Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

September 2018, cyber risk and compliance in Switzerland

Dear readers,

The word deepfake is derived from the words “deep” and “fake”. Using artificial intelligence and modern technology, everybody can swap celebrities' faces into porn videos, and put words in politicians' mouths.

Anything else? Yes, it can be much worse. Fake videos or audio recordings that look and sound just like the real ones, can be used in disinformation operations and social engineering. Only imagination is the limit.

In classical conditioning, two stimuli can be linked together to produce a response. Developing patterns of stimulus and response can dramatically affect the population.

During the 1890s, Ivan Pavlov observed the salivation in dogs, in response to being fed. But his dogs could begin to salivate whenever he entered the room, even when he was not bringing them food.

Pavlov decided to use a bell as a stimulus. When he gave food to his dogs, he also rang a bell. After some time, the bell on its own caused an increase in salivation.

Pavlov's dog had learned an association between the bell and the food, and a new behaviour had been learned.

Deepfakes can exploit patterns of stimulus and response. Just like the association between the bell and the food, we can have associations between deepfake emergency alerts and responses.

In an interesting letter, Rep. Adam Schiff (D-Calif.), Rep. Stephanie Murphy (D-Fla.) and Rep. Carlos Curbelo (R-Fla.) express their deep

concern that deepfake technology could be deployed by malicious foreign actors. They asked the Director of National Intelligence, Dan Coats, to examine the matter:

Congress of the United States
Washington, DC 20515

September 13, 2018

The Honorable Daniel R. Coats
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Coats:

We request that the Intelligence Community report to Congress and the public about the implications of new technologies that allow malicious actors to fabricate audio, video and still images.

Hyper-realistic digital forgeries — popularly referred to as "deep fakes" — use sophisticated machine learning techniques to produce convincing depictions of individuals doing or saying things they never did, without their consent or knowledge. By blurring the line between fact and fiction, deep fake technology could undermine public trust in recorded images and videos as objective depictions of reality.

You have repeatedly raised the alarm about disinformation campaigns in our elections and other efforts to exacerbate political and social divisions in our society to weaken our nation. We are deeply concerned that deep fake technology could soon be deployed by malicious foreign actors.

Forged videos, images or audio could be used to target individuals for blackmail or for other nefarious purposes. Of greater concern for national security, they could also be used by foreign or domestic actors to spread misinformation. As deep fake technology becomes more advanced and more accessible, it could pose a threat to United States public discourse and national security, with broad and concerning implications for offensive active measures campaigns targeting the United States.

Given the significant implications of these technologies and their rapid advancement, we believe that a thorough review by the Intelligence Community is appropriate, including an assessment of possible counter-measures and recommendations to Congress. Therefore, we request that you consult with the heads of the appropriate elements of the Intelligence Community to prepare a report to Congress, including an unclassified version, that includes:

(a) An assessment of how foreign governments, foreign intelligence services or foreign individuals could use deep fake technology to harm United States national security interests;

(b) A description of any confirmed or suspected use of deep fake technology by foreign governments or foreign individuals aimed at the United States that has already occurred to date;

(c) An identification of technological counter-measures that have been or could be developed and deployed by the United States Government or by the private sector to deter and detect the use of deep fakes, as well as analysis of the benefits, limitations and drawbacks, including privacy concerns, of such counter-technologies;

(d) An identification of the elements of the Intelligence Community that have, or should have, lead responsibility for monitoring the development of, use of and response to deep fake technology;

(e) Recommendations regarding whether the Intelligence Community requires additional legal authorities or financial resources to address the threat posed by deep fake technology;

(f) Recommendations to Congress regarding other actions we may take to counter the malicious use of deep fake technologies; and

(g) Any other information you believe appropriate.

We would appreciate your cooperation in producing this report as soon as feasible, but no later than December 14, 2018. Thank you for your assistance.

Sincerely,

Adam B. Schiff
MEMBER OF CONGRESS

Stephanie Murphy
MEMBER OF CONGRESS

Carlos Curbelo
MEMBER OF CONGRESS

You can find the letter at: https://schiff.house.gov/imo/media/doc/2018-09%20ODNI%20Deep%20Fakes%20letter.pdf

---

Well, this is one of the phrases I often hear: *"Luckily, we are proud to say that we have never been hacked."*

First, I hate the word *luckily*. We cannot rely on good luck for effective cyber risk management. Benjamin Franklin has said that "diligence is the mother of good luck".

Second, I hate the word *proud,* especially because we are lucky.

Third, I hate the word *never*. Never say never. There are exceptions, Confucius believed that "only the wisest and stupidest of men *never* change".

Fourth, *how do they know* that they have never been hacked? How can they be so certain? According to Voltaire "doubt is not a pleasant condition,

but certainty is absurd."

According to Hans-Georg Maassen, head of the Bundesamt für Verfassungsschutz (BfV, the domestic intelligence agency in Germany), intelligence officials are increasingly worried about so-called "cyber bombs" that could be planted in the network of an unsuspecting company and detonated later.

This is true. For decades, sleeper agents are very effective and efficient. Now we have cyber sleeper agents.

Sleeper agents move to the target countries, acquire jobs that give them access to important persons and information, blend into everyday life as normal citizens.

For years they do not communicate with their handlers or other agents. When there is time to wake up, they are part of the system they attack.

Cyber sleeper agents move to the target systems, acquire access and privileges in the system, that give them further access to user accounts and information (horizontal and vertical privilege escalation), blend into everyday system use.

For years they do not communicate with their bot masters. When there is time to wake up, they can disrupt critical government functions, attack the critical infrastructure, steal sensitive information and become part of disinformation operations.

Once upon a time you sold your car, handed over the keys, bought a new car, and thought no more about it. No longer. In today's connected world, you may have just sold a computer on wheels.

This is how the National Cyber Security Centre (NCSC), the UK's authority on cyber security, describes this major issue.

Confucius believed that "the superior man understands what is right; the inferior man understands what will sell." Car salespersons want to sell to everybody, not only to superior persons. They know very well that security is right, but it is not an attractive subject during the sale.

The NCSC continues:

"As of late 2017 there were around 9 million internet-connected cars on UK roads. Most new cars have features that allow the owner to interact with the vehicle, even when nowhere near it. This varies from the ability to set climate control, through to uploading sat nav destination details and more. This information is then stored in the online account associated with the car.

This data is not the only personal information that remains with the car. For instance, phones that have been paired with the car should also be unpaired when the car is sold.

When selling an old phone or device most people would ensure that any personal data on it was completely wiped. The same principle applies when an internet-connected car is sold; it is generally the seller's responsibility to disable the online account that they used with that car.

Many car manufacturers and dealers state this in their terms and conditions. However, some customers may not read them that closely and fail to delete their personal accounts and access.

When the car is then sold on, the previous owner can track and monitor the car's location and other data without the new owner's knowledge.

The key message is to treat a modern car like any other connected device that is being sold: delete all personal data and disable the account that has been used with the car. Privacy is already seen as a key issue with phones, tablets, and laptops. Cars and other internet connected devices should also be added to the list."

Welcome to our monthly newsletter.

Best Regards,

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:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf

Number 1 (Page 11)

Strengthened safeguards against foreign influence on Danish elections and democracy

UDENRIGSMINISTERIET
Ministry of Foreign Affairs of Denmark

The Government seeks to strengthen Danish resilience against foreign attempts to influence our democracy and society.

Uncovering influence campaigns, a high level of preparedness and a closer dialogue with media and political parties on how to manage the threat posed by influence campaigns; these are some of the elements from the Government's new action plan.

Certain countries use influence campaigns targeting the domestic political environments in Western countries as a tool to reach their own foreign policy goals.

Number 2 (Page 16)

Department of Commerce Launches Collaborative *Privacy* Framework Effort

NIST Will Hold Public Workshop on Oct. 16, 2018

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

Innovative technologies such as the "internet of things" (IoT) and artificial intelligence enhance convenience, efficiency and economic growth.

At the same time, these and other technologies increasingly require complex networking environments and use detailed data about individuals that can make protecting their privacy harder.

To help meet this challenge, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) announced that it has launched a collaborative project to develop a voluntary privacy framework to help organizations manage risk.

Number 3 (Page 18)

Senate Select Committee on Intelligence Hearing on "Foreign Influence Operations' Use of Social Media Platforms"

Kent Walker, Senior Vice President, Global Affairs & Chief Legal Officer, Google - Written Congressional Testimony

"Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for the opportunity to provide an update on the efforts we're making to secure our platforms ahead of the 2018 midterm elections in the US and for future elections around the world."

Number 4 (Page 20)

Restoring Trust in Electronic Documents

DARPA program aims to radically improve software's ability to recognize and reject invalid and malicious electronic data

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

The expeditious delivery of electronic documents, messages, and other data is relied on for everything from communications to navigation. As the near instantaneous exchange of information has increased in volume, so has the variety of electronic data formats–from images and videos to text and maps.

Number 5 (Page 22)

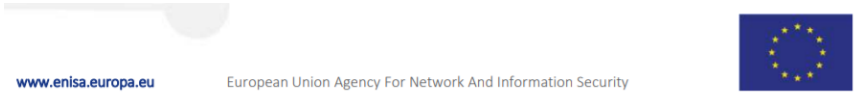
Emotet Malware

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.

Number 6 (Page 24)

Annual report
Telecom security incidents 2017



Electronic communication providers in the EU have to notify significant security incidents to the national telecom regulatory authorities (NRAs) in each EU member state. Every year the NRAs report summaries about a selection of these notified incidents, the most significant incidents, based on a set of agreed thresholds.

Number 7 (Page 27)

The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility

Colonel David Wallace, Lieutenant Colonel Mark Visger

The overarching aim of computer security is to reduce or eliminate risks to an organization's computer networks and cyber infrastructure.

One increasingly common way cybersecurity professionals are defending their networks is through the use of so-called "honeypots".

Number 8 (Page 29)

DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies

DARPA's multi-year strategy seeks contextual reasoning in AI systems to create more trusting, collaborative partnerships between humans and machines

Over its 60-year history, DARPA has played a leading role in the creation and advancement of artificial intelligence (AI) technologies that have produced game-changing capabilities for the Department of Defense.

Number 1

Strengthened safeguards against foreign influence on Danish elections and democracy

UDENRIGSMINISTERIET
Ministry of Foreign Affairs of Denmark

The Government seeks to strengthen Danish resilience against foreign attempts to influence our democracy and society.

Uncovering influence campaigns, a high level of preparedness and a closer dialogue with media and political parties on how to manage the threat posed by influence campaigns; these are some of the elements from the Government's new action plan.

Certain countries use influence campaigns targeting the domestic political environments in Western countries as a tool to reach their own foreign policy goals.

In recent years, a number of examples of Russian attempts to influence elections and referendums in both Europe and the United States have been uncovered.

According to the Danish Defence Intelligence Service, it is very likely that foreign states will also have the ability to conduct influence campaigns targeting Denmark, for instance relating to the upcoming parliamentary elections.

The Government takes this threat posed against Danish interests and democratic values very seriously.

Therefore, the Government presents a plan with 11 initiatives aimed at strengthening Danish resilience against influence campaigns.

An influence campaign can for instance include attempts to spread untrue information and stories in the media or to create a distorted coverage of a topic in order to influence an important political decision.

These kind of campaigns are often designed to create discord amongst the population and seek to undermine the trust in for instance elections or public institutions.

Minister of Justice Søren Pape Poulsen:

"With the risk of influence campaigns, we are facing a threat against our liberal democracy which we need to firmly address.

We therefore now launch this action plan to ensure that our government authorities, democracy and media are better prepared if foreign countries attempt to influence important decisions of high significance to Denmark.

Denmark's security and safety is the top priority for me as Minister of Justice, and today we take another step to protect these particular values."

Minister of Foreign Affairs Anders Samuelsen:

"It is basically a question of defending our liberty and democracy. Russian influence campaigns targeting elections in the United States and France show the importance of staying abreast of this development.

That is why we act now. The Danish people must remain completely confident in our democracy.

Many of our allies are in the same situation. It is important to me that we also draw on their experiences to ensure that we stand united and as strong as possible against the threat."

Minister of Defence Claus Hjort Frederiksen:

"We have by now seen a number of examples of Kremlin attempts to influence democratic elections in the West with campaigns focusing on creating discord and disagreement in the population.

They focus on existing political dilemmas or even seek to amplify points of views on both sides on a conflict – solely with the purpose of creating discord and undermine trust in in our political institutions, authorities and ultimately within the population itself.

I am not particularly nervous for the polling itself or the counting of votes in this country because we have a robust system which is difficult to "hack" so to speak. However, we have seen how Russia has interfered with democratic elections in the United States and France.

Which effect it has had, we can only imagine. But it must never happen in Denmark. The Government's action plan is therefore an important element in strengthening our ability to counter influence operations against

Denmark – including, but not limited to, the upcoming parliamentary election."

The elections action plan consists of 11 initiatives, which concern the general work by public authorities to counter influence campaigns, secure the election itself, council the main actors of the election and initiate closer cooperation with relevant actors in the media and social media:

1. The Government has set up an inter-governmental task force, which has strengthened the authorities' coordination and efforts in countering influence campaigns, including with regard to Danish elections.

Drawing on experiences from abroad, a number of initiatives have been launched in order to increase capacities in the relevant authorities and to develop concrete countermeasures.

2. The Ministry of Foreign Affairs has launched a strengthened monitoring of disinformation in the media directed at Denmark and will – inspired by other Nordic countries – initiate training for communication officers from government authorities on the ongoing handling of disinformation.

3. The Danish Security Intelligence Service (DSIS) and the Danish Defence Intelligence Service (DDIS) strengthen their focus on hostile foreign actors targeting Denmark with influence campaigns, including with regard to the upcoming parliamentary elections.

4. The Ministry for Economic Affairs and the Interior will in cooperation with DSIS and DDIS/The Centre for Cyber Security (CFCS) ensure that the necessary threat and vulnerability assessments are conducted in relation to the election.

5. The Ministry for Economic Affairs and the Interior's response with regard to the election will have an increased focus on threats posed by potential foreign influence.

The work will be organised in close cooperation with the appointed inter-governmental task force, especially DSIS and DDIS/CFCS.

6. The Government will offer all political parties eligible to be elected to Parliament counselling on the risk of foreign influence in relation to the upcoming parliamentary elections, including cyber-attacks, and on the options for countering such influence and attacks.

The counselling will be offered through the national security authorities (DSIS and DDIS/CFSC).

7. The Government will invite all political party leaders to a meeting to inform about the risk of foreign influence with regard to the upcoming parliamentary elections.

8. The Government will invite representatives from the media to a dialogue on possible models for cooperation on countering potential foreign attempts to influence the upcoming parliamentary elections.

This will happen with full respect for the central principles of a free and independent press.

9. The Government will invite representatives from prevalent social media platforms to a dialogue on possible models for cooperation on countering potential foreign attempts to influence the upcoming parliamentary elections.

This initiative will amongst other things be based on experiences from other countries.

10. The Government will invite media with public service obligations to a dialogue on models for cooperation on countering potential foreign attempts on influencing the upcoming parliamentary elections.

One of the aims being to raise awareness about the threat amongst the population.

11. The Government will present a bill to ensure that the criminal code is up to date to protect Denmark against the threat from influence campaigns launched by foreign intelligence services.

Facts:

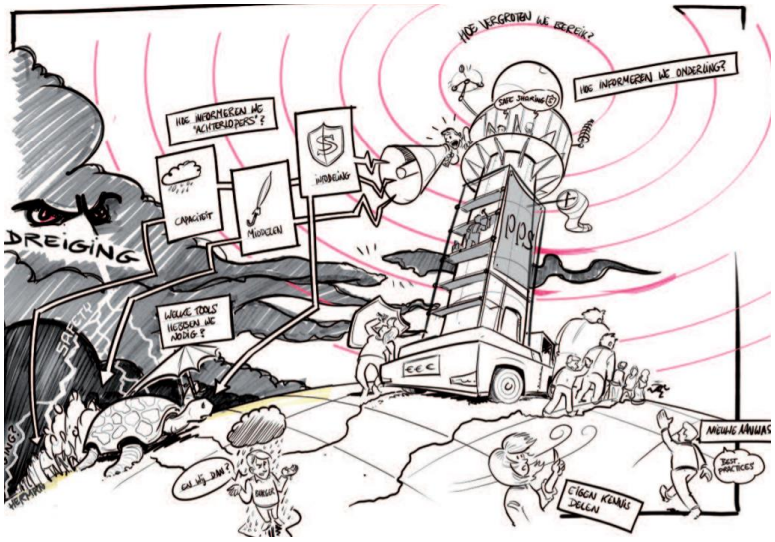
In its Intelligence Risk Assessment from 2017, Danish Defence Intelligence Service assesses that it is likely that Russian influence campaigns will pose an increased threat against Denmark.

Denmark could with short notice or no notice at all be target of Russian influencing attempts.

It is highly likely that Russia will be able to target and tailor influence campaigns against Denmark.

Russian influence could for instance happen in relation to an election campaign or as a result of a broader Russian interest in influencing the state of affairs in the Baltic Sea Region to its own advantage.
It is in this regard likely that Russia's strengthened influence operations in for instance the Baltic states, Sweden and Finland also will lead to an increased focus on Denmark.

To read more:
https://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2017_EnglishVersion.pdf



The attack on Danish Defence email system

In 2015 and 2016, a hacker group known as APT28, among other names, believed by the public to operate on behalf of the Russian intelligence service, compromised a Danish Defence email system used for non-classified communication.
Defence staff members were lured into entering their usernames and passwords on fake login pages, thereby allowing the actor access through the real login pages.

Number 2

Department of Commerce Launches Collaborative *Privacy* Framework Effort

NIST Will Hold Public Workshop on Oct. 16, 2018

Innovative technologies such as the "internet of things" (IoT) and artificial intelligence enhance convenience, efficiency and economic growth.

At the same time, these and other technologies increasingly require complex networking environments and use detailed data about individuals that can make protecting their privacy harder.

To help meet this challenge, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) announced that it has launched a collaborative project to develop a voluntary privacy framework to help organizations manage risk.

"We've had great success with broad adoption of the NIST Cybersecurity Framework, and we see this as providing complementary guidance for managing privacy risk," said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan.

"The development of a privacy framework through an open process of stakeholder engagement is intended to deliver practical tools that allow continued U.S. innovation, together with stronger privacy protections."

The envisioned privacy framework (https://www.nist.gov/privacy-framework) will provide an enterprise-level approach that helps organizations prioritize strategies for flexible and effective privacy protection solutions so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust.

Parallel with this effort, Commerce's National Telecommunications and Information Administration is developing a domestic legal and policy approach for consumer privacy in coordination with the department's International Trade Administration to ensure consistency with international policy objectives.

To collect input from stakeholders, NIST will kick off the effort with a public workshop on Oct. 16, 2018, in Austin, Texas—in conjunction with the International Association of Privacy Professionals' Privacy. Security. Risk. 2018 conference.

Good cybersecurity practices are central to managing privacy risk but are not sufficient. According to NIST's description of the new project, organizations need access to additional tools to better address the full scope of privacy risk.

"Consumers' privacy expectations are evolving at the same time that there are multiplying visions inside and outside the U.S. about how to address privacy challenges," said NIST Senior Privacy Policy Advisor and lead for the project, Naomi Lefkovitz.

"NIST's goal is to develop a framework that will bridge the gaps between privacy professionals and senior executives so that organizations can respond effectively to these challenges without stifling innovation."

The Austin public workshop is the first in a series planned to collect current practices, challenges and needs in managing privacy risks in ways that go beyond common cybersecurity practices.

Over the coming year, through these workshops and other outreach efforts, said Lefkovitz, "we want to gather the best ideas from many stakeholders so that the privacy framework tool we develop is useful and effective for a wide range of organizations."

NIST has also posted an overview of the development schedule for this framework. To learn more, and to register for the Austin public workshop, visit the event website by Oct. 9, 2018.

The workshop will be recorded and shared on the Privacy Framework website.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

NIST is a non-regulatory agency of the U.S. Department of Commerce. To learn more about NIST, visit www.nist.gov.

To read more:
https://www.nist.gov/privacy-framework

Number 3

Senate Select Committee on Intelligence
Hearing on "Foreign Influence Operations' Use of Social Media Platforms"

Kent Walker, Senior Vice President, Global Affairs & Chief Legal Officer, Google - Written Congressional Testimony

Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for the opportunity to provide an update on the efforts we're making to secure our platforms ahead of the 2018 midterm elections in the US and for future elections around the world.

My name is Kent Walker. I am Senior Vice President, Global Affairs and Chief Legal Officer at Google, and I lead our Legal, Policy, Trust and Safety, and Google.org teams.

I've worked at the intersection of technology, security, and the law for over 25 years, including time spent early in my career as an Assistant US Attorney at the Department of Justice focusing on technology crimes.

We believe that we have a responsibility to prevent the misuse of our platforms and we take that very seriously.

Google was founded with a mission to organize the world's information and make it universally accessible and useful.

The abuse of the tools and platforms we build is antithetical to that mission.

In my testimony to the Committee last fall (https://www.intelligence.senate.gov/sites/default/files/documents/os-kwalker-110117.pdf), I described the investigation we had conducted to understand whether individuals apparently connected to government-backed entities were using our products to disseminate information with the purpose of interfering with the 2016 US election.

We based that review on research into misinformation campaigns

from our Jigsaw group, our information security team's own methods, and leads provided by other companies.
We identified limited activity and we took swift action, disabling any accounts we found.

To read more:
http://services.google.com/fh/files/blogs/kent_walker_testimony_senate_select_committee_on_intelligence_09052018.pdf

Number 4

Restoring Trust in Electronic Documents

DARPA program aims to radically improve software's ability to recognize and reject invalid and malicious electronic data

The expeditious delivery of electronic documents, messages, and other data is relied on for everything from communications to navigation. As the near instantaneous exchange of information has increased in volume, so has the variety of electronic data formats–from images and videos to text and maps.

Verifying the trustworthiness and provenance of this mountain of electronic information is an exceedingly difficult task as individuals and organizations routinely engage with data shared by unauthenticated and potentially compromised sources.

Further, the software used to process electronic data is error-prone and vulnerable to exploitation through maliciously crafted data inputs, opening the technology and its underlying systems to compromise.

An attacker's ability to deliver novel cyberattacks via electronic documents, messages, and streaming data formats appears unbounded, creating an unsustainable situation for software security.

To reduce the sizable attack surface created across consumer, enterprise, and critical infrastructure systems and to help tackle the threat posed by unauthenticated and potentially compromised electronic data, DARPA announced a new program called Safe Documents (SafeDocs).

The goal of the SafeDocs program is to dramatically improve software's ability to detect and reject invalid or maliciously crafted input data, without impacting the key functionality of new and existing electronic data formats.

"With today's online risk environment, allowing software to interact with untrusted electronic documents and messages is akin to downloading and running untrusted programs on your computer," said Sergey Bratus, the DARPA Information Innovation Office (I2O) program manager leading SafeDocs. "To create a safer internet, we must first create safer electronic

documents. Through SafeDocs, we are looking for ways to reduce the complexity of electronic document exchange and minimize the means of exploitation for all malicious actors–from cybercriminals to nation states."

SafeDocs seeks to create technological assurance that an electronic document or message is automatically checked and safe to open, while also generating safer document formats that are subsets of current, untrustworthy versions. To accomplish its goals, the program will focus on two primary technical research thrusts.

The first thrust seeks to develop methodologies and tools for capturing and defining human-intelligible, machine-readable descriptors of electronic data formats.

To do this, researchers will explore means of extracting the de facto syntax of existing data formats and identifying each format's simpler subset that can be parsed safely and unambiguously, and used in verified programming without impacting the format's essential functionality.

Under the second technical thrust, researchers will create software construction kits for building secure, verified parsers, using the simplified format subsets where the existing format's inherent complexity or ambiguity has been reduced for safety.

Parsers, which are used to break data inputs down into manageable objects for further processing, can contain exploitable flaws and behaviors. Research under this thrust will strive to create the methodologies and tools needed to build high-assurance and verifiable parsers for new and existing data formats to help reduce the technology's chances of compromise.

For additional information:
https://www.fbo.gov/index?s=opportunity&mode=form&id=dd089906ecc1c3417a7ef399a0510cc7&tab=core&_cview=0

A full description of the program will be made available in a forthcoming Broad Agency Announcement.

Number 5

Emotet Malware

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.

This joint Technical Alert (TA) is the result of Multi-State Information Sharing & Analysis Center (MS-ISAC) analytic efforts, in coordination with the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC).

Description

Emotet continues to be among the most costly and destructive malware affecting SLTT governments. Its worm-like features result in rapidly spreading network-wide infection, which are difficult to combat. Emotet infections have cost SLTT governments up to $1 million per incident to remediate.

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Additionally, Emotet is a polymorphic banking Trojan that can evade typical signature-based detection.

It has several methods for maintaining persistence, including auto-start registry keys and services. It uses modular Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities. Furthermore, Emotet is Virtual Machine-aware and can generate false indicators if run in a virtual environment.

Emotet is disseminated through malspam (emails containing malicious attachments or links) that uses branding familiar to the recipient; it has even been spread using the MS-ISAC name.

As of July 2018, the most recent campaigns imitate PayPal receipts, shipping notifications, or “past-due” invoices purportedly from MS-ISAC.

Initial infection occurs when a user opens or clicks the malicious download link, PDF, or macro-enabled Microsoft Word document included in the malspam. Once downloaded, Emotet establishes persistence and attempts to propagate the local networks through incorporated spreader modules.

Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator.

To read more:
https://www.us-cert.gov/ncas/alerts/TA18-201A

Number 6

Annual report
Telecom security incidents 2017

www.enisa.europa.eu European Union Agency For Network And Information Security

Electronic communication providers in the EU have to notify significant security incidents to the national telecom regulatory authorities (NRAs) in each EU member state.

Every year the NRAs report summaries about a selection of these notified incidents, the most significant incidents, based on a set of agreed thresholds.

This document, the Annual Report on Telecom Security Incidents 2017, aggregates the incident reported in 2017, and provides a single EU-wide overview of telecom security incidents in the EU.

Mandatory breach reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011.

The breach reporting in Article 13a focuses on security incidents causing significant outages.

The Commission recently proposed an update of the telecom rules.

The new breach reporting requirements in Article 40 of the Electronic Communications Code have a broader scope, including not only incidents causing outages, but also confidentiality breaches.

Security breach reporting is also mandatory for trust service providers in the EU (under Article 19 of the EIDAS regulation), for Operators of Essential Services in the EU (under Article 14 of the NIS directive) and for Digital Service Providers (under Article 16 of the NIS directive) in the EU.

Key statistics from the 2017 reporting

This year's annual incident report covers 169 incidents, reported by the NRAs across the EU. The reports come from the 28 EU countries and additionally 2 EFTA countries participated.

6 EU countries reported no incidents with significant impact, submitting so-called empty reports.

We highlight some of the statistics:

- Most incidents have an impact on mobile telephony and internet: In 2017 most incidents affected mobile telephony (51% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 when fixed telephony was the most affected.

- Incidents with mobile telephony and mobile internet impact, on average, most users: Incidents affecting mobile internet or mobile telephony affected most users, on average around half a million users per reported incident, around 8% of the national user base. Over the past years we observe is a downward trend, meaning that the average size of reported incidents is decreasing. This could be due to the fact that many EU countries are adopting lower reporting thresholds.

- System failures are the dominant root cause of reported incidents: Most incidents reported were caused by system failures (62% of the incidents) as a root cause. Often these are hardware failures or software bugs.

- Human errors affect (on average) a high number of user connections: In 2017 human errors was the root cause category involving most users affected per incident (around 1.2 million user connections on average).

- Incidents caused by malicious actions are rare: Only a small percentage of reported incidents (2.5% in 2017) was categorized as caused by malicious actions. This percentage reduced by half compared to the previous year (5.1% in 2016).

- System failures are the dominant root cause: In 2017 most incidents were caused by system failures, i.e. more than 62 % had system failure as a root cause. This is in line with previous years (always between 60% and 80%). In the category system failures, software bugs and hardware failures were the most common causes. The assets failing in these cases are most often switches, routers, and power supplies.

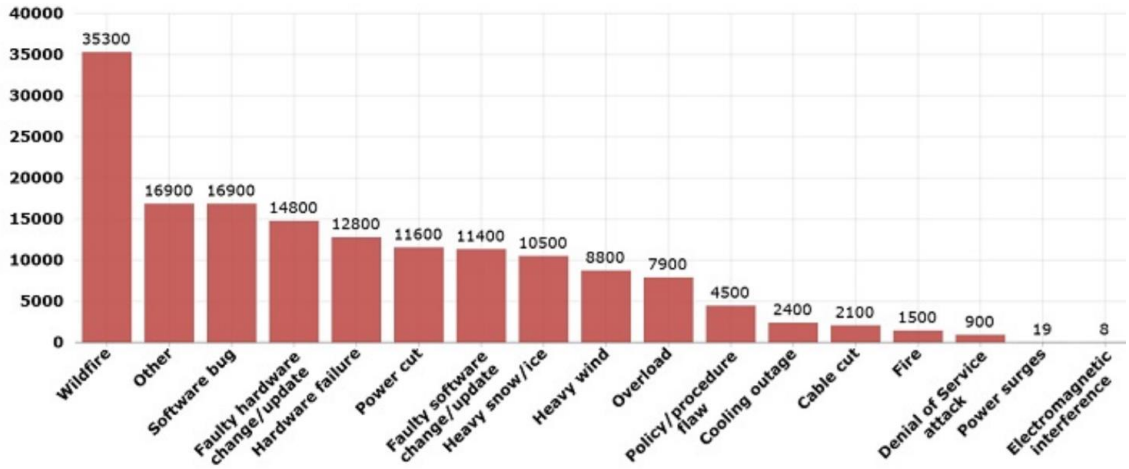
- Natural phenomena are causing more incidents: In 2017 a larger number of incidents (18%) were caused by natural phenomena, such as heavy snow/ice, storms and wild fires. This is significantly higher than 2016, 2015, and 2014 when natural phenomena accounted for around 5% of the incidents. Natural phenomena also cause the highest number

of user hours lost, on average, per incident, with 56800 user hours. Natural phenomena will continue to be a concern for telecom providers across the EU, with extreme weather becoming more common due to climate change.

- A fifth of the incidents are third party failures: Almost a fifth of the incidents (18%) are third party failures. This is similar to last year (22%). Third party failure incidents are interesting for NRAs to investigate further because often third-party failures involve other sectors, and are complex and costly to tackle for providers. Most of the incidents categorized as a third party failures are also categorized as caused by natural phenomena. A common incident scenario is when a natural disaster, like a storm or wildfire, disrupts the power grid infrastructure, which then impacts the mobile network infrastructure.

- Mobile base stations and controllers the most affected assets: Overall, mobile base stations and controllers and mobile switches were the network components most affected by incidents (9% and 8% respectively).

- Wild fires cause, on average, most impact in user hours: A good measure for the total impact is to multiply the number of users and the number of hours outage: this gives a total number of user hours. The diagram below shows the total number of user hours lost, per detailed cause, for the incidents reported in 2017.



To read more:
https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017

Number 7

The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility

Colonel David Wallace
Lieutenant Colonel Mark Visger

VOLUME 3 ◆ NUMBER 2 SUMMER 2018

THE CYBER DEFENSE REVIEW

The overarching aim of computer security is to reduce or eliminate risks to an organization's computer networks and cyber infrastructure.

One increasingly common way cybersecurity professionals are defending their networks is through the use of so-called "honeypots".

The term honeypot has come to mean a deception technique to defend computer systems against malicious operations.

Generally, it is an information system resource whose value lies in its unauthorized or illicit use by a hacker.

In essence, it is a virtual sting operation.

Honeypots can also be weaponized. That is, a honeypot includes files that contain malware that, once exfiltrated by intruders, will cause significant damage and disruption to the intruders' computer networks.

The legal issues associated with the use of weaponized honeypots under international law are complex, multi-faceted, and unsettled.

This article investigates the legality of using weaponized honeypots under the international law of State responsibility.

More specifically, the precise issue addressed is whether the use of weaponized honeypots is an internationally wrongful act under the customary law of State responsibility?

Ultimately, the answer to the question is “it depends” on the facts and circumstances of a given situation.

However, as the analysis below shows, a State should proceed with caution before employing them.

To read more:
Page 34 / 142 of:
https://cyberdefensereview.army.mil/Portals/6/CDR_V3N2_SUMMER-2018_Complete.pdf

Number 8

DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies

DARPA's multi-year strategy seeks contextual reasoning in AI systems to create more trusting, collaborative partnerships between humans and machines

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Over its 60-year history, DARPA has played a leading role in the creation and advancement of artificial intelligence (AI) technologies that have produced game-changing capabilities for the Department of Defense.

Starting in the 1960s, DARPA research shaped the first wave of AI technologies, which focused on handcrafted knowledge, or rule-based systems capable of narrowly defined tasks.

While a critical step forward for the field, these systems were fragile and limited. Starting in the 1990s, DARPA helped usher in a second wave of AI machine learning technologies that created statistical pattern recognizers from large amounts of data.

The agency's funding of natural language understanding, problem solving, navigation and perception technologies has led to the creation of self-driving cars, personal assistants, and near-natural prosthetics, in addition to a myriad of critical and valuable military and commercial applications.

However, these second wave AI technologies are dependent on large amounts of high quality training data, do not adapt to changing conditions, offer limited performance guarantees, and are unable to provide users with explanations of their results.

To address the limitations of these first and second wave AI technologies, DARPA seeks to explore new theories and applications that could make it possible for machines to adapt to changing situations.

DARPA sees this next generation of AI as a third wave of technological advance, one of contextual adaptation.

To better define a path forward, DARPA is announcing today a multi-year investment of more than $2 billion in new and existing programs called the "AI Next" campaign.

Agency director, Dr. Steven Walker, officially unveiled the large-scale effort during closing remarks today at DARPA's D60 Symposium taking place Wednesday through Friday at the Gaylord Resort and Convention Center in National Harbor, Maryland.

"With AI Next, we are making multiple research investments aimed at transforming computers from specialized tools to partners in problem-solving," said Dr. Walker. "Today, machines lack contextual reasoning capabilities, and their training must cover every eventuality, which is not only costly, but ultimately impossible. We want to explore how machines can acquire human-like communication and reasoning capabilities, with the ability to recognize new situations and environments and adapt to them."

DARPA is currently pursing more than 20 programs that are exploring ways to advance the state-of-the-art in AI, pushing beyond second-wave machine learning techniques towards contextual reasoning capabilities.

In addition, more than 60 active programs are applying AI in some capacity, from agents collaborating to share electromagnetic spectrum bandwidth to detecting and patching cyber vulnerabilities.

Over the next 12 months, DARPA plans to issue multiple Broad Agency Announcements for new programs that advance the state of the art in AI.

Under AI Next, key areas to be explored may include automating critical DoD business processes, such as security clearance vetting in a week or accrediting software systems in one day for operational deployment; improving the robustness and reliability of AI systems; enhancing the security and resiliency of machine learning and AI technologies; reducing power, data, and performance inefficiencies; and pioneering the next generation of AI algorithms and applications, such as "explainability" and commonsense reasoning.

In addition to new and existing DARPA research, a key component of the campaign will be DARPA's Artificial Intelligence Exploration (AIE) program, first announced in July 2018.

“In today’s world of fast-paced technological advancement, we must work to expeditiously create and transition projects from idea to practice,” said Dr. Walker.

Accordingly, AIE constitutes a series of high-risk, high payoff projects where researchers will work to establish the feasibility of new AI concepts within 18 months of award.

Leveraging streamlined contracting procedures and funding mechanisms will enable these efforts to move from proposal to project kick-off within three months of an opportunity announcement.

For more information about AI Next, you may visit:
http://www.darpa.mil/work-with-us/ai-next-campaign

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.