



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

*June 2018, cyber risk and compliance in Switzerland*

Dear readers,

A nanotech sensor turns molecular fingerprints into bar codes.

A new system developed at the École Polytechnique Fédérale de Lausanne (EPFL) can detect and analyze molecules with very high precision and without needing bulky equipment.



It opens the door to large-scale, [image-based detection](#) of materials aided by artificial intelligence. The research has been published in Science.

Infrared spectroscopy is the benchmark method for detecting and analyzing organic compounds.

But it requires complicated procedures and large, expensive instruments, making device miniaturization challenging and hindering its use for some industrial and medical applications and for data collection out in the field, such as for measuring pollutant concentrations.

Furthermore, it is fundamentally limited by low sensitivities and therefore requires large sample amounts.

However, scientists at EPFL's School of Engineering and at Australian National University (ANU) have developed a compact and sensitive nanophotonic system that [can identify a molecule's absorption characteristics](#) without using conventional spectrometry.

The scientists have already used their system to detect polymers, pesticides and organic compounds.

What's more, it is compatible with CMOS technology.

To learn more, you may visit:

<https://actu.epfl.ch/news/a-nanotech-sensor-turns-molecular-fingerprints-int/>



We have some really good developments in the European Union. I follow carefully every step for some years, and I am pleased they are effective and efficient.

The [High Representative](#) for the Common Foreign and Security Policy was originally created under the Amsterdam Treaty. The Lisbon Treaty maintained the function of the High Representative for Foreign Affairs and Security Policy.

The High Representative conducts the Common Foreign and Security Policy, including the Common Security Defence policy, presides over the Foreign Affairs Council and is one of the vice-presidents of the European Commission.

The [Hybrid Fusion Cell](#) has been established within the [European External Action Service](#), as a single EU point of focus for Hybrid Threat Analysis.

The High Representative will *expand* the EU Hybrid Fusion Cell with specialised Chemical, Biological, Radiological and Nuclear, [Counter Intelligence as well as Cyber](#) analytical components.

EU Member States are increasing their intelligence contributions to the [EU Intelligence and Situation Centre \(INTCEN\)](#), to permit deeper analysis of potential threats.

According to the new joint communications paper “Increasing resilience and bolstering capabilities to address hybrid threats” (number 1 in our top 10 list), an important challenge with respect to hybrid threats, is to raise awareness and [educate the general public](#) to discern information from disinformation.

[Election periods](#) have proven to be a particularly strategic and sensitive target for cyber enabled attacks and online circumvention of conventional ("off-line") safeguards and rules, such as silence periods, transparent funding rules, and equal treatment of candidates.

This has included attacks against electoral infrastructures and [campaign IT systems](#), as well as [politically-motivated mass online disinformation campaigns](#) and cyber-attacks by third countries with the aim to discredit and delegitimise democratic elections.

This is an interesting development. We spend so much time understanding and implementing measures and countermeasures. Plato believed that only the dead have seen the end of war.

Read more at Number 1 below.



We have a very interesting consultative document from the Financial Stability Board (FSB): “Recommendations for consistent national reporting of data on the use of compensation tools to address [misconduct risk](#).”

We read: “For the purposes of this document, [misconduct is defined](#) as “conduct that falls short of expected standards, including legal, professional, internal conduct and ethical standards” (please see also footnote 9).

You guessed it. Immediately after reading that, I visited footnote 9, where I learned that throughout this document, the term “[misconduct risk](#)” is kept for consistency with the terminology used in the FSB work on measures to address “misconduct risk”. It is however noted that many firms [prefer](#) the use of the term “[conduct risk](#)” as conduct programmes extend well beyond efforts to address misconduct, and increasingly exhibit, for example, measures aimed at promoting positive conduct as well as remediating inappropriate conduct.

I love the creative idea to change “misconduct risk” to “conduct risk”. Positive thinking doesn't mean that you keep your head in the sand and ignore life's less pleasant situations. Sometimes it means that you try to keep the heads of investors in the sand too. No, the FSB paper didn't say that.

[Lao Tzu](#) believed that “when virtue is lost, benevolence appears, when benevolence is lost [right conduct appears](#), when right conduct is lost, expedience appears. Expediency is the mere shadow of right and truth; it is the beginning of disorder.”

I liked footnote 18: “Compensation is just one of the available tools to address misconduct risk. In certain instances, the incentivising/deterrent effect of compensation might not be sufficient, and it may be necessary to resort to other measures such as [disciplinary sanctions](#), [dismissal](#), deferment in career progression, [mandatory training](#), depending on the severity of the misconduct.”

Mandatory training sounds like the scariest option.  
Read more at Number 2 below.



We have a very interesting report that responds to the May 11, 2017, U.S. Executive Order 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

The report defines the [cybersecurity workforce](#) as “members of the workforce with roles and responsibilities that have an impact on an organization’s ability to protect its data, systems, and operations.”

The terms “[cybersecurity jobs](#)” and “[cybersecurity-related jobs](#)” often are used interchangeably in reference to positions held by those who are part of this workforce.

In Executive Order 13800 we had another interesting definition: “[Cybersecurity risk management](#) comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents.”

In the Executive Order 13800 we also had an interesting sentence about *known but unmitigated* vulnerabilities:

“Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities [include](#) using operating systems or hardware beyond the vendor’s support lifecycle, declining to implement a vendor’s security patch, or failing to execute security-specific configuration guidance.”

*Well, too much transparency in information security is not a best*

*practice.*

According to the report:

- There are an estimated 299,000 active openings for cybersecurity - related jobs in the United States as of August 2017. Globally, projections suggest a cybersecurity workforce **shortage of 1.8 million** by 2022.
- Positions needing to be filled **range** from entry-level jobs attainable with minimal credentials, to roles where successful performance is most knowledge-dependent and require advanced academic degrees, multiple certifications, and lengthy on-the-job technical, managerial, and business experience.
- In many instances, employers need workers with specialized knowledge or skills for specific sectors **along with** cybersecurity competencies.
- Employers are **increasingly concerned** about the relevance of cybersecurity related education programs in meeting the needs of their organizations.



Anton Chekhov believed that any idiot can face a crisis, it's day to day living that **wears you out**.

Perhaps this is the reason the European Network and Information Security Agency (ENISA) decided to **wear us out** in their *intense* scenario:

“Imagine this: It is a normal day at the airport. All of a sudden, the automated check-in machines display a system failure. Travel apps on smartphones stop functioning. The agents at the check-in counters cannot operate their computers.

Travellers can neither check in their luggage, nor pass through security checks. There are huge lines everywhere. All flights are shown as cancelled on the airport monitors. For **unknown reasons**, baggage claim has stopped working and more than half of the flights must remain on the ground.

A radical group have reportedly taken control of the airport's critical systems by means of digital and **hybrid attacks**. They have **already claimed**

responsibility for the incident and are using their propaganda channels to spread a call to action and attract more people to adopt their radical ideology.”

This was **the intense scenario** which over 900 European cybersecurity specialists from 30 countries had to face on 6 and 7 June 2018, during the ‘Cyber Europe 2018’ (CE2018) – the most mature EU cybersecurity exercise to date.

I love Europe. Some travellers are annoyed, nobody dies, and this is the **intense** scenario. I assume that **less intense** scenarios could be:

- IoT refrigerators at the airport are hacked, and travellers must drink wine in a temperature that is considered by sommeliers a stigma. (Important note: Bouquets usually take years to develop, so don't mention the word bouquet in your scenario response when you're describing a recent vintage.)
- Attackers steal many mobile devices at the airport. Consider the privacy violations and the liability of the airport after the GDPR regulation.

Read more at Number 4 below.



We also have a very interesting part in the G7 Summit Communiqué.

## The Charlevoix G7 Summit Communiqué

CHARLEVOIX COMMITMENT ON DEFENDING DEMOCRACY FROM  
**FOREIGN THREATS**



We, the Leaders of the G7, share common democratic values that are central to the development of free, open, well-governed, pluralistic and

prosperous societies and recognize that equality is a core component of democracy.

These democratic values are essential for generating broad-based economic growth that benefits everyone, creates quality jobs and ensures opportunities for all.

Democracy and the rules-based international order are **increasingly being challenged** by authoritarianism and the defiance of international norms. In particular, foreign actors seek to undermine our democratic societies and institutions, our electoral processes, our sovereignty and our security.

These malicious, multi-faceted and ever-evolving tactics constitute a **serious strategic threat** which we commit to confront together, working with other governments that share our democratic values.

Defending democracy will require us to adopt a strategic approach that is consistent with universal human rights and fundamental freedoms, our international commitments to peace and security, and that promotes equality.

We welcome the work of G7 Foreign and Security Ministers in Toronto to establish a common understanding of **unacceptable actions by foreign actors** with the malicious intent of undermining our countries' democratic systems as the basis for our collective and individual response.

We, the Leaders of the G7, **commit to:**

- Respond to foreign threats, both together and individually, in order to meet the challenges facing our democracies.
- Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state.
- Establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.
- Share lessons learned and best practices in collaboration with governments, civil society and the private sector that are developing related initiatives including those that promote free, independent and pluralistic media; fact-based information; and freedom of expression.

- Engage directly with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy.
- Support public learning and civic awareness aimed at promoting critical thinking skills and media literacy on intentionally misleading information, and improving online security and safety.
- In accordance with applicable laws, ensure a high level of transparency around sources of funding for political parties and all types of political advertising, especially during election campaigns.

To read more:

<https://g7.gc.ca/wp-content/uploads/2018/06/DefendingDemocracyFromForeignThreats.pdf>

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](mailto:george.lekatis@cyber-risk-gmbh.com)  
Web: [www.cyber-risk-gmbh.com](http://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](http://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf)



*Number 1 (Page 13)***Increasing resilience and bolstering capabilities to address hybrid threats**

HIGH REPRESENTATIVE  
OF THE UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

Hybrid activities by **State and non-state actors** continue to pose a serious and acute threat to the EU and its Member States.

Efforts to **destabilise countries** by undermining public trust in government institutions and by challenging the core values of societies have become more common.

*Number 2 (Page 17)***FSB publicly consults on recommendations for compensation data reporting to address misconduct risk**

The Financial Stability Board (FSB) published a public consultation on Recommendations for **consistent national reporting** of data on the use of compensation tools to address **misconduct risk**.

*Number 3 (Page 19)***GDPR-inspired phishing scams**

The arrival of the new EU General Data Protection Regulation (GDPR) has **gifted scammers** with a new hook for sending phishing emails. Many internet users are now receiving emails from organisations that they have online dealings with, explaining the new regulations and **asking them** for permission to carry on storing their information.

*Number 4 (Page 20)***Cyber Europe 2018 – Get prepared for the next cyber crisis**

EU Cybersecurity Agency ENISA organised an international cybersecurity exercise



Imagine this: It is a normal day at the airport. All of a sudden, the automated check-in machines display a system failure. Travel apps on smartphones stop functioning. The agents at the check-in counters cannot operate their computers.

*Number 5 (Page 23)***Four EU cybersecurity organisations enhance cooperation**

The European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) today signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations.

*Number 6 (Page 26)***A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future**

Transmitted by The Secretary of Commerce and The Secretary of Homeland Security



This report responds to the May 11, 2017, Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

*Number 7 (Page 28)*

## Active Social Engineering Defense (ASED)

Wade Shen




While we focus the vast majority of our security efforts on protecting computers and networks, **more than 80% of cyber attacks and over 70% of those from nation states are initiated by exploiting humans rather than computer or network security flaws.** To build secure cyber systems, it is necessary to protect not only the computers and networks that make up these systems but their human users as well.

*Number 8 (Page 30)*

## Are you Cyber-Savvy?



U.S. SECURITIES AND  
EXCHANGE COMMISSION

 Are You  
Cyber-Savvy?

Take the quiz!

*Number 9 (Page 31)*

European Commission - Statement

## Cybersecurity: Joint Statement by Vice-President Ansip and Commissioner Gabriel on political agreement from the Council



The European Commission welcomes the *political agreement* reached by the Telecommunications Council on a general approach on the Cybersecurity Act, which was presented by President Jean-Claude Juncker in his annual State of the Union Address in 2017.

*Number 10 (Page 33)*

### Drone Forensics Gets a Boost With New Data on NIST Website

*How do you extract forensic data from an aerial drone? Very carefully.*



Aerial drones might someday *deliver* online purchases to your home. But in some prisons, drone delivery is already a thing.

Drones have been spotted flying *drugs, cell phones, and other contraband* over prison walls, and in several cases, drug traffickers have used drones to ferry narcotics across the border.

If those drones are *captured*, investigators will try to extract data from them that might point to a suspect. But there are many types of drones, each with its own quirks, and that can make data extraction tricky.

*Number 11 (Page 36)*

### Cybersecurity Enforcement Actions



U.S. SECURITIES AND  
EXCHANGE COMMISSION

*Number 1*

## Increasing resilience and bolstering capabilities to address hybrid threats



HIGH REPRESENTATIVE  
OF THE UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

Hybrid activities by **State and non-state actors** continue to pose a serious and acute threat to the EU and its Member States.

Efforts to **destabilise countries** by undermining public trust in government institutions and by challenging the core values of societies have become more common.

Our societies face a serious challenge from those who seek to **damage** the EU and its Member States, from cyber-attacks disrupting the economy and public services, through targeted disinformation campaigns to hostile military actions.

Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary.

They are designed to be difficult to detect or attribute and can be used by both state and non-state actors.

The nerve agent attack in **Salisbury** last March further underlined the versatility of hybrid threats and the multitude of tactics now available.

In response, the European Council highlighted the need to step up the capacity of the EU and its Member States to detect, prevent and respond to **hybrid threats** in areas such as cyber, strategic communication and counter-intelligence.

It also drew particular attention to the need for resilience in the face of Chemical, Biological, Radiological and Nuclear-related threats.

The threats posed by non-conventional weapons fall in a category of their own because of the potential scale of the damage they can cause.

As well as being difficult to detect and attribute, they are complex to remedy. Chemical, Biological, Radiological and Nuclear related threats, going [beyond hybrid threats](#) and covering also terrorist threats, are also a general concern of the international community, particularly the evolving risk of proliferation both geographically and to non-State actors.

Strengthening resilience to these threats and bolstering capabilities are predominantly Member State responsibilities.

However, the EU institutions have already taken a number of actions to help to reinforce national efforts.

This has included working in close collaboration with other international actors, including in particular the [North Atlantic Treaty Organisation \(NATO\)](#), and such work could deepen further into support to Member States in areas like rapid response.

This Joint Communication responds to the European Council's invitation to take this work forward.

It is part of a broader package which also includes the latest Security Union progress report, which takes stock and presents next steps in implementing the Chemical, Biological, Radiological and Nuclear Action Plan of October 2017, as well as the Second progress report on the implementation of the 22 actions of the Joint Framework on countering Hybrid Threats – a European Union response.

## The EU response

The Commission and the High Representative have invested consistent efforts to build up the EU's capabilities and effectively support Member States to counter hybrid and Chemical, Biological, Radiological and Nuclear-related threats.

Tangible results have already been achieved in areas such as strategic communications, situational awareness, strengthening preparedness and resilience, and reinforcing crisis response capacities.

The [East Stratcom Task Force](#), established after the March 2015 European Council, has spearheaded work on forecasting, tracking and tackling [disinformation](#) originating from foreign sources.

Its expert analyses and public products<sup>10</sup> have significantly raised awareness about the impact of Russian disinformation.

Over the past two years, it has [uncovered over 4000 individual disinformation cases](#), many of which deliberately targeting Europe.

The work of the East Stratcom Task Force has also focused on the improved delivery of positive communications, with increased outreach in the Eastern Neighbourhood.

Following this success, two other taskforces have been created with different geographic focus - a Task Force for the Western Balkans and a dedicated Task Force South for the Arab-speaking world.

Important steps have been taken to build up structures needed to improve situational awareness and support decision-making.

The [Hybrid Fusion Cell](#) was established within the EU Intelligence and Situation Centre of the European External Action Service in 2016.

The Fusion Cell receives and analyses classified and open source information from different stakeholders concerning hybrid threats.

Over 100 assessments and briefings have been produced to date, shared within the EU and amongst Member States to inform EU decision-making.

The Hybrid Fusion Cell has a close working relationship with the [European Centre of Excellence for Countering Hybrid Threats](#) in Helsinki.

Set up in April 2017 to encourage strategic dialogue and carry out research and analysis on hybrid threats, the Centre of Excellence has now expanded its membership to 16 countries<sup>11</sup> and receives sustained support from the EU.

There have also been important steps in bolstering preparedness and resilience, in particular against Chemical, Biological, Radiological and Nuclear-related threats.

The past six months have seen major steps in [identifying gaps](#) in preparedness for Chemical, Biological, Radiological and Nuclear-related security incidents, notably in terms of detection capacity to help prevent Chemical, Biological, Radiological and Nuclear-attacks.

At the Commission's initiative, a consortium of national experts carried out an analysis of the gaps in the detection equipment for different types of Chemical, Biological, Radiological and Nuclear-related scenarios.

The gap analysis report has been shared with Member States, allowing them to make informed decisions on detection strategies and take operational measures to address the identified gaps.

To read more:

[https://eeas.europa.eu/sites/eeas/files/joint\\_communication\\_increasing\\_resilience\\_and\\_bolstering\\_capabilities\\_to\\_address\\_hybrid\\_threats.pdf](https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf)



*Number 2***FSB publicly consults on recommendations for compensation data reporting to address misconduct risk**

The Financial Stability Board (FSB) published a public consultation on Recommendations for **consistent national reporting** of data on the use of compensation tools to address **misconduct risk**.

Collecting and evaluating compensation data on a regular basis can provide both firms and supervisors with important insights into the effectiveness of compensation programmes and potential areas of weakness.

Currently the gathering and analysis of compensation data **varies significantly** across jurisdictions and firms.

The Recommendations seek to assist national supervisory authorities from all financial sectors by enhancing their capacity to consider and monitor the effectiveness of compensation tools and other mechanisms in promoting good conduct and addressing misconduct risk.

The proposed data set included in the Recommendations is designed to help firms and supervisors answer a number of important questions, **including** whether governance and risk management processes surrounding compensation:

- appropriately include conduct considerations **in the design** of their compensation and incentive systems, including the setting of individual goals, ex ante performance measurement mechanisms and ex post compensation adjustments;
- support the effective use of **compensation tools** to help promote good conduct or to remediate individual conduct that is not in line with the firm's expectations, including holding individuals accountable for any misconduct that occurs;
- promote **wider risk management goals**, including for conduct issues, consistent with the firm's strategy and risk tolerance; and

- support the [effective identification](#) of emerging misconduct risks and where appropriate, review use of incentive systems and compensation decisions in response to conduct incidents to ensure alignment of incentives, risk and reward.

The FSB welcomes comments and responses to the questions set out in the consultative document by Friday 6 July 2018. Responses will be published on the FSB website unless respondents expressly request otherwise.

The FSB has also published today a summary note of an industry workshop organised last December as part of the FSB's work to develop the Recommendations. The FSB also welcomes any feedback on topics discussed at the workshop that are included in the summary note, also by Friday 6 July 2018.

To read more:

<http://www.fsb.org/wp-content/uploads/PO70518-1.pdf>

*Number 3***GDPR-inspired phishing scams**

The arrival of the new EU General Data Protection Regulation (GDPR) has **gifted scammers** with a new hook for sending phishing emails.

Many internet users are now receiving emails from organisations that they have online dealings with, explaining the new regulations and **asking them** for permission to carry on storing their information.

Scammers have taken advantage of this to send fake GDPR-themed emails in an attempt to spread malware or steal personal data.

Apple customers, for example, have been sent a link advising users that their accounts had been “limited” due to unusual activity and then asking them to update their security information.

Users are then directed to a fraudulent webpage where they are asked to input security information. Once this has been completed, users are then directed back to a legitimate Apple web page.

The scammers also used Advanced Encryption Standard (AES) protocols when directing users to the page controlled by them, **bypassing anti-phishing tools** embedded in some antivirus software.

GDPR came into effect **on 25th May 2018**, so the scammers had a short window in which to use GDPR as cover for their activities.

The NCSC has published phishing guidance and you can also read the GDPR security outcomes that have been developed by the NCSC and the Information Commissioners Office (ICO).

The ICO is the UK's supervisory authority for the GDPR and has published a lot of helpful guidance on its website.

To read more:

<https://www.ncsc.gov.uk/phishing>

*Number 4***Cyber Europe 2018 – Get prepared for the next cyber crisis**

EU Cybersecurity Agency ENISA organised an international cybersecurity exercise



Imagine this: It is a normal day at the airport. All of a sudden, the automated check-in machines display a system failure. Travel apps on smartphones stop functioning. The agents at the check-in counters cannot operate their computers.

Travellers can neither check in their luggage, nor pass through security checks. There are huge lines everywhere. All flights are shown as cancelled on the airport monitors. For **unknown reasons**, baggage claim has stopped working and more than half of the flights must remain on the ground.

A radical group have reportedly taken control of the airport's critical systems by means of digital and **hybrid attacks**. They have already claimed responsibility for the incident and are using their propaganda channels to spread a call to action and attract more people to adopt their radical ideology.

This was **the intense scenario** which over 900 European cybersecurity specialists from 30 countries had to face on 6 and 7 June 2018, during the 'Cyber Europe 2018' (CE2018) – the most mature EU cybersecurity exercise to date.

The two-day exercise was orchestrated by ENISA. The participants either stayed at their usual workplace or gathered in crisis cells.

ENISA controlled the exercise via its **Cyber Exercise Platform (CEP)**, which provided a 'virtual universe' (integrated environment) for the simulated world, including incident material, virtual news websites, social media channels, company websites and security blogs.

Organised by the EU cybersecurity agency ENISA in collaboration with cybersecurity authorities and agencies from all over Europe, the CE2018 was intended to enable the European cybersecurity community to further strengthen their capabilities in identifying and tackling large-scale threats

as well as to provide a better understanding of cross-border incident contagion.

Most importantly, CE2018 focused on helping organisations to test their internal business continuity and crisis management plans including media crisis communication, while also reinforcing cooperation between public and private entities.

The scenario contained [real life-inspired](#) technical and non-technical incidents that required network and malware analysis, forensics, and [steganography](#). The incidents in the scenario were designed to escalate into a crisis at all possible levels: organisational, local, national and European.

Mariya Gabriel, Commissioner for the Digital Economy and Society, said:

“Technology offers [countless opportunities](#) in all sectors of our economy. But there are [also risks](#) for our businesses and our citizens.

The European Commission and the Member States must work together and equip themselves with the necessary tools to detect cyber-attacks and protect the networks and systems. This is how ENISA’s ‘Cyber Europe’ exercise was born eight years ago.

It has grown into a major cybersecurity exercise and has become an EU flagship event which brings together hundreds of cybersecurity specialists from all over Europe.

We should [build on this success](#) and I am confident that we can develop further the EU cooperation mechanisms, in particular to respond to large scale cyber incidents.”

Prof. Dr. Udo Helmbrecht, Executive Director of ENISA, explained: “Over the last decade, the aviation sector has made a tremendous leap into the evolving age of technology.

We can now enjoy the benefits of navigational apps, online check-in, and automated baggage screening. Smart technology saves time, money, and makes travellers’ lives easier. However, [just as technology evolves, so do cyber threats](#).

Through events such as the Cyber Europe 2018, our agency strengthens the level of cybersecurity within the EU. European countries and organisations working together as one entity is the modern response to borderless cyber

threats. On behalf of ENISA and its staff, I would like to congratulate everyone involved in the Cyber Europe 2018.”

In the end, the participants were able to mitigate the incidents timely and effectively. This shows that the European cybersecurity sector has matured over the last few years and the actors are much more prepared.

ENISA and the participants will shortly follow up on the exercise and analyse the actions taken to identify areas that could be improved. ENISA will publish a final report in due course.

## Facts at a glance

- Participating countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom
- Participating organisations: approximately 300
- Number of participants: over 900 cybersecurity professionals
- Number of injects: 23 222

## About Cyber Europe exercises

‘Cyber Europe’ exercises are simulations of large-scale cybersecurity incidents that escalate to EU-wide cyber crises. The exercises offer opportunities to analyse advanced cybersecurity incidents, and to deal with complex business continuity and crisis management situations. ENISA has already organised **four** pan-European cyber exercises in 2010, 2012, 2014 and 2016.

International cooperation between all participating organisations is inherent to the gameplay, with most European countries participating. It is a flexible learning experience: from a single analyst to an entire organisation, opt-in and opt-out scenarios, the participants can customise the exercise to their needs.

*Number 5***Four EU cybersecurity organisations enhance cooperation**

The European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) today signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations.



The Memorandum of Understanding was signed by Udo Helmbrecht, ENISA's Executive Director, Jorge Domecq, Chief Executive of the EDA, Steven Wilson, Head of EC3 and Ken Ducatel, CERT-EU's Acting Head.

The MoU aims at **leveraging synergies** between the four organisations, promoting cooperation on cyber security and cyber defence and is a testament to the trusted partnership that exists between these EU agencies. More specifically, it focuses on five areas of cooperation, namely Exchange of information; Education & Training; Cyber exercises; Technical cooperation; and Strategic and administrative matters. It also allows for cooperation in other areas identified as mutually important by the four organisations.

This collaboration will ensure the **best possible use of existing resources** by avoiding duplicative efforts and building on the complementarity of ENISA, EDA, EC3 and CERT-EU. This framework brings added value to the expertise, support and services that these parties provide to the European Union organisations, Member States and all stakeholders concerned.

High Representative/Vice-President and Head of the European Defence Agency, Federica Mogherini said: **“Cyberspace threats do not know of national borders.** Cooperation among Member States but also at European level is therefore essential. Europe is stronger when it tackles threats together, in a common and coordinated approach. And this is exactly where this Memorandum of Understanding is key and where the added value of the European Union lies: working together, joining forces, putting the experiences and the knowledge of all at the service of our citizens' security.”

Vice-President for Digital Single Market Andrus Ansip said: “We can face cyber threats successfully if we have in place a functioning exchange of information, we have strong technical capabilities and we work on basic cyber hygiene. Better cooperation between these EU agencies will lead to this result.”

Commissioner for Migration, Home Affairs and Citizenship Dimitris Avramopoulos said: “The threats against both our **physical and virtual worlds are becoming increasingly connected**. This is why increasing cyber security is one of the priorities of the European Union. But we can only do this effectively through stronger cooperation and joint actions, where our operational agencies, like Europol, can play a critical role with the expertise they bring to the table in support of our Member States.”

Commissioner for the Security Union Julian King said: “The cross-border nature of the cyber threat means that cooperation has never been more important. This improved collaboration between ENISA, EDA, EC3 and CERT-EU will help us to strengthen our cyber resilience, build effective deterrence and help deliver credible cyber defence and international cooperation.”

Commissioner for Digital Economy and Society, Mariya Gabriel said: “Trust and security are key components of the digital economy and society. The EU agencies should **lead by example**. Only by working closely together will we have a chance to mitigate the cybersecurity risks.”

Prof. Dr. Udo Helmbrecht, Executive Director of ENISA said: “ENISA welcomes the opportunity to work closely with our partner organisations. Cybersecurity is a shared responsibility, and it is only by cooperating closely with all relevant stakeholders that the EU has a chance to address cybersecurity challenges.”

Jorge Domecq, Chief Executive of the EDA: “EDA supports Member States in the development of their defence capabilities. As such, we also act as the military interface to EU policies. Today’s Memorandum of Understanding is an important step towards increased civil-military cooperation and synergies in the area of cyber security and cyber defence.”

Steven Wilson, Head of Europol’s European Cybercrime Centre (EC3): “This MoU illustrates **how a safe and open cyberspace can only be achieved through enhanced cooperation and commitment**. Through their participation, all parties involved demonstrate that they are willing to join forces and recognise that together we can provide the necessary response to cyber related threats. From EC3, we welcome the opportunity to enter a



new era of working together with our MoU partners and are delighted to share our expertise and experience.”

Ken Ducatel, Acting Head of CERT-EU, said: “The EU institutions, bodies and agencies rely on the specialised skills and tools in threat intelligence and incident response of CERT-EU. But, we don’t maintain these capacities by acting alone. That is why acting together with our peers and partners in the other signatories to this Memorandum is so important.”

The 2014 [Cyber Defence Policy Framework](#) called for the promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector.

ENISA, EDA, EC3 and CERT-EU began initial discussions in 2016 which eventually led to this milestone signature. The principles behind this Memorandum of Understanding are fully in line with the implementation of the Joint Communication on Cyber issued by the High Representative and the European Commission in September 2017.

*Number 6*

## A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future

Transmitted by The Secretary of Commerce and The Secretary of Homeland Security



### Executive Summary

This report responds to the May 11, 2017, Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

That order directs the Secretary of Commerce and the Secretary of Homeland Security to:

- 1) Assess the **scope and sufficiency** of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and
- 2) Provide a **report** to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

Other departments and agencies, industry, academia, and others in the private and public sectors contributed helpful information and views. Previous studies were reviewed to provide additional context.

#### Basic characteristics of the cybersecurity workforce<sup>1</sup> include:

- The majority of U.S. critical infrastructure is owned and operated by private companies, making its cybersecurity workforce vital.
- The federal government **depends heavily** on its cybersecurity workforce, supplemented by contractors.

- There are an estimated 299,000 active openings for cybersecurity-related jobs in the United States as of August 2017. Globally, projections suggest a cybersecurity workforce shortage of 1.8 million by 2022.
- Positions needing to be filled range from entry-level jobs attainable with minimal credentials to roles where successful performance is most knowledge-dependent and require advanced academic degrees, multiple certifications, and lengthy on-the-job technical, managerial, and business experience.
- In many instances, employers need workers with specialized knowledge or skills for specific sectors along with cybersecurity competencies.
- Competition for qualified cybersecurity workers is intense across all sectors.
- In comparison to the national workforce, minorities and women are underrepresented among those working in cybersecurity.
- Veterans represent an [available and underutilized](#) workforce supply.
- Pay for cybersecurity positions tends to be above the average levels for other positions in many parts of the economy, but in some areas—including the federal government—cybersecurity pay is below the level needed to attract the necessary talent.

To read more:

[https://www.nist.gov/sites/default/files/documents/2018/05/10/eo\\_wf\\_report\\_to\\_potus.pdf](https://www.nist.gov/sites/default/files/documents/2018/05/10/eo_wf_report_to_potus.pdf)

*Number 7*

## Active Social Engineering Defense (ASED)

Wade Shen



Over the past 40 years, our world has become increasingly connected. These connections have enabled major advances in national security from pervasive real-time intelligence and communications to optimal logistics.

With this connectivity has come the threat of cyber attacks on both military systems and critical infrastructure.

While we focus the vast majority of our security efforts on protecting computers and networks, **more than 80% of cyber attacks and over 70% of those from nation states are initiated by exploiting humans rather than computer or network security flaws.** To build secure cyber systems, it is necessary to protect not only the computers and networks that make up these systems but their human users as well.

We call attacks on humans “social engineering” because they manipulate or “engineer” users into performing desired actions or divulging sensitive information.

The most general social engineering attacks simply attempt to get unsuspecting internet users to click on malicious links. More focused attacks attempt to **elicit sensitive information**, such as passwords or private information from organizations or steal things of value from particular individuals by earning unwarranted trust.

These attacks always have **an “ask,”** a desired behavior that the attacker wants to induce from the victim. To do this, they need trust from the victim, which is typically earned through interaction or co-opted via a spoofed or stolen identity. Depending on the level of sophistication, these attacks will go after individuals, organizations, or wide swathes of the **population.**

Social engineering attacks work because it is **difficult** for users to **verify** each and every communication they receive. Moreover, verification requires a level of technical expertise that most users lack. To compound

the problem, the number of users that have access to privileged information is often large, creating a commensurately large attack surface.

The **Active Social Engineering Defense (ASED)** program aims to develop the core technology to enable the capability to automatically elicit information from a malicious adversary in order to identify, disrupt, and investigate social engineering attacks. If successful, the ASED technology will do this by mediating communications between users and potential attackers, actively detecting attacks and coordinating investigations to discover the identity of the attacker.

Additional information is available at:

<https://www.fbo.gov/index?s=opportunity&mode=form&id=c49a3e60af206263c01a144487867f55&tab=core&cvview=0>

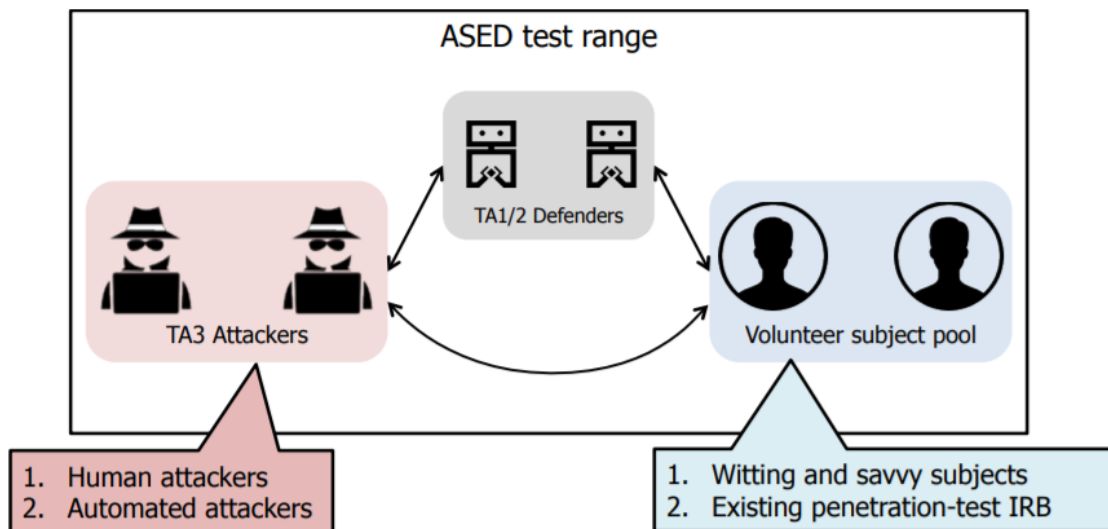


Figure 1: ASED Technical Areas and Evaluation Strategy

*Number 8*

## Are you Cyber-Savvy?

U.S. SECURITIES AND  
EXCHANGE COMMISSIONAre You  
Cyber-Savvy?

Take the quiz!

## Cybersecurity Quiz

## Question 1 of 5

You get an email from your broker telling you your information has been compromised and you need to click on a link in the email to update your login information. What do you do?

- A. Click on the link, fast, before someone logs in and takes all of your money.
- B. Call the number provided in the email to see if the email is legitimate before you click the link.
- C. Do not click on the link. Look up the contact information of your broker and contact them to see if your information was compromised.
- D. Ignore it. You get too many annoying emails.
- E. Forward to everyone you know and ask them if they think it's suspicious.

You may visit:

<https://www.sec.gov/spotlight/cybersecurity>

*Number 9*

European Commission - Statement

**Cybersecurity: Joint Statement by Vice-President Ansip and Commissioner Gabriel on political agreement from the Council**



The European Commission welcomes the *political agreement* reached by the Telecommunications Council on a general approach on the Cybersecurity Act, which was presented by President Jean-Claude Juncker in his annual State of the Union Address in 2017.

Vice-President Andrus Ansip, responsible for the Digital Single Market, and Commissioner Mariya Gabriel, in charge of Digital Economy and Society, issued the following statement:

"We are pleased that the Council adopted today a general approach on the Cybersecurity Act proposals.

Today's agreement opens the door to *transform and strengthen* the mandate of European Union Agency for Network and Information and Security (ENISA) into the EU's Cybersecurity Agency which will support Member States with tackling cybersecurity threats and attacks.

Additionally, the proposal aims to establish an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

Strengthening Europe's cybersecurity is the only way to assure a strong and viable Digital Single Market for the benefit of all.

It is vital for Member States to *work together* in building a more cyber secure European Union and avoid the complication of different national laws.

We would also like to congratulate and thank the Bulgarian Presidency for their hard work to find a consensus on this important file, only nine months after we presented our proposal in September 2017. Their work paves the way for the Austrian Presidency to soon reach a final

compromise with the European Parliament and adopt the package before the end of 2018."

## Background

In September 2017, the Commission proposed a wide-ranging set of measures to deal with cyber-attacks and to build strong cybersecurity in the EU.

This included the Cybersecurity package, a proposal for strengthening the EU Agency for Cybersecurity as well as a new European certification framework, ensuring that products and services in the digital world are cybersecure.



*Number 10***Drone Forensics Gets a Boost With New Data on NIST Website**

*How do you extract forensic data from an aerial drone? Very carefully.*



Aerial drones might someday **deliver** online purchases to your home. But in some prisons, drone delivery is already a thing.

Drones have been spotted flying **drugs, cell phones, and other contraband** over prison walls, and in several cases, drug traffickers have used drones to ferry narcotics across the border.

If those drones are **captured**, investigators will try to extract data from them that might point to a suspect. But there are many types of drones, each with its own quirks, and that can make data extraction tricky.

It would help if investigators could instantly conjure another drone of the same type to practice on first, and while that may not be possible, they can now do the next best thing: download a “forensic image” of that type of drone.

A forensic image is a complete data extraction from a digital device, and NIST maintains a repository of images made from personal computers, mobile phones, tablets, hard drives and other storage media.

The images in NIST’s **Computer Forensic Reference Datasets, or CFReDS**, contain simulated digital evidence and are available to download for free. Recently, NIST opened a new section of CFReDS dedicated to drones, where forensic experts can find images of 14 popular makes and models, a number that is expected to grow to 30 by December 2018.

“The drone images will allow investigators to do a dry run before working on high-profile cases,” said Barbara Guttman, manager of digital forensic research at NIST. “You don’t want to practice on evidence.”

The drone images were created by VTO Labs (<https://www.vtolabs.com>), a Colorado-based digital forensics and cybersecurity firm. NIST added the images to CFReDS because that website is well-known within the digital forensics community.

“Listing the drone images there is the fastest way to get them out to experts in the field,” Guttman said.

Work on the drone images began in May of last year, when VTO Labs received a contract from the Department of Homeland Security’s (DHS) Science and Technology Directorate.

“When we proposed this project, there was little existing research in this space,” said Steve Watson, chief technology officer at VTO.

The drone research was needed not only to combat drug smuggling, but also to allow officials to **respond more quickly** should a drone ever be used as a weapon inside the United States.

For each make and model of drone he studied for this DHS-funded project, Watson purchased three and flew them until they accumulated a baseline of data. He then **extracted data from one** while leaving it intact.

He **disassembled a second** and extracted data from its circuit board and onboard cameras.

**With the third**, he removed all the chips and extracted data from them directly.

He also disassembled and extracted data from the pilot controls and other remotely connected devices.

“The forensic images contain all the 1s and 0s we recovered from each model,” Watson said.

The images were created using industry standard data formats so that investigators can connect to them using forensic software tools and inspect their contents.

The images for each model also come with step-by-step, photo-illustrated teardown instructions.

Watson was **able to retrieve** serial numbers, flight paths, launch and landing locations, photos and videos. On one model, he found a database that stores a user’s credit card information.

Investigators can use the images to practice recovering data, including deleted files. Universities and forensic labs can use them for training, proficiency testing and research.

And application developers can use the images to test their software. “If you’re writing tools for drone forensics, you need a lot of drones to test them on,” Guttman said.

A description of the drone images and instructions for accessing them are available on the new drones section of the CFReDS website.

*Number 11*

## Cybersecurity Enforcement Actions



U.S. SECURITIES AND  
EXCHANGE COMMISSION

Secure | <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>

2017 Broker-Dealer  
Compliance

Advisory Committee on  
Small and Emerging  
Companies

Affinity Fraud

Crowdfunding

Cybersecurity

Disclosure Effectiveness

Enforcement  
Cooperation Initiative

Equity Market Structure  
Roundtables

Feds Feed Families

Financial Reporting and  
Audit Group

Fixed Income Market

## Cybersecurity Enforcement Actions



### Digital Currency/Initial Coin Offerings

Action Name	Description	Date Filed
Centra Tech., Inc.	The Commission filed an amended complaint to the April 2, 2018, district court action against a third member of a purported financial services start-up, charging him with orchestrating a fraudulent ICO.	4/20/2018
SEC v. Longfin Corp., et al.	The Commission filed a district court action and obtained an emergency asset freeze against Longfin Corp., its CEO and three of its affiliates, alleging that the company and its CEO engaged in an unregistered distribution of securities and the three affiliates sold unregistered securities after the company announced a related-party acquisition of a purported cryptocurrency website, causing a dramatic increase its stock price.	4/6/2018

You may visit:

<https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>

## 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.*

