-time alerts and detected the unauthorized changes the hackers were making.

Equifax Waited Six Weeks Before Notifying the Public It Was Breached. Equifax employees discovered the suspicious activity that was later determined to be a data breach on July 29, 2017.

Equifax's then-Chief Executive Officer, Richard Smith, learned of the breach on July 31 and that consumer PII maintained by Equifax had likely been stolen on August 15, 2017.

Mr. Smith waited until August 22 to begin notifying members of Equifax's Board of Directors. Equifax publicly announced the data breach on September 7, six weeks after learning of it and nearly four months after the hackers entered Equifax's networks.

Because Equifax was unaware of all the assets it owned, unable to patch the Apache Struts vulnerability, and unable to detect attacks on key portions of its network, for months consumers were unaware that criminals had obtained their most sensitive personal and financial information and that they should take steps to protect themselves from fraud.

Equifax officials say the company chose to notify the public only after determining every single individual impacted by the breach.

To read the paper:
https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

Number 2

Think Global, Act Global: cyberspace and emerging technology

Ciaran Martin, CEO of the NCSC, speaking at CyberSec in Brussels

Thank you to Izabela Albrycht and her colleagues at CyberSec for hosting this excellent conference and for inviting me. CyberSec is an outstanding institution making a very positive contribution to global cyber security.

I'm very proud to represent the UK's National Cyber Security Centre, a part of GCHQ, our signals intelligence agency. It is a pleasure to be among friends discussing our shared aim of improving our digital environment.

Our commitment to working with partners here on the European continent is unshakeable. Whatever form the future relationship between the UK and the European Union takes beyond 29 March this year, the Prime Minister and her Cabinet have long made clear that our support to European security as a whole is unconditional.

More practically, within the cyber security sphere, it is objectively true that nearly all of the functions of the UK's National Cyber Security Centre fall outside the scope of EU competence.

It follows that our enhanced cooperation with European partners, and the EU as a whole, in cyber security over recent years is not automatically affected by the UK's changing relationship with the EU.

Pretty much everything we do now to help European partners, and what you do to help us, on cyber security can, should, and I am confident will continue beyond 29 March.

Over the past few years we have shared classified and other threat data with the vast majority of member states and with the institutions. We have also, we hope, played an important role in the development of European thinking in areas like standards and incident response.

We hope we've helped through our work with CERT-EU on incidents and with ENISA and ETSI on standards.

As the next phase of the UK's relationship with the rest of Europe takes shape, we will want to take these partnerships further and to develop new ones. I am proud of the increasing frequency with which I see my European counterparts and the deepening friendships we have nurtured, the boundaries we are removing and the ground we are breaking.

The protection of our shared values of freedom, democracy and prosperity, all underpinned by the rule of law, is what we strive for.

My theme today is about how we cooperate together in the age of globalised technology.

Because whatever final form the UK's relationship with the EU takes, we need, together, to be at the forefront of global efforts to build an internet that remains not just free but safer too.

In this era of truly globalised technology, it is more important than ever that that effort is – truly – global.

There are limitations to what even a continent of the size and wealth of Europe can do on its own in an age where the US and China dominate tech development.

I want to deal today with two structural challenges for the future of internet security.

The first is about telecommunications infrastructure, now and in the future.

The second is how we improve structural flaws in the wider internet environment.

In both areas, EU and non-EU European nations will need to act with others outside the continent to shape future technology and the security around it.

So first, let's talk about telecommunications infrastructure.

The next generation of telecoms security is particularly important given the sorts of networks dependent on it – there will be large-scale use of autonomous vehicles, desktop experiences from the cloud, high-definition streaming, the underpinning of smart cities.

A hard headed, risk based approach to the policymakers taking decisions

Like many countries, including our five eyes partners, and partners here in Europe, the UK is looking at the right policy approach to 5G security.

That policy process is being led by the Digital Department and its Secretary of State. It concludes its analysis in the spring. The government will then take decisions.

As its public terms of reference make clear, it is a holistic review, taking account of economic, security, quality of service and other factors. It is considering a full range of policy options.

Everything is on the table. Contrary to some reporting no decisions have been taken and no decisions are being announced today.

The National Cyber Security Centre's role is to offer expert, objective, technologically literate input into the security considerations around 5G.

That is consistent with the NCSC's wider mission to bring objective rigour to complex technical issues. And today I want to talk to you about the lessons we have learned.

And the first thing to say is that 5G is complicated.

It hugely accelerates the pace of technological change but there is no cliff edge transition.

It will change the way we think about risk because of what will, over time, depend on it. But it doesn't change immutable concepts of security or the laws of science.

And whilst key to the virtual world, it requires a huge amount of complex physical infrastructure. And how that physical infrastructure is configured varies from country to country, not least depending on the size of the country's landmass and is population.

And it is not a fresh start. It has to build on existing telecommunications infrastructure.

Understanding these complexities is essential. The National Cyber Security Centre is an open and transparent organisation. We have set out before our understanding of how telecommunications networks work and what is needed to secure them.

And we will continue to publish objective, technically credible, clear-headed and rigorous analyses of cyber security requirements.

And we need to set out telecommunications security in the context of the threat picture. Again, here we are open and transparent about the threats we see and how they impact the UK.

Over the past two years, the UK government has, based on NCSC findings, attributed state-sponsored malicious cyber activity against the UK to Russia, China, North Korea and Iran. There is also a serious and sustained threat from organised cyber crime.

These attacks have come against a range of targets spanning different sectors. Their aims have been different. The methods have been different.

The supply chain, and where suppliers are from, is one issue but it is not the only issue. Last year, the NCSC publicly attributed some attacks on UK networks, including telecoms networks, to Russia. As far as we know, those networks didn't have any Russian kit in them, anywhere.

The techniques the Russians used to target those networks were looking for weaknesses in how they were architected and how they were run.

So we are not naïve. Far from it. In the 1,200 or so significant cyber security incidents the NCSC has managed since we were set up, the country of origin of suppliers has not featured among the main causes for concern in how these attacks are carried out.

Three technical pre-conditions for telecommunications e-security

That's one example of our objective, evidence-based analysis of the threat.

We take a similar objective, evidence-based approach to the technical security requirements for 5G.

Taking threat and requirements together, this leads us to conclude that there are three technical pre-conditions for secure 5G networks.

They are:

First, we must have higher standards of cyber security across the entire telecommunications sector.

The biggest threat to our cyber security is weak cyber security.

Practices must be improved. That is the real lesson of the 1,200 cyber security incidents.

The market does not currently incentivise good cyber security.

That has to change.

The number one pre-condition for safe 5G is better cyber security.

Second, telecoms networks must be more resilient.

We must assume that a global supply chain will have multiple vulnerabilities, whether intentional or, more likely, unintentional. Networks are built by human beings and human beings make mistakes. No network can be totally safe.

From the point of view of managing corporate risk, or, in our case, national risk, it essentially doesn't matter whether the vulnerabilities are deliberate or the result of honest mistakes. What matters is that those vulnerabilities can and will be exploited.

But the networks can and should be designed in a way that will cauterise the damage. That is what we need to do. Put it another way, if you've built a telecommunications network in a way that the compromise of one supplier can cause catastrophic national harm, then you've built it the wrong way.

Resilience is key.

The third pre-condition flows from that. There must be sustainable diversity in the supplier market.

Should the supplier market consolidate to such an extent that there are only a tiny number of viable options, that will not make for good cyber security, whether those options are Western, Chinese, or from anywhere else.

Any company in an excessively dominant market position will not be incentivised to take cyber security seriously. And at the same time that company could also become the prime target for attack for the globe's most potent cyber attackers.

These pre-conditions are technical. They are generic. They are about the technology and the architecture and the structure of our networks.

They are about creating the necessary conditions for a safe 5G network.

As already mentioned, like everywhere else, the UK is not starting from scratch. We have an existing telecommunications infrastructure. It is highly internationalised.

And we already have a framework for managing risk. Again, I stress that this is based on an objective understanding of how telecoms networks work. As our guidance to operators shows, we assume that every bit of kit in any network can fail. And so what's vital is that the failure of individual bits of kit, either because of a malfunction or because of an attack, will not cause catastrophic harm.

That's the framework we apply at national level. There are things we particularly care about. National security networks, most obviously. And for those, we apply special protections.

Huawei and standards of cyber security

One well-known specific aspect of our current mitigation framework is how we manage Huawei's presence in UK networks.

Huawei's presence is subject to detailed, formal oversight, led by the NCSC. Because of our 15 years of dealings with the company and ten years of a formally agreed mitigation strategy which involves detailed provision of information, we have a wealth of understanding of the company.

We also have strict controls for how Huawei is deployed. It is not in any sensitive networks – including those of the government. Its kit is part of a balanced supply chain with other suppliers.

Our regime is arguably the toughest and most rigorous oversight regime in the world for Huawei.

And it is proving its worth. Last July, our annual Oversight Board downgraded the assurance we could provide to the UK government on mitigating the risks associated with Huawei because of serious problems with their security and engineering processes.

As we said then, and repeat today, these problems are about standard of cyber security; they are not indicators of hostile activity by China.

The company have accepted these findings and have pledged to address them, acknowledging that this will be a process of some years.

We will monitor and report on progress and we will not declare the problems are on the path to being solved unless and until there is clear evidence that this is the case.

We will not compromise on the improvements we need to see from Huawei.

And, based on our hard-headed assessment of risk and our detailed knowledge of how networks work, we are putting in place our own plans for helping our operators to manage these risks.

It's complicated

So today I am setting out how the NCSC is looking to manage the risks now, for example those around Huawei, and how we could seek to manage the risks into the future.

The UK community is united in this effort.

As the head of MI6, Alex Younger, said in Munich last week, it's complicated. As the Director of GCHQ, my boss, Jeremy Fleming, has set out before and will do so again shortly, it is vital that the UK's stance is informed by the most rigorous assessment of threat, risk and technical requirements. GCHQ, of which the NCSC is part, is at the heart of that discussion.

It is the NCSC's job, working with partners in central government, the regulators and elsewhere to make sure the UK can prosper securely in these complex market conditions through a hard-headed, technically informed assessment of the risk.

That will enable government to weigh up those vital decisions on things like suppliers from different countries.

5G is about much more than just cyber security.

Our job is to make sure that the government can be confident that behind whatever decision it takes, there will be a technical framework that works and a competent national technical authority that knows what it is doing.

Whatever decisions are taken will need to ensure that those three essential pre-conditions for cyber security that we have set out today can be met: stronger standards, more resilience and supplier diversity.

Indeed our experience with Huawei, if nothing else, demonstrates the importance of raising standards of performance in cyber security.

5G security is not a simple, binary choice. It is about complex technical functions, a complex global threat environment, and a complex global market.

One thing is clear: the way that market works has to change.

Security must be a bigger consideration in market decisions in the future than it has been to date. We will help fix that.

Active/automated cyber defence

And the push to improve standards in cyber security should be a global effort. So the more we can do with partners to deliver those, the better.

That brings me to the wider issue of how we cooperate to improve the global digital infrastructure more generally.

The internet was not built with security in mind. That's no one's fault. It wasn't malicious. It's just the way it happened. A model evolved over time where the price of entry for online services became the provision of personal data.

It's safe to say that the limitations of that model are becoming more apparent as time passes.

And they also leave us with structural security problems in the way the internet works.

At the National Cyber Security Centre we focus on the technical solutions that the market hasn't provided because of the way the internet environment has evolved.

We aim to make the internet automatically safer for people to use. It's not fair on busy individuals with complicated, rushed lives and other priorities if we expect them to make judgments every day about how trustworthy one of the hundreds or thousands of bits of communication they get every day are.

That is what is behind our active, or automated, cyber defence programme.

Its aim is to provide a framework to take away most of the harm from most of the people most of the time.

Here are some of the early results.

We have developed a system to use our vast quantity of threat data to block connections to malicious sites from government networks. We are now protecting 1.3 million government internet users.

In 2018, we blocked 11,000 unique malicious domains every month. In the course of the year, we blocked 54 million malicious connections. That's 54 million incidents that automatically didn't happen.

We developed an anti-spoofing mechanism to protect government brands. In the first year, we helped our tax authority block half a billion attempts to spoof it. Half a billion fake emails that didn't land in people's inboxes.

We developed a system for automatically taking down known phishing sites. They used to be up for a day on average. Now it's about an hour. And the UK's share of global phishing that we can see has fallen from 5.3 per cent to 2.2 per cent in the past two and a half years.

Think of the potential if we can amplify these sorts of improvements internationally.

None of them has required legislation, and none has been particularly contentious. They are technical improvements – targeted government interventions where commercial solutions can't work. They are low classification – we publish details for most of them. I cannot think of an area more ripe for international cooperation.

So whether it's future telecommunications infrastructure, or digital security more generally, we want to work with everyone across Europe and beyond to push these changes, to deliver the digital world we all want to see, one that is not just free and prosperous, but safer as well.

Thank you.

Number 3

Smart Home devices vulnerable to remote attacks due to weak credentials

National Cyber Security Centre
a part of GCHQ

It is no secret that the number of connected devices in the average home is rising.

However the Internet of Things (IoT), which is likely to be the norm in the next couple of years, can also contain vulnerabilities and security issues.

Smart home devices can be vulnerable to attacks due to outdated software, unpatched security flaws, and weak credentials according to a new report produced by Avast. It can be found at: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf

In total, 16 million different home networks worldwide are included in Avast's study with the report focusing on 21 countries in North and South America, Europe, and the Asia Pacific region. 56 million devices were scanned as part of the study.

The report states that two out of five (40.8%) smart home devices worldwide have at least one device that is vulnerable to attacks, out of which, 69.2% are vulnerable due to weak credentials.

The UK Government advocates for strong security to be built into internet-connected products by design.

In October 2018, the government published the Code of Practice for Consumer IoT Security to support all parties involved in the development, manufacturing and retail of consumer IoT. It can be found at: https://www.gov.uk/government/collections/secure-by-design

The NCSC has called for the adoption of Secure by Default which covers the long-term technical effort to ensure that the right security primitives are built in to software and hardware.

It can be found at: https://www.ncsc.gov.uk/articles/secure-default

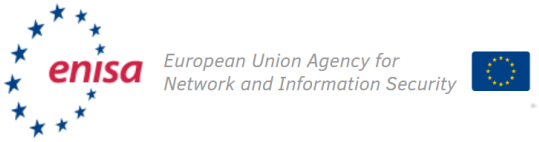
Advice about how to use smart devices safely at home as also been published.

It can be found at: https://www.beta.ncsc.gov.uk/guidance/smart-devices-in-the-home

Number 4

Better security measures for smartphones, ENISA has created a SMAShiNG new tool!

ENISA releases SMAShiNG – SMArtphone Secure developmeNt Guidelines – an online tool that maps security measures for smartphone guidelines. The tool supports developers to build secure mobile applications.



The SMAShiNG tool supports developers to build secure mobile applications.

It is technologically agnostic, hence can be applied to all mobile applications developed for any operating system on the market nowadays

New developments in both software and hardware area have resulted into new significant threats for the mobile computing environment, highlighting the need for a tool to help the developers' community.

SMAShiNG touches upon crucial security measures such as:

- User authentication;
- Sensitive data protection;
- Secure software distribution;
- Device and application integrity;
- Protection from client side injections;
- Correct usage of biometric sensors.

SMAShiNG makes it easier for the developers' community to follow guidelines, by selecting only the ones that are relevant to them.

The tool allows for selecting security measures associated with a specific domain and export them as a checklist to follow in the design phase, based on the requirements of the developer.

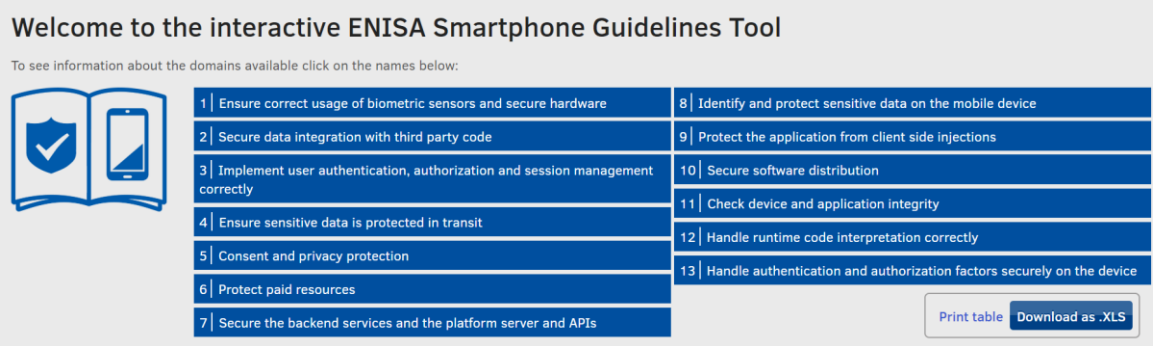
The security measures featured by SMAShiNG are defined in the ENISA Smartphone Secure Development Guidelines report, which provides a guide for developing secure mobile applications.

The release of SMAShiNG is an important part of ENISA's continuous work in promoting the 'security-by-design' principle, by which strong

cybersecurity is built into products as early as the design phase, easing the burden of EU citizens to secure their devices and products.

SMAShiNG complements the work done by ENISA in this area, such as the recently launched online tool for IoT and Smart Infrastructures and the privacy enhancing technologies (PETs) knowledge management and maturity assessment.

ENISA aims to implement a series of enhancements and to broaden the scope of this tool, in order to facilitate users' live interaction with security recommendations through a visualised and interactive page.



To read more:
https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool

Number 5

Patient calls to Swedish healthcare hotline left unprotected online

National Cyber Security Centre
a part of GCHQ

A server that was used to store recordings of phone calls made to a Swedish "healthcare hotline" has reportedly been found exposed online without password protection. The service provided medical advice via a national health service telephone line.

170,000 hours of calls containing highly personal information were reportedly stored on an open web server without any encryption or authentication. The server contained recordings of conversations going back to 2013.

The calls included sensitive information about patients' diseases and ailments, medication, and medical history, and many of the calls were stored alongside telephone numbers.

The Swedish Data Protection Authority told the BBC: "If the reports in the media are correct, we view this incident as very serious since it involves sensitive personal data about many people for a long time. We intend to do a supervision of this incident. We have not formally initiated the supervision yet, though."

Any organisation that deals with sensitive personal information is at a higher risk of being targeted by malicious actors.

The NCSC has published 15 good practice measures for the protection of bulk personal data.

You may visit:
https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main

Organisations handling sensitive information should also ensure they are adhering to the General Data Protection Regulation (GDPR).

The NCSC has published GDPR security outcomes which was developed in partnership with the Information Commissioner's Office (ICO).

You may visit:
https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

Number 6

Public intrusion test

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Post is making its future e-voting system available for a public intrusion test from 25 February to 24 March 2019.

The e-voting system is the first Swiss system that can be completely verified. The complete verifiability makes e-voting available to a broader public, and ensures that systematic malfunction resulting from software errors, human errors or attempted manipulations is detected.

Category	Vulnerabilities	Minimum Compensation
Undetectable vote manipulation	Manipulation of individual votes that is undetectable by voters and trusted auditors;	Between 30'000.- and 50'000.-
	Scalable manipulation of votes that is undetectable by voters and trusted auditors;	
Vote manipulation	Manipulation of individual votes while maintaining universal verifiability mechanism (manipulation detectable by a trusted auditor) - e.g. the vote is modified after being cast;	20'000.-
Vote privacy (server-side)	The privacy of a voter is broken (who voted) on the server;	10'000.-
	The privacy of a vote is broken (what did he or she vote) on the server;	

In accordance with the requirements of federal law, the system must be certified before first use and the source code must be disclosed.

In addition, the Confederation and the cantons have decided that completely verifiable e-voting systems must undergo an intrusion test before they are used for the first time.

Intrusion tests stage attacks to verify a system's security. An intrusion test is already being carried out by an accredited body as part of the certification process.

The public intrusion test has the added benefit of including a large number of people to test the security of a system.

Those interested can register at https://onlinevote-pit.ch and access further information on the test modalities.

To read more:
https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system

https://www.evoting.ch/en

Number 7

ENISA makes recommendations on EU-wide election cybersecurity

In the context of the upcoming elections for the European Parliament, ENISA has published an opinion paper on the cybersecurity of elections and provides concrete and forward-looking recommendations to improve the cybersecurity of electoral processes in the EU.

ENISA explores cyber-enabled threats, which have the potential to undermine the EU democratic process.

Of particular significance is the possibility of interference in elections by cyber means, due to the widespread use of digital technology to support electoral processes in activities such as confidential communications of politicians and political parties, political campaigns, the electoral register, the counting of votes, and the dissemination of the results.

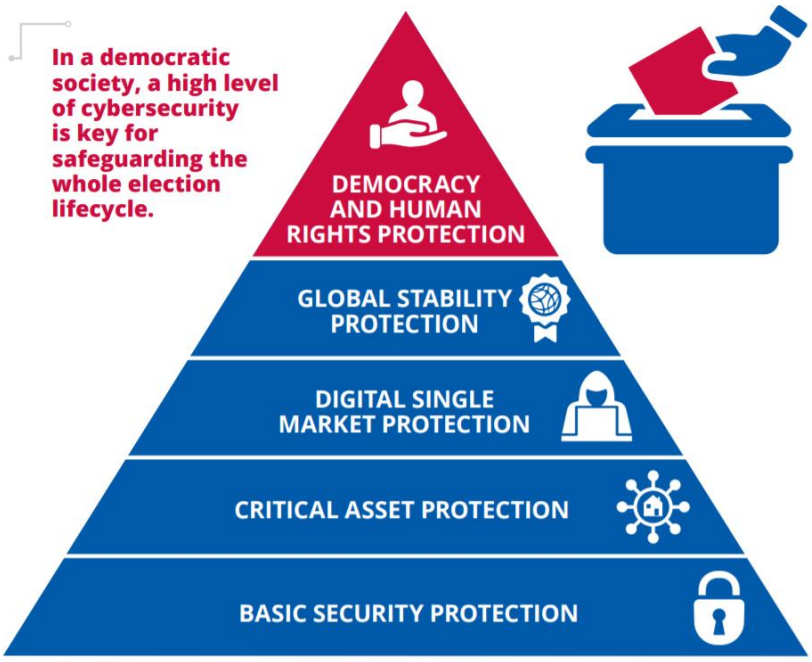
Udo Helmbrecht, Executive Director of ENISA: "As some EU Member States have either postponed or discontinued the use of electronic voting, the risk associated with the voting process can be considered to be somewhat reduced. Nonetheless, the public political campaigning process is susceptible to cyber interference.

We have witnessed in the past election campaigning processes being compromised due to data leaks. ENISA encourages the EU Member States and key stakeholders such as political parties to partake in more cyber exercises aimed at testing election cybersecurity in order to improve preparedness, understanding, and responding to possible election-related cyber threats and attack scenarios.

These stakeholders should have incident response plans in place, in the event that they become a victim of data leaks."

An evolving threat is the motivation behind the actors interfering with the due process of elections by cyber means. The motivation for the actors can be manifold, for example for financial gain, fame and reputation, or to provoke chaos and anarchy, undermine trust in democracy, and subvert political opposition.

Through this paper, ENISA puts forward a set of recommendations aimed at improving the cybersecurity of elections across the EU and supporting the Member States in their efforts.



The most important recommendations that ENISA makes are:

- Member States should consider introducing national legislation to tackle the challenges associated with online disinformation while protecting to the maximum extent possible the fundamental rights of EU citizens;

- Member States should continue to actively work together with the aim to identify and take down botnets;

- Consideration should be given to regulation of Digital Service Providers, social media, online platforms and messaging service providers at an EU level to ensure a harmonised approach across the EU to tackling online disinformation aimed at undermining the democratic process;

- The above players are also advised to deploy technology that will identify unusual traffic patterns that could be associated with the spread of disinformation or cyberattacks on election processes;

- A legal obligation should be considered to classify election systems, processes and infrastructures as critical infrastructure so that the necessary cybersecurity measures are put in place;

- A legal obligation should be put in place requiring political organisations to deploy a high level of cybersecurity in their systems, processes and infrastructures;

- Official channels/technologies for the dissemination of the results should be identified, as well as back-up channels/technologies that validate the results with the count centres. Where websites are being used, DDoS mitigation techniques should be in place.

To read the paper:
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities

Number 8

Written testimony of CISA Director Christopher Krebs for a House Committee on Homeland Security hearing titled "Defending Our Democracy: Building Partnerships to Protect America's Elections"

Chairman Thompson, Ranking Member Rogers, and members of the Committee, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) progress in reducing and mitigating risks to our Nation's election infrastructure.

DHS has worked to establish trust-based partnerships with state and local officials who administer our elections, and I look forward to sharing with you an update on our work during the 2018 midterm election cycle.

Leading up to the 2018 midterms, DHS worked hand in hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. This partnership led to a successful model that we aim to continue and improve upon in the 2020 election cycle.

Since 2016, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information.

CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response.

To ensure a coordinated approach, CISA convened stakeholders from across the Federal Government through the Election Task Force.

The Department and the Election Assistance Commission (EAC) have convened federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance.

Since 2016, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives,

to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector-Specific Plan.

Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

DHS and the EAC have also worked with election vendors to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by sector membership.

The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies.

This collaboration is conducted under DHS's authority to provide a forum in which federal and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. The SCC has helped DHS further its understanding of the systems, processes, and relationships particular to operation of the EIS.

Within the context of today's hearing, I will address our efforts in 2018 to help enhance the security of elections that are administered by jurisdictions around the country, along with our election related priorities through 2020.

While there was activity targeting our election infrastructure leading up to the midterms, this activity is similar to what we have seen previously and occurs on the Internet every day.

This activity has not been attributed to nation-state actors and along with the Department of Justice (DOJ), we concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections

Assessing the Threat

The Department regularly coordinates with the Intelligence Community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has engaged with state and local officials, as well as relevant private sector entities, to assess the scale and

scope of malicious cyber activity potentially targeting the U.S. election infrastructure.

Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

In addition to working directly with state and local officials over the past two years, we have partnered with trusted third parties to analyze relevant cyber data, including the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the National Association of Secretaries of State, and the National Association of State Election Directors.

DHS field personnel deployed around the country furthered information sharing and enhanced outreach.

Enhancing Security

During the 2018 midterms, CISA provided a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure.

Working with election infrastructure stakeholders was essential to ensuring a more secure election.

CISA and our stakeholders increased awareness of potential vulnerabilities and provided capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections.

In partnering with these officials through both new and ongoing engagements, CISA will continue to work to provide value-added—yet voluntary—services to support their efforts to secure elections in the 2020 election cycle.

Improving Coordination with State, Local, Tribal, Territorial and Private Sector Partners

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience, but also exposes systems to cybersecurity risks, just like in any other enterprise environment.

Just like with other sectors, CISA helps stakeholders in federal departments and agencies, state, local, tribal, and territorial (SLTT) governments, and the private sector to manage these cybersecurity risks.

Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

CISA works with the EI-ISAC to provide threat and vulnerability information to state and local officials. Through funding by CISA, the Center for Internet Security created and continues to operate the EI-ISAC.

The EI-ISAC has representatives co-located with CISA's National Cybersecurity and Communications Integration Center (NCCIC) to enable regular collaboration and access to information and services for election officials.

Providing Technical Assistance and Sharing Information

Knowing what to do when a security incident happens—whether physical or cyber—before it happens, is critical. CISA supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks.

Crisis communications is a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively when an incident unfolds.

In some cases, we do this directly with state and local jurisdictions. In others, we partner with outside organizations.

We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission. CISA actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, CISA provides a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments. These in-depth, on-site evaluations include a

system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage election officials to report suspected malicious cyber activity to NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the Federal Government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Information sharing: CISA maintains numerous platforms and services to share relevant information on cyber incidents. Election officials may also receive information directly from the NCCIC. The NCCIC also works with the EI-ISAC, allowing election officials to connect with the EI-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems.

Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the information sharing and use of such cybersecurity threat indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide as much intelligence as possible at the lowest classification level possible. While DHS prioritizes declassifying information to the extent possible, DHS also provides classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances.

Field-based cybersecurity advisors and protective security advisors: CISA has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: CISA provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

Election Security Efforts Leading up to the 2018 Midterms

In the weeks leading up to the 2018 midterm elections, DHS officials supported a high degree of preparedness nationwide. DHS provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns.

EI-ISAC threat alerts were shared with all 50 states, over 1,400 local and territorial election offices, 6 election associations, and 12 election venders.

In August 2018, DHS hosted a "Tabletop the Vote" exercise, a three-day, first-of-its-kind exercise to assist our federal partners, state and local election officials, and private sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery.

Through tabletop simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and the integrity of elections. Partners for this exercise included 44 states and the District of Columbia; EAC; Department of Defense, including the Office of the Secretary of Defense, U.S. Cyber Command, and the National Security Agency; DOJ; Federal Bureau of Investigation; Office of the Director of National Intelligence; and National Institute of Standards and Technology (NIST).

Through the "Last Mile Initiative," DHS worked closely with state and local governments to outline critical cybersecurity actions that should be implemented at the county level. For political campaigns, DHS disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, DHS deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers.

DHS also hosted the National Cybersecurity Situational Awareness Room, an online portal for state and local election officials and vendors that

facilitates rapid sharing of information. It gives election officials virtual access to the 24/7 operational watch floor of the CISA NCCIC. This setup allowed DHS to monitor potential threats across multiple states at once and respond in a rapid fashion.

Our goal has been for the American people to enter the voting booth with the confidence that their vote counts and is counted correctly. I am proud to say that our efforts over the past two years have resulted in the most secure election in modern history.

No Evidence of Election Interference

The Secretary of Homeland Security and the Acting Attorney General have concluded that there is no evidence to date that any identified activities of a foreign government or foreign agent had a material impact on the integrity or security of election infrastructure or political or campaign infrastructure used in the 2018 midterm elections for the United States Congress.

The activity we did see was consistent with what we shared in the weeks leading up to the election. Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests.

Election Security Efforts Moving Forward

Ensuring the security of our electoral process remains a vital national interest and one of our highest priorities at DHS.

In the run up to the 2020 election season, DHS will continue to prioritize elections by broadening the reach and depth of information sharing and assistance that we are providing to state and local election officials, and continuing to share information on threats and mitigation tactics.

DHS goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with the National Institute of Standards and Technology (NIST) and the states to develop cybersecurity profiles utilizing the NIST Cybersecurity Framework for Improving Critical Infrastructure. We will also continue to engage any political entity that wants our help. DHS offers these entities the same tools and resources that we offer to state and local election officials, including trainings, cyber hygiene support, information sharing, and other resources.

DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks.

Just last week, DHS officials provided updates to the secretaries of state, state election directors, and members of the GCC and SCC on the full package of election security resources that are available from the Federal government, along with a roadmap on how to improve coordination across these entities.

DHS also worked with our Intelligence Community partners to provide a classified one day read-in for these individuals regarding the current threats facing our election infrastructure.

We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure.

However, we recognize that there is a significant technology deficit across SLTT governments, and state and local election systems, in particular.

It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

Our voting infrastructure is diverse, subject to local control, and has many checks and balances.

As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

Note

Christopher Krebs serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs was originally sworn in on June 15, 2018 as the Under Secretary for the predecessor of CISA, the National Protection and Programs Directorate (NPPD). Mr. Krebs was nominated for that position by President Trump in February 2018.

Before serving as CISA Director, Mr. Krebs was appointed in August 2017 as the Assistant Secretary for Infrastructure Protection. In the absence of a

permanent NPPD Under Secretary at the time, Mr. Krebs took on the role of serving as the Senior Official Performing the Duties of the Under Secretary for NPPD until he was subsequently nominated as the Under Secretary and confirmed by the Senate the following year.

Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

Before Microsoft, Mr. Krebs advised industry and Federal, State, and local government customers on a range of cybersecurity and risk management issues. This is his second tour working at DHS, previously serving as the Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs.

As Director, Mr. Krebs oversees CISA's efforts to defend civilian networks, secure federal facilities, manage systemic risk to National critical functions, and work with stakeholders to raise the security baseline of the Nation's cyber and physical infrastructure.

Mr. Krebs holds a bachelor's degree in environmental sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

Number 9

Record fine handed to TikTok following data privacy issues

National Cyber Security Centre
a part of GCHQ

The video sharing app, TikTok, has received the largest ever fine recorded in a US case following issues with its management of children's data privacy.

Musical.ly app, which was later acquired and incorporated into TikTok, was handed a $5.7m fine because it was knowingly hosting content that had been published by underage users.

The company has accepted the fine and will implement new measures to handle users who are under the age of 13.

Additionally, TikTok have been ordered to delete the data and users in the US will have to verify their age when opening the app.

The issue here however is that users can simply lie about their date of birth to gain access.

The firm commented: "We care deeply about the safety and privacy of our users. This is an ongoing commitment, and we are continuing to expand and evolve our protective measures in support of this."

Users of the app outside of the US should be aware that these measures will not be implemented in other countries with the settlement only applied to the US.

TikTok was one of the most downloaded apps last year and it said to have more than one billion users worldwide.

Social media continues to be a huge part of modern digital life and it's important to ensure you and your loved ones are secure on the various platforms.

The NCSC has published advice on how to use social media safely at:
https://www.beta.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Advice from social media platforms

The following guidance is provided by each of the major social media platforms. Click to read detailed information.

- **Facebook**: basic privacy settings and tools
- **Twitter**: how to protect and unprotect your Tweets
- **YouTube**: privacy and safety
- **Instagram**: privacy settings and information
- **LinkedIn**: account and privacy settings overview
- **Snapchat**: privacy settings

Number 10

A Privacy-Focused Vision for Social Networking

My focus for the last couple of years has been understanding and addressing the biggest challenges facing Facebook. This means taking positions on important issues concerning the future of the internet.

In this note, I'll outline our vision and principles around building a privacy-focused messaging and social networking platform. There's a lot to do here, and we're committed to working openly and consulting with experts across society as we develop this.

•••

Over the last 15 years, Facebook and Instagram have helped people connect with friends, communities, and interests in the digital equivalent of a town square. But people increasingly also want to connect privately in the digital equivalent of the living room.

As I think about the future of the internet, I believe a privacy-focused communications platform will become even more important than today's open platforms. Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks.

Today we already see that private messaging, ephemeral stories, and small groups are by far the fastest growing areas of online communication.

There are a number of reasons for this. Many people prefer the intimacy of communicating one-on-one or with just a few friends. People are more cautious of having a permanent record of what they've shared. And we all expect to be able to do things like payments privately and securely.

Public social networks will continue to be very important in people's lives -- for connecting with everyone you know, discovering new people, ideas and content, and giving people a voice more broadly.

People find these valuable every day, and there are still a lot of useful services to build on top of them. But now, with all the ways people also

want to interact privately, there's also an opportunity to build a simpler platform that's focused on privacy first.

I understand that many people don't think Facebook can or would even want to build this kind of privacy-focused platform -- because frankly we don't currently have a strong reputation for building privacy protective services, and we've historically focused on tools for more open sharing. But we've repeatedly shown that we can evolve to build the services that people really want, including in private messaging and stories.

I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever. This is the future I hope we will help bring about.

We plan to build this the way we've developed WhatsApp: focus on the most fundamental and private use case -- messaging -- make it as secure as possible, and then build more ways for people to interact on top of that, including calls, video chats, groups, stories, businesses, payments, commerce, and ultimately a platform for many other kinds of private services.

This privacy-focused platform will be built around several principles:

Private interactions. People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share.

Encryption. People's private communications should be secure. End-to-end encryption prevents anyone -- including us -- from seeing what people share on our services.

Reducing Permanence. People should be comfortable being themselves, and should not have to worry about what they share coming back to hurt them later. So we won't keep messages or stories around for longer than necessary to deliver the service or longer than people want them.

Safety. People should expect that we will do everything we can to keep them safe on our services within the limits of what's possible in an encrypted service.

Interoperability. People should be able to use any of our apps to reach their friends, and they should be able to communicate across networks easily and securely.
Secure data storage. People should expect that we won't store sensitive data in countries with weak records on human rights like privacy and

freedom of expression in order to protect data from being improperly accessed.

Over the next few years, we plan to rebuild more of our services around these ideas. The decisions we'll face along the way will mean taking positions on important issues concerning the future of the internet.

We understand there are a lot of tradeoffs to get right, and we're committed to consulting with experts and discussing the best way forward. This will take some time, but we're not going to develop this major change in our direction behind closed doors.

We're going to do this as openly and collaboratively as we can because many of these issues affect different parts of society.

To read more:
https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

Number II

Cybersecurity Disclosure Act of 2019?

Will publicly traded companies be required to disclose to investors whether any members of their board of directors have cybersecurity expertise?

A BILL

To amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Disclosure Act of 2019".

To read more:
https://www.congress.gov/116/bills/s592/BILLS-116s592is.pdf

Number 12

Progress on Lifelong Learning Machines Shows Potential for Bio-Inspired Algorithms

USC milestone on L2M program shows how machines could be capable of learning through experience

Today's machine learning systems are restricted by their inability to continuously learn or adapt as they encounter new situations; their programs are fixed after training, leaving them unable to react to new, unforeseen circumstances once they are fielded.

Adding new information to cover programming deficits overwrites the existing training set.

With current technology, this requires taking the system offline and retraining it on a dataset that incorporates the new information.

It is a long and arduous process that DARPA's Lifelong Learning Machines (L2M) program is working to overcome.

"The L2M program's prime objective is to develop systems that can learn continuously during execution and become increasingly expert while performing tasks, are subject to safety limits, and capable of applying previous skills and knowledge to new situations, without forgetting previous learning," said Dr. Hava Siegelmann, program manager in DARPA's Information Innovation Office (I2O). "Though complex, it is an area where we are making significant progress."

First announced in 2017, L2M is over a year into research and development of next generation AI systems and their components, as well as learning mechanisms in biological organisms capable of translation into computational processes. L2M supports a large base of 30 performer groups via grants and contracts of different duration and size.

Today, L2M researcher Francisco J. Valero-Cuevas, professor of biomedical engineering and biokinesiology at USC Viterbi School of Engineering, along with USC Viterbi School of Engineering doctoral students Ali Marjaninejad, Dario Urbina-Melendez and Brian Cohn published results regarding exploration into bio-inspired AI algorithms. In an article outlined in the March cover of Nature Machine Intelligence, Valero-Cuevas' team details their successful creation of an AI-controlled robotic limb driven by animal-like tendons capable of teaching itself a

walking task, even automatically recovering from a disruption to its balance.

Behind the USC researchers' robotic limb is a bio-inspired algorithm that can learn a walking task on its own after only five minutes of "unstructured play" – or conducting random movements that enable the robot to learn its own structure as well as its surrounding environment.

The robot's ability to learn-by-doing is a significant advancement towards lifelong learning in machines. The current machine learning approaches rely on pre-programming a system for all potential scenarios, which is complex, labor intensive, and inefficient.

What the USC researchers have accomplished shows that it is possible for AI systems to learn from relevant experience, finding and adapting solutions to challenges overtime.

Siegelmann noted, "We're at a major moment of transition in the field of AI. Current fixed methods underlying today's smart systems will quickly give way to systems capable of learning in the field. The missing ingredients to safer, more flexible, and more useful AI are the abilities to both learn while in operation and to apply learning to new circumstances for which the system was not previously trained. These abilities are necessary, for instance, for complex systems like self-driving cars to become truly functional. Incorporating L2M technologies will allow them to become increasingly expert as they drive in different conditions and will make them safer than human-driven cars. Professor Valero-Curevas and his team have successfully taken us closer to that goal; that's what the L2M project is about."

The full article: https://www.nature.com/articles/s42256-019-0029-0

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.