*April 2020, cyber risk and compliance in Switzerland*

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

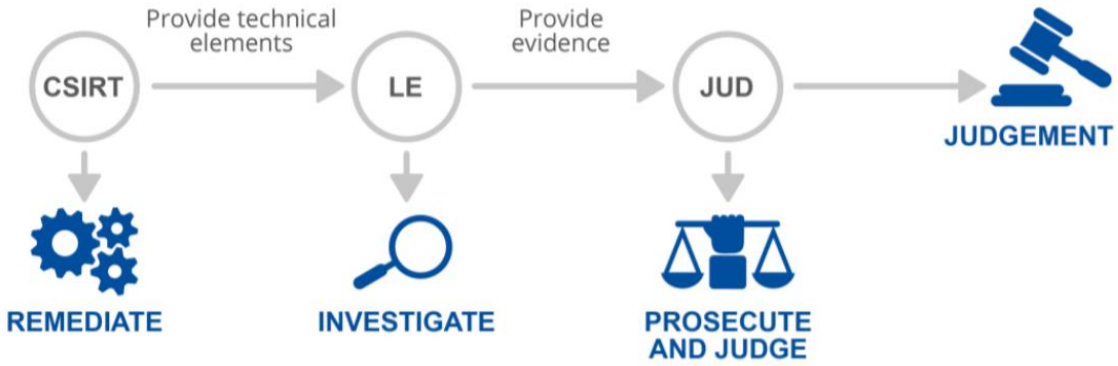
Dear readers,

Computer Security Incident Response Teams (CSIRTs), Law Enforcement (LE) and the judiciary (prosecutors and judges) have *different* approaches or mindsets, as they often have different educational and scientific backgrounds.

In particular, CSIRTs have a 'technical mentality' while the judiciary has a 'legal mentality'. The LE have partly a 'legal mentality' and partly a 'technical mentality' that is entrenched in how society operates in the area of crime.

The different mentalities make communication among these three entities not always easy. This can also lead to limitations of cooperation or at least a slowdown in cooperation.

This is an interesting approach, explained in the paper "*Roadmap on the cooperation between CSIRTS and LE"* from the European Union Agency for Cybersecurity (ENISA).




According to the paper, each community has its own discreet set of responsibilities, duties, expertise, powers and technical and procedural tools.

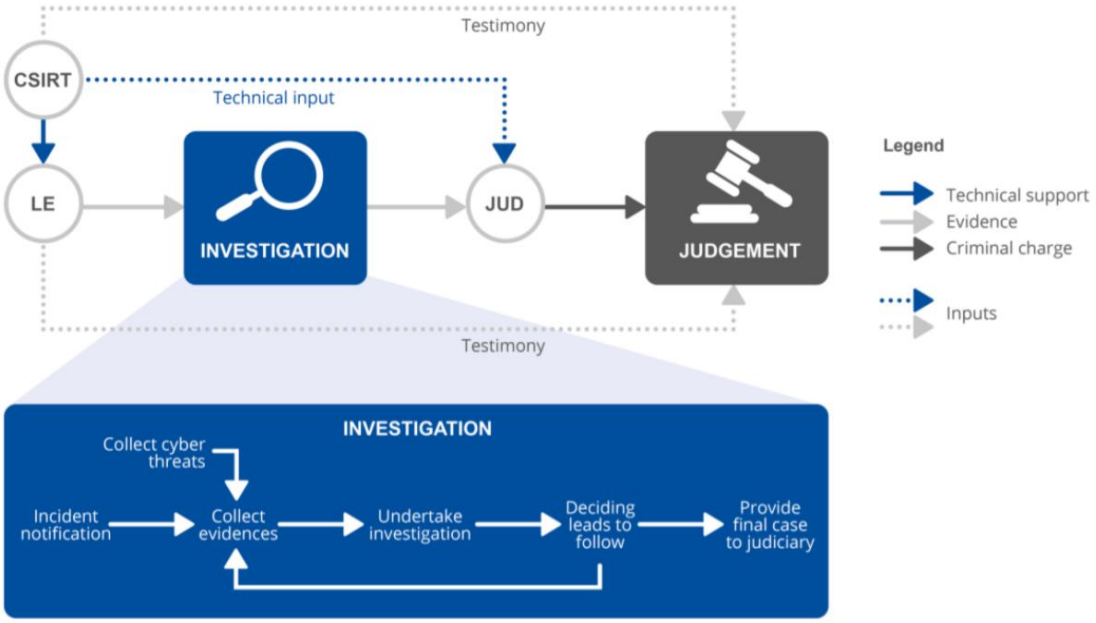
Sometimes, however, duties and responsibilities overlap, and this might lead to undesirable interference to each other's activities. Therefore, it is important for the communities to understand each other's duties.

*CSIRTs* are responsible to ensure the confidentiality, availability and integrity of systems within their constituency. *LE* aims to trace offenders and gather evidence that describes the course of the offence and show offenders' guilt.

On the basis of the results of the work of the law enforcement authorities, the *judiciary* assesses the factual and legal conclusions resulting from the evidence obtained and decides on guilt and punishment.

The CSIRTs' role is to prevent incidents from happening by implementing appropriate security measures or suggesting such measures to their constituency.

And in the event of an incident, their aim is to detect and analyse the incident and apply appropriate measures, remedy the damage and subsequently secure the exploited vulnerabilities, or other existing threats.




As first responders, however, they could be also responsible for advising their constituency to report the incident to LE (or in some cases they might have themselves a duty to report), expected to share the information with other sectors or targeted industries, and required to provide necessary assistance to other communities and collect evidence.

LE is dedicated to investigate cybercrimes and investigate possible culprits. They have legal power to mandate entities to cooperate in the investigation and disclose information or to contribute to the investigation in different ways: seizes, searches, and interceptions.

LE responsibility is to collect evidence in a lawful way, even if it may challenge remediation or business continuity. Of course, they seek to avoid further consequences to the victims, but sometimes, evidence collection can postpone remediation or return to normal.

Read more at number 6 below.

---

*Extortion* occurs when a person attempts to obtain money or property by threatening to commit violence, accuse the victim of a crime, or reveal private or damaging information about the victim. It is a felony in almost all countries.

*Blackmail* is a form of *extortion* in which a person attempts to threaten victims that embarrassing and damaging information or details about their private lives will be exposed to family, friends, or the public.

*Sexual extortion (sextortion)* often starts with efforts to strike up close friendships with future victims online. Once the trust is solidified, criminals and state-sponsored hackers from several countries encourage their victims to send inappropriate pictures or videos, or they hack systems and find these files. They then use these files to blackmail their victims.

Children are increasingly becoming targets too. According to the FBI, due to *school closings* as a result of COVID-19, children will potentially have an increased online presence and/or be in a position that puts them at an inadvertent risk.

Due to this newly developing environment, the FBI is seeking to warn parents, educators, caregivers, and children about the dangers of online sexual exploitation and signs of child abuse.

According to the FBI, *sextortion* begins when a predator reaches out to a young person over a game, app, or social media account. Through deception, manipulation, money and gifts, or threats, the predator convinces the young person to produce an explicit video or image.

When the young person starts to resist requests to make more images, the criminal will use threats of harm or exposure of the early images to pressure the child to continue producing content.

It is good to discuss with our children and their friends (with the permission of their parents) the following questions and answers, compiled by the FBI.

*What is sextortion?*

Sextortion describes a crime that happens online when an adult convinces a person who is younger than 18 to share sexual pictures or perform sexual acts on a webcam.

*How does it start?*

Sextortion can start on any site where people meet and communicate. Someone may contact you while you are playing a game online or reach out over a dating app or one of your social media accounts.

In some cases, the first contact from the criminal will be a threat. The person may claim they already have a picture or video of you that they will share if you don't send more pictures.

More often, however, this crime starts when young people believe they are communicating with someone their own age who is interested in a relationship or someone who is offering something of value.

The adult can use threats, gifts, money, flattery, lies, or other methods to get a young person to produce these images. After the criminal has one or more videos or pictures, they use the threat of sharing or publishing that content to get the victim to produce more images. The adult has committed a crime as soon as they ask a young person for a single graphic image.

*Why do young people agree to do this?*

The people who commit this crime have studied how to reach and target children and teens.

One person the FBI put in prison for this crime was a man in his 40s who worked as a youth minister so he could learn how teens talked to each other. Then, he created social media profiles where he pretended to be a teenage girl. This "girl" would start talking to boys online and encourage them to make videos.

Another person offered money and new smartphones to his victims.

In one case, the criminal threatened a girl—saying he would hurt her and bomb her school—if she didn't send pictures.

Other cases start with the offer of currency or credits in a video game in exchange for a quick picture.

*How do you know who can be trusted online?*

That's what is so hard about online connections. The FBI has found that those who commit this crime may have dozens of different online accounts and profiles and are communicating with many young people at the same time—trying to find victims.

Be extremely cautious when you are speaking with someone online who you have not met in real life. It's easy to think: I'm on my phone, in my own house, what could possibly happen? But you can very quickly give a criminal the information and material he needs to do you harm.

*But how can this harm me?*

It's true that these criminals don't usually meet up with kids in real life, but the victims of this crime still experience negative effects. The criminals can become vicious and non-stop with their demands, harassment, and threats. Victims report feeling scared, alone, embarrassed, anxious, and desperate. Many feel like there's no way out of the situation.

Read more at number 10 below.

---

Hippocrates believed that *it is more important to know what sort of person has a disease, than to know what sort of disease a person has*.

We still need international standards and cooperation.

The Financial Stability Board (FSB) has been established to coordinate at the international level the work of national financial authorities and international standard setting bodies (SSBs), in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies.

According to the FSB, the COVID-19 crisis calls for a *reprioritisation* of FSB initiatives to maximise the value of FSB work during the current crisis and to use members' resources effectively.

The reprioritisation of FSB projects takes into account the following criteria:

- whether the work is relevant to current crisis management;

- whether the evolution of the crisis may substantially change the

findings (and the analysis could therefore benefit from a delay);

- whether there are other important reasons to maintain the existing timing and/or scope of the project; and

- whether postponing or scaling back the work could relieve COVID-related additional resource pressures on FSB members and their staff and on financial institutions and other stakeholders.

The main elements of the reprioritisation are as follows:

Assessment of vulnerabilities. The FSB will focus on monitoring current risks to global financial stability, and in particular the impact of COVID-19 on the resilience of the financial system.

Non-bank financial intermediation (NBFI). Prioritisation will support timely discussion of policy issues arising from vulnerabilities in NBFI that are surfacing in the COVID-19 crisis, and decisions on how to organise such work in the FSB going forward.

Financial innovation. Prioritisation will ensure that key deliverables to the Saudi G20 Presidency will be provided, and that the FSB completes initiatives on topics that are likely to remain of policy relevance in the near term.

Cross-border payments. The three-stage work to develop a roadmap on cross-border payments, in coordination with the Committee on Payments and Market Infrastructures (CPMI), will continue as scheduled, given the importance of efficient cross-border payments systems.

Resolution. Technical work on central counterparty resolution and the implementation of the Total Loss-Absorbing Capacity standard remains a priority, given the importance as part of effective crisis management.

OTC derivatives. Finalising the oversight arrangements for Unique Product Identifier (UPI) and Unique Transactions Identifier will continue as the UPI service provider awaits clarity on the oversight arrangements.

Benchmark transition. The transition from LIBOR remains a priority as firms cannot rely on LIBOR being produced after end 2021. Benchmark transition will help to strengthen the global financial system.

Other work on supervisory and regulatory policies. FSB will prioritise work to focus on policy responses to the COVID-19 crisis, including forward-looking issues concerning crisis management.

Implementation monitoring. Implementation monitoring will track measures taken by SSBs in response to the COVID crisis. Other work will be reduced to the completion of near-final projects and the production of a streamlined annual report to the G20.

According to the *statement on COVID-19* from the G20 leaders, the unprecedented COVID-19 pandemic is a powerful reminder of our interconnectedness and vulnerabilities.

The virus respects no borders. Combatting this pandemic calls for a transparent, robust, coordinated, large-scale and science-based global response in the spirit of solidarity.

The G20 has a pivotal role in ensuring global coordination. We read at the Statement on COVID-19:

“We are strongly committed to presenting a united front against this common threat. We are deeply saddened by the tragic loss of life and the suffering faced by people around the world.

Tackling the pandemic and its intertwined health, social and economic impacts is our absolute priority. We express our gratitude and support to all frontline health workers as we continue to fight the pandemic.

The G20 is committed to do whatever it takes to overcome the pandemic, along with the World Health Organization (WHO), International Monetary Fund (IMF), World Bank Group (WBG), United Nations (UN), and other international organizations, working within their existing mandates.”

---

According to the Swiss Financial Market Supervisory Authority (FINMA), the impact of the COVID-19 pandemic on financial markets and the real economy remains significant and is associated with a great deal of uncertainty.

In this connection, FINMA refers to the measures taken by the Swiss government and the National Bank as well as FINMA Guidance 2/2020 published on 31 March 2020.

In a recent guidance FINMA communicates further exemptions for supervised institutions as well as certain clarifications pertaining to the banking sector.

The exemptions concern the insurance sector and anti-money laundering regulations.

These selective exemptions are intended to help the supervised institutions overcome the crisis.

Since the start of the COVID-19 pandemic, there has been a sharp increase in volatility, particularly for certain yield curves.

As the Swiss Solvency Test (SST) is calculated on a specific date, this volatility can result in large fluctuations in the SST.

A smoothing of the yield curves over a period of 10 days reduces these fluctuations significantly, without masking important market signals.

Upon request, FINMA is therefore willing to accept a 10-day average of the yield curves as the calculation basis for the SST. Such a choice cannot be reversed within a calendar year and must be disclosed accordingly.

To read the paper:
https://www.finma.ch/en/documentation/dossier/dossier-covid-19/

---

The Office of the Attorney General of Switzerland (OAG) has filed an indictment against an Iraqi citizen in the Federal Criminal Court. He is accused of being a member of and carrying out various activities for the Islamic State terrorist organisation (IS) while operating from Switzerland. The suspect held a position of authority in relation to other IS members, some also in high-ranking positions.

The OAG alleges that the suspect violated the Federal Act on the Proscription of the Groups «Al-Qaeda», «Islamic State» and Associated Organisations (SR 122). He is also accused of participation in IS as a criminal organisation (Art. 260ter no 1 Swiss Criminal Code (SCC)), commercial fraud (Art. 146 para. 1 and 2 SCC) and multiple counts of producing and storing representations of acts of violence (Art. 135 para. 1 SCC).

The OAG opened criminal proceedings in the case in November 2016. The suspect was arrested in May 2017 and has since been in pre-trial detention. On filing the indictment, the OAG requested the competent compulsory measures court to order the suspect to be held in preventive detention.

*Membership of the proscribed terrorist organisation IS*

The OAG alleges that the suspect, from around 2014, but at the latest from mid-2016 and until his arrest in May 2017, was a member of terrorist organisation IS, operating from Switzerland. Investigations in this

connection uncovered an extensive transnational network involving the suspect and over 20 other IS members in Switzerland, Syria, Iraq, Turkey, Lebanon, Finland and in another location as yet unidentified. The suspect held a position of authority in relation to other IS members, some also high-ranking, and functioned as a recruiter, trafficker, cash-provider and as the recipient of instructions from leading IS members.

The suspect is alleged to have carried out numerous activities for IS. He is accused of attempting in April 2017 to incite an IS member living in Lebanon to carry out a suicide attack in Lebanon on behalf of IS. The attack was prevented in time.

The suspect is also alleged to have agreed to carry out orders from a high-ranking IS member to prepare for attacks in Switzerland. In addition, according to the indictment, he provided IS with financial support, recruited several persons for the IS and assisted them in travelling to join IS and instructed an IS member living in Syria to set up IS sleeper cells.

The investigations did not reveal any indication that an actual attack was imminent in Switzerland. The persons named in the indictment as having been recruited for or sent to IS by the suspect did not include anyone resident in Switzerland or any Swiss citizens.

*Commercial fraud*

According to the indictment, in the period from February 2017 until his arrest in May 2017, the suspect provided false information with regard to his financial circumstances to the social services department in his commune in the canton of Thurgau on more than a dozen occasions when requested and thus obtained social assistance benefits to which he was not entitled.

*Multiple counts of producing and storing representations of acts of violence*

The OAG also alleges that in the period from 2016 until his arrest in May 2017, the suspect downloaded numerous representations of acts of violence from the internet to his data carriers and stored them there for his own consumption and in order to pass them on to others. Most cases involved propaganda material showing various forms of brutal executions.

*Successful cooperation at national and international level*

The complex investigations in this case were carried out under the OAG's leadership by a joint investigation team involving fedpol and the Zurich Cantonal Police. In addition, the OAG worked through international

mutual assistance channels with several other countries. The OAG would like to thank fedpol, the Zurich Cantonal Police and its other national and international partners for their excellent cooperation in this case, which has now made it possible to bring the matter to court.

As is customary, the OAG will make its proposals for the disposal of the case at the main hearing before the Federal Criminal Court. With the filing of the indictment, the Federal Criminal Court becomes responsible for procedural matters and media communications. This also applies with regard to the suspect's detention. The presumption of innocence applies until a legally binding conviction has been secured.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

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

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

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

*Number 1 (Page 14)*

## Marriott International Notifies Guests of Property System Incident (March 31, 2020)


*Number 2 (Page 16)*

## A Framework of Partnership

Professor Jim Q. Chen, Ph.D.

THE CYBER DEFENSE REVIEW

*Number 3 (Page 19)*

## Launch of our cybersecurity platform: get involved and educate yourself


*Number 4 (Page 22)*

## FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC


*Number 5 (Page 24)*

## NIST Releases Online Economic Decision Tool to Help Communities Plan for Disaster

*Number 6 (Page 27)*

## Supporting the fight against cybercrime

The map to the road less traveled: CSIRTs & Law Enforcement cooperation

*Number 7 (Page 30)*

## SEC Coronavirus (COVID-19) Response

*Number 8 (Page 32)*

## See how your community is moving around differently due to COVID-19

*Number 9 (Page 33)*

## Episode 24: Preventing Pandemics

Voices from DARPA podcast restarts with episode on programs aiming to take pandemics off the table for good

*Number 10 (Page 35)*

## School Closings Due to COVID-19 Present Potential for Increased Risk of Child Exploitation

*Number 11 (Page 38)*

## FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

*Number 12 (Page 40)*

## PIPES Researchers Demonstrate Optical Interconnects to Improve Performance of Digital Microelectronics

Researchers replace traditional electronic I/O with optical signaling interfaces to achieve major improvements in link reach and efficiency

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

*Number 13 (Page 43)*

## Proliferated Commercial Satellite Constellations, Implications for National Security

By Matthew A. Hallex and Travis S. Cottom

Joint Force Quarterly
Issue 97, 2nd Quarter 2020

*Number 14 (Page 45)*

## Advisory: COVID-19 exploited by malicious cyber actors

National Cyber Security Centre
a part of GCHQ

CISA
CYBER+INFRASTRUCTURE

*Number 15 (Page 49)*

U.S. Attorney Scott Brady and Pennsylvania Attorney General Josh Shapiro

## Zoom-Bombing and Hacking Teleconferences During Coronavirus Pandemic

*Number 1*

## Marriott International Notifies Guests of Property System Incident (March 31, 2020)

Marriott International announced that it is notifying some of its guests today of an incident involving a property system.

The notice explains what occurred, the information involved, the measures taken by Marriott to investigate and address the issue, how Marriott is assisting guests, and steps guests can consider taking.

Hotels operated and franchised under Marriott's brands use an application to help provide services to guests at hotels.

At the end of February 2020, the company identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property.

The company believes that this activity started in mid-January 2020.

Upon discovery, the company confirmed that the login credentials were disabled, immediately began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests.

Marriott also notified relevant authorities and is supporting their investigations.

Although Marriott's investigation is ongoing, the company currently has no reason to believe that the information involved included Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers.

At this point, the company believes that the following information may have been involved for up to approximately 5.2 million guests, although not all of this information was present for every guest involved:

- contact details (e.g., name, mailing address, email address, and phone number)

- loyalty account information (e.g., account number and points balance, but not passwords)

- additional personal details (e.g., company, gender, and birthday day and month)

- partnerships and affiliations (e.g., linked airline loyalty programs and numbers)

- preferences (e.g., stay/room preferences and language preference)

Today, Marriott is sending emails to guests involved. Marriott has also set up a dedicated website (www.mysupport.marriott.com) and call center resources with additional information for guests. The call center resources can be reached by calling the numbers listed on the dedicated website.

The email sent to guests and the website also contain a list of steps guests involved can consider taking and information about enrolling in a personal information monitoring service that Marriott is providing.

Marriott carries insurance, including cyber insurance, commensurate with its size and the nature of its operations, and the company is working with its insurers to assess coverage. The company does not currently believe that its total costs related to this incident will be significant.

*Number 2*

## A Framework of Partnership

Professor Jim Q. Chen, Ph.D.

THE CYBER DEFENSE REVIEW

There exist many partnership methods. Here, in this research, three major ones are focused on. These are: cooperation, collaboration, and integration.

These three methods sit on varied points on a partnership spectrum. Within this spectrum, cooperation requires the least effort from both sides, while integration requires the most effort from both sides.

The high-level representation of the spectrum is displayed in Figure 1 below:

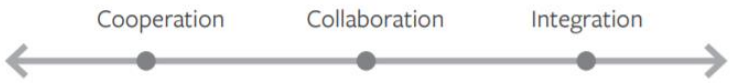



Figure 1. Spectrum of different partnership methods

In a cooperative relationship, a horizontal management structure is maintained. Both sides are independent from each other, even though they have a common task to accomplish.

No roles or responsibilities are clearly assigned to relevant team members. No formal procedure is followed.

There is no special budget for a task in most cases. Both sides may put resources together whenever needed. The relevant people from both sides work together in an informal environment whenever needed.

This relationship is symbolically represented below:


Figure 2. Cooperation

A voluntary, cyber-related, information-reporting mechanism is an example of cooperation.

A government agency may acquire a critical piece of information from a private-sector company, which, in return, may receive useful pieces of advice for cyber defense from a government agency.

Both sides may benefit from this mechanism, but neither side is in absolute control. Besides, neither side needs to have a big investment for the use of this mechanism.

In a collaborative relationship, a horizontal management structure is maintained. Both sides remain independent from the other while they take on a common task.

They select people from both sides to form a special group to work together on a particular task. Both sides are in charge. Roles and responsibilities may or may not be assigned.

People from both sides form a group and work together in an informal environment. A special budget may or may not be allocated. Both sides may put resources together whenever needed.

This relationship is represented below:


Figure 3. Collaboration

An active threat intelligence-sharing group is an example of collaboration. It involves stakeholders and participants, such as national security agencies, law enforcement agencies, cybersecurity industry companies, non-cybersecurity commercial companies, and other relevant actors.

Well-established, cyber-focused, public-private collaboration in current practice includes, but is not limited to, Information Sharing and Analysis Centers (ISACs), automated indicator sharing though Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), and the Cyber Information Sharing and Collaboration Program (CISCP).

Personnel and resource investment is required to support these efforts, which are beneficial for all stakeholders and participants.

The true public-private collaboration in Healey's framework falls into this category, as joint governance is guaranteed and personnel exchange is supported.

In an integrative relationship, one side absorbs the other side into its organization.

Now, one side is in total control.

A horizontal management structure changes into a hierarchical management structure. Those who work on a task form a special unit of the organization. They work in a formal environment.

A formal procedure is followed. A special budget is allocated. Resources are provided. Bureaucracy may be developed in some cases.

This relationship is represented below:


Figure 4. Integration

To read more (page 17/204):
https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%20FULL_WEB_1.pdf

*Number 3*

## Launch of our cybersecurity platform: get involved and educate yourself

## Cybersecurity Skills Development in the EU

The new whitepaper on "Cybersecurity Skills Development in the EU" focuses on the state of the cybersecurity education system and the difficulty in attracting more students to cybersecurity studies.

It looks at how we can increase the number of graduates with relevant cybersecurity knowledge and skills.

This report provides considerations and recommendations for policy actions at national and at European level in order to address the shortage in cybersecurity skills.

In addition, further areas of research are being considered to identify the nature and extent of the EU cybersecurity skills shortage.

The paper addresses:

- The policy challenge of the cybersecurity skills shortage;
- The causes of the shortage; explaining why many stakeholders agree on the need to set standards for cybersecurity certification degrees;
- The processes and criteria established by 4 countries in order to certify cybersecurity degrees and the implications of establishing certification for cybersecurity degrees;
- The creation of the ENISA's Cybersecurity Higher Education Database;
- Recommendations for increasing the number of graduates with the right cybersecurity knowledge and skills.

## The Cybersecurity Higher Education Database

All the EU higher education institutions with cybersecurity degrees are invited to add their degrees to the Cybersecurity Higher Education Database.

This will allow young talents to make informed decisions in light of the different possibilities offered by higher education in cybersecurity. It will also help universities to attract highly motivated students interested in keeping Europe cyber secure.

By creating a single and easy-to-use online platform where citizens can find relevant information on cybersecurity degrees, the Agency seeks to fill potential information gaps.

Such gaps are obvious, for example, when students might be interested in a cybersecurity career but don't know where to find information on the best educational pathways available.

The database therefore intends to bridge the gap between cybersecurity supply and demand.

The EU Agency for Cybersecurity, Executive Director, Juhan Lepassaar, stated:

"Having enough professionals to secure information systems has become an absolute priority. The database and skills development white paper are two tools the Agency created to support cybersecurity awareness and education which are needed to build Europe's cyber capacities."

## Background of the EU Cybersecurity Education Policy

Cybersecurity education and skills have attracted policy interest since the publication by the European Commission of the first EU cybersecurity strategy in 2013.

The Commission invited Member States to increase their education and training efforts around network and information security (NIS) topics.

The intention was to create a 'NIS driving licence' as a voluntary certification programme to promote advanced skills and validate the competences of IT professionals.

In 2017, in the Joint Communication 'Resilience, deterrence and defence: Building strong cybersecurity for the EU' , the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy confirmed again that 'there is a strong education dimension to cybersecurity'.

They declared also that 'effective cybersecurity relies heavily on the skills of the people concerned'.

The Agency has been an active player in cybersecurity education, awareness and research.

Since 2012, seven publications were produced of high relevance to the topic. In addition, the agency has been running the European Cyber Security Challenge and the European Cyber Security Month, an awareness campaign taking place every October.

To read more: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

*Number 4*

## FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following:

Fake CDC Emails. Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize.

Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.

Phishing Emails. Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government.

While talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:

- Charitable contributions
- General financial relief
- Airline carrier refunds
- Fake cures and vaccines
- Fake testing kits

Counterfeit Treatments or Equipment. Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert

to counterfeit products such as sanitizing products and Personal Protective Equipment (PPE), including N95 respirator masks, goggles, full face shields, protective gowns, and gloves.

More information on unapproved or counterfeit PPE can be found at www.cdc.gov/niosh. You can also find information on the U.S. Food and Drug Administration website, www.fda.gov, and the Environmental Protection Agency website, www.epa.gov.

Report counterfeit products at www.ic3.gov and to the National Intellectual Property Rights Coordination Center at iprcenter.gov.

If you are looking for accurate and up-to-date information on COVID-19, the CDC has posted extensive guidance and information that is updated frequently. The best sources for authoritative information on COVID-19 are www.cdc.gov and www.coronavirus.gov. You may also consult your primary care physician for guidance.

The FBI is reminding you to always use good cyber hygiene and security measures. By remembering the following tips, you can protect yourself and help stop criminal activity:

- Do not open attachments or click links within emails from senders you don't recognize.

- Do not provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email or robocall.

- Always verify the web address of legitimate websites and manually type them into your browser.

- Check for misspellings or wrong domains within a link (for example, an address that should end in a ".gov" ends in .com" instead).

If you believe you are the victim of an Internet scam or cyber crime, or if you want to report suspicious activity, please visit the FBI's Internet Crime Complaint Center at www.ic3.gov

*Number 5*

## NIST Releases Online Economic Decision Tool to Help Communities Plan for Disaster

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

Preparing a community's buildings and infrastructure for a hurricane or earthquake can be an incredibly complicated and costly endeavor.

A new online tool from the National Institute of Standards and Technology (NIST) could streamline this process and help decision makers invest in cost-effective measures to improve their community's ability to mitigate, adapt to and recover from hazardous events.

With input from local and state government officials, NIST researchers developed the Economic Decision Guide Software (EDGe$) tool, a platform-independent web app, to provide a standard and easy-to-use method of evaluating and comparing different community projects to improve resilience.

For community planners weighing options — whether to build a levee or add green space to reduce flooding in a neighborhood, for example — EDGe$ could reveal key economic insights about which choice would be a better fit. The new tool could be beneficial for state, local and private sector planners.

### NIST Economic Decision Guide Software

The Economic Decision Guide Software (EDGe$) Tool brings to your fingertips a powerful technique for selecting cost-effective community resilience projects. This decision support software is designed to support those engaged in community-level resilience planning, including community planners and resilience officers, as well as economic development, budget, and public works officials. It provides a standard economic methodology for evaluating investment decisions required to improve the ability of communities to adapt to, withstand, and quickly recover from natural, technology, and human-caused disruptive events. The tool helps to identify and compare the relevant present and future resilience costs and benefits associated with new capital investment versus maintaining a community's status-quo. The benefits include cost savings and damage loss avoidance because enhancing resilience on a community scale creates value, including co-benefits, even if a hazard event does not strike.

You may visit: https://edges.nist.gov/

"We have tried to make EDGe$ as user-friendly and straightforward as possible for economists and non-economists alike," said Jennifer Helgeson, a NIST research economist and lead developer of the tool.

Because myriad factors affect how communities respond to disaster, decision-makers could spend an eternity mulling over which resilience measures would provide the greatest benefits relative to the costs. But EDGe$ users may have an easier time cutting through the noise.

The online tool requests user input about variables that are most crucial for determining the value of a resilience action, including often overlooked factors, such as benefits that accrue day to day even if disaster does not strike. It can also include the effects of projects on neighboring communities, Helgeson said.

Would improving the earthquake resistance of a bridge also ease traffic for a neighboring town? Could a green space in a flood-prone area double as a public park? EDGe$ supports these types of considerations, Helgeson said.

EDGe$ calculates several important figures that indicate the value of investments, such as benefit-to-cost ratios, internal rates of return and returns on investment (whether a hazardous event occurs or not). The metrics from each potential plan, including one where no action is taken, are then laid out side by side so they can be easily compared.

You may visit: https://edges.nist.gov/

https://www.nist.gov/news-events/news/2020/03/nist-releases-online-economic-decision-tool-help-communities-plan-disaster


3.
DETERMINE GOALS & OBJECTIVES
• Establish long-term community goals
• Establish performance goals
• Define community hazards
• Determine anticipated performance
• Summarize results
4.
PLAN DEVELOPMENT
• Evaluate gaps
• Identify solutions
• Develop implementation strategy
5.
PLAN PREPARATION, REVIEW, AND APPROVAL
• Document plan and strategy
• Obtain feedback and approval
• Finalize and approve plan
6.
PLAN IMPLEMENTATION AND MAINTENANCE
• Execute approved solutions
• Evaluate and update
• Modify strategy as needed
Community Resilience
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

*Number 6*

## Supporting the fight against cybercrime

The map to the road less traveled: CSIRTs & Law Enforcement cooperation

In an effort to further enhance the cooperation between the Computer Security Incident Response Teams (CSIRTs), especially national and governmental, and law enforcement agencies (LEAs), ENISA has carried out a survey and analysis of significant issues at hand that are likely to inhibit cooperation.

As ENISA usually takes a holistic view of the policy area of CSIRT and LEA cooperation, interactions with the judiciary have also been taken into consideration to the extent possible.

The result of this study is a Roadmap on the cooperation between CSIRTS and LE.

The fight against cybercrime requires the involvement of Law Enforcement Agencies (LEAs), which supported by CSIRTs are likely to be better positioned to investigate complex criminal structures.

This picture is incomplete though, unless interactions with the judiciary are equally taken into account due to the pre-eminent role it plays across the Member States in terms of directing criminal investigations.

When CSIRTs, LEAs and the judiciary cooperate, they face challenges that previously, have been categorized, by ENISA as being technical, legal, organizational and/or human behaviour as they associate with organisational culture.

Understanding these challenges is essential in an effort to tackle them, further enhance the cooperation and thus stand a better chance in the fight against cybercrime.

In 2018, ENISA confirmed that CSIRTs, LEAs and the judiciary have complementary roles and that incident handling varies across Member States. The data CSIRTs and LEAs have access to varies, and it affects information sharing between them when they seek to respond to cybercrime.

While CSIRTs interact frequently with LEAs rather than with public prosecutors, CSIRTs when collecting and analysing different types of

evidence, they are called upon rarely as witness in court, even though material they collect during the incident handling typically supports an investigation and prosecution of a crime.

The data supporting this roadmap was collected via desk research, interviews with subject-matter experts and an online survey. The data collected has demonstrated that CSIRTs, LEAs and the Judiciary come across a range of challenges that are likely to impact their ability to cooperate effectively.

The legal framework has been quoted as an impeding factor when seeking to exchange data. Discrepancies in the levels of technical or legal knowledge is another one, as it may make communication challenging.

The chain of custody in evidence collection might also be an issue when using methods that might make evidence likely inadmissible in Court. Incident notifications and cybercrime reporting differ across Member States as different legal obligations might have been laid out by national law.

*Recommendations:*

- Core areas of further analysis and ENISA recommendations in an effort to improve cooperation between CSIRTs, LEAs and their interaction with the judiciary include:

- Promoting the use of 'Segregation of duties' matrix for avoiding conflicting roles and responsibilities of CSIRTs, LE and the judiciary throughout the cybercrime investigation lifecycle.

- Developing a competency framework for cybersecurity workforce and education and training policies.

- Promoting knowledge of digital forensics rules.

- Promoting interoperability of cooperation tools deployed and conceived considering future technologies.

- Assessing the suitability of cybersecurity certification for common tools and procedures.

- Simplifying arrangements by creating internal cooperation procedures to streamline exchanges.

The target audience of this roadmap includes mainly, but it is not limited to CSIRTs, LEAs, prosecutors, and judges. This roadmap builds on past

ENISA work and it contributes to the implementation of the ENISA programming document 2019-2021, Output O.4.2.2.

To read more:
https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

*Number 7*

## SEC Coronavirus (COVID-19) Response

The U.S. Securities and Exchange Commission's efforts are centered, first and foremost, on the health and safety of our employees and all Americans.

[+] Agency Operations: Transition to Telework and Continuity of Operations

[+] Market Monitoring and Engagement with Market Participants

[+] Guidance and Targeted Regulatory Assistance and Relief

[+] Enforcement, Examinations and Investor Education

[+] Effect on Comment Periods for Certain Pending Actions

We also are focused on, among other things:

- maintaining the continuity of Commission operations;
- monitoring market functions and system risks;
- providing prompt, targeted regulatory relief and guidance to issuers, investment advisers and other registrants impacted by COVID-19 to facilitate continuing operations, including in connection with the execution of their business continuity plans (BCPs); and
- maintaining our enforcement and investor protection efforts, particularly with regard to the protection of our critical market systems and our most vulnerable investors.

We continue to work in close coordination with other financial regulators and governmental authorities in the United States and globally.

Through this period of collective, national challenge, we have remained fully operational and committed to our tripartite mission to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.

While the agency is engaging on numerous COVID-19 initiatives as noted above, we also continue our regular agency operations.

For example, we have continued to advance rulemaking initiatives, conduct risk-based inspections, bring enforcement actions, and review and comment on issuer and fund filings.

Our staff has been intently focused on continuing to display the level of professionalism and dedication on which our investors and markets have come to rely.

We recognize the importance of our mission to America's investors and our markets and believe it is a privilege to serve.

To read more: https://www.sec.gov/sec-coronavirus-covid-19-response

*Number 8*

## See how your community is moving around differently due to COVID-19

As global communities respond to COVID-19, we've heard from public health officials that the same type of aggregated, anonymized insights we use in products such as Google Maps could be helpful as they make critical decisions to combat COVID-19.

These Community Mobility Reports aim to provide insights into what has changed in response to policies aimed at combating COVID-19.

The reports chart movement trends over time by geography, across different categories of places such as retail and recreation, groceries and pharmacies, parks, transit stations, workplaces, and residential.


You may visit:
https://www.google.com/covid19/mobility/

*Number 9*

## Episode 24: Preventing Pandemics

Voices from DARPA podcast restarts with episode on programs aiming to take pandemics off the table for good

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

We find ourselves in pandemic times. The global population is under siege by an infectious virus new to humankind. It's called Severe Acute Respiratory Syndrome Coronavirus 2, or SARS-CoV-2. It's the causative agent of the pandemic disease designated COVID-19.

This viral adversary knows no politics. It recognizes no national boundaries. It is unconcerned with anyone's identity. All 7.8 billion of us are the same to the virus: we are all hosts suitable to commandeer to make copies of itself.

DARPA has long recognized how devastating pandemic diseases like COVID-19 could be and the Agency embraced the attitude that it could do something about this threat.

In recent years, the agency has been developing and supporting communities of innovators who are doing the science and applying the lessons they are learning to create a technology platform that stands a chance of this: preventing any outbreak of infectious disease—anywhere and anytime—from growing into a global conflagration like the one we are experiencing right now.


In this new episode of the Voices from DARPA podcast, join a team of program managers in the agency's Biological Technologies Office as they explain how they are striving to develop a multi-pronged technology

platform that has the potential to render COVID-19 humanity's last pandemic.

This latest episode of the Voices from DARPA podcast, as well as all of the others, are accessible from the DARPA website (https://www.darpa.mil/about-us/podcast).

Blubrry (podcast host): https://blubrry.com/voices_from_darpa/57709321/episode-24-preventing-pandemics/

YouTube: https://youtu.be/Op1yFcwsxjs

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

Episode 24: Preventing Pandemics: Transcript at: https://www.darpa.mil/attachments/Episode_24_curated.pdf

*Number 10*

## School Closings Due to COVID-19 Present Potential for Increased Risk of Child Exploitation

Due to school closings as a result of COVID-19, children will potentially have an increased online presence and/or be in a position that puts them at an inadvertent risk.

Due to this newly developing environment, the FBI is seeking to warn parents, educators, caregivers, and children about the dangers of online sexual exploitation and signs of child abuse.

## Background

Online sexual exploitation comes in many forms. Individuals may coerce victims into providing sexually explicit images or videos of themselves, often in compliance with offenders' threats to post the images publicly or send the images to victims' friends and family.

Other offenders may make casual contact with children online, gain their trust, and introduce sexual conversation that increases in egregiousness over time.

Ultimately this activity may result in maintaining an online relationship that includes sexual conversation and the exchange of illicit images, to eventually physically meeting the child in-person.

In order for the victimization to stop, children typically have to come forward to someone they trust—typically a parent, teacher, caregiver, or law enforcement.

The embarrassment of being enticed and/or coerced to engage in unwanted behavior is what often prevents children from coming forward.

Offenders may have hundreds of victims around the world, so coming forward to help law enforcement identify offenders may prevent countless other incidents of sexual exploitation.

Abuse can occur offline through direct contact with another individual.

During these uncertain conditions, where time with other adults and caregivers has increased immensely, parents/guardians should communicate with their children about appropriate contact with adults and watch for any changes in behavior, including an increase in nightmares, withdrawn behavior, angry outbursts, anxiety, depression, not wanting to be left alone with an individual, and sexual knowledge.

## Recommendations

Parents and guardians can take the following measures to help educate and prevent children from becoming victims of child predators and sexual exploitation during this time of national emergency:

## Online Child Exploitation

- Discuss Internet safety with children of all ages when they engage in online activity.
- Review and approve games and apps before they are downloaded.
- Make sure privacy settings are set to the strictest level possible for online gaming systems and electronic devices.
- Monitor your children's use of the Internet; keep electronic devices in an open, common room of the house.
- Check your children's profiles and what they post online.
- Explain to your children that images posted online will be permanently on the Internet.
- Make sure children know that anyone who asks a child to engage in sexually explicit activity online should be reported to a parent, guardian, or other trusted adult and law enforcement.
- Remember that victims should not be afraid to tell law enforcement if they are being sexually exploited. It is not a crime for a child to send sexually explicit images to someone if they are compelled or coerced to do so.

## Child Abuse Awareness

- Teach your children about body safety and boundaries.
- Encourage your children to have open communication with you.
- Be mindful of who is watching your child for childcare/babysitting, playdates and overnight visits.
- If your child discloses abuse, immediately contact local law enforcement for assistance.
- Children experiencing hands-on abuse may exhibit withdrawn behavior, angry outbursts, anxiety, depression, not wanting to be left alone with a specific individual, non-age appropriate sexual knowledge, and an increase in nightmares.

## Victim Reporting

Reporting suspected sexual exploitation can help minimize or stop further victimization, as well as lead to the identification and rescue of other possible victims.

If you believe you are—or someone you know is—the victim of child sexual exploitation:

- Contact your local law enforcement agency.
- Contact your local FBI field office or submit a tip online at tips.fbi.gov.
- File a report with the National Center for Missing & Exploited Children (NCMEC) at 1-800-843-5678 or online at www.cybertipline.org.

When reporting, be as descriptive as possible in the complaint form by providing as much of the following as possible:

- Name and/or username of the subject.
- Email addresses and phone numbers used by the subject.
- Websites used by the subject.
- Description of all interaction with the subject.
- Try to keep all original documentation, emails, text messages, and logs of communication with the subject. Do not delete anything before law enforcement is able to review it.
- Tell law enforcement everything about the online encounters—we understand it may be embarrassing for the parent or child, but providing all relevant information is necessary to find the offender, stop the abuse, and bring him/her to justice.

More information about the FBI's guidance on child sexual exploitation and protecting your kids at: https://www.fbi.gov/scams-and-safety/protecting-your-kids

*Number 11*

## FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide.

The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.

Within the FBI Boston Division's area of responsibility (AOR), which includes Maine, Massachusetts, New Hampshire, and Rhode Island, two schools in Massachusetts reported the following incidents:

- In late March 2020, a Massachusetts-based high school reported that while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialed into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction.

- A second Massachusetts-based school reported a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos.

As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.

- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.

- Manage screensharing options. In Zoom, change screensharing to "Host Only."

- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

If you were a victim of a teleconference hijacking, or any cyber-crime for that matter, report it to the FBI's Internet Crime Complaint Center at ic3.gov

*Number 12*

## PIPES Researchers Demonstrate Optical Interconnects to Improve Performance of Digital Microelectronics

Researchers replace traditional electronic I/O with optical signaling interfaces to achieve major improvements in link reach and efficiency


Under DARPA's Photonics in the Package for Extreme Scalability (PIPES) program, researchers from Intel and Ayar Labs have demonstrated early progress towards improving chip connectivity with photons – or light.

Signaling over optical fibers enables the internet today and optical transceivers are ubiquitous in data centers, yet digital systems still rely upon the movement of electrons over metal wires to push data between integrated circuits (ICs) on a board.

Increasingly, the limitations of electrical signaling from the chip package restrict overall bandwidth and signaling efficiency, throttling the performance of advanced systems.

The PIPES program is exploring ways to expand the use of optical components to address these constraints and enable digital microelectronics with new levels of performance.

Researchers from Intel and Ayar Labs working on PIPES have successfully replaced the traditional electrical input/output (I/O) of a state-of-the-art field programmable gate array (FPGA) with efficient optical signaling interfaces.

The demonstration leverages an optical interface developed by Ayar Labs called TeraPHY, an optical I/O chiplet that replaces electrical serializer/deserializer (SERDES) chiplets.

These SERDES chiplets traditionally compensate for limited I/O when there is a need for fast data movement, enabling high-speed communications and other capabilities.

Using Intel's advanced packaging and interconnect technology, the team integrated TeraPHY and the Intel FPGA core within a single package, creating a multi-chip module (MCM) with in-package optics.

The integrated solution substantially improves interconnect reach, efficiency, and latency – enabling high-speed data links with single mode optical fibers coming directly from the FPGA.

Built in GlobalFoundries' advanced photonics process, the co-packaged TeraPHY chiplet used for this demonstration is capable of 2 Terabits per second (Tbps) of I/O bandwidth at a small fraction of power compared to electrical I/O.

"This early PIPES program demonstration is a big step towards enabling powerful systems that leverage the advantages of optical signaling," said Dr. Gordon Keeler, the DARPA program manager leading PIPES.

"A key goal of the program is to develop advanced ICs with photonic interfaces capable of driving >100 terabits per second (Tbps) I/O per package at energies below one picojoule per bit (pJ/bit).

FPGAs with photonic interfaces will have broad impact, improving high-performance computing, artificial intelligence, large-scale emulation, and DoD-specific capabilities such as advanced radars.

With this demonstration, the Intel team has made a solid step towards our goal."

To accomplish the demonstration, Intel and Ayar Labs' researchers leveraged technical advances achieved under two other DARPA programs – the Photonically Optimized Embedded Microprocessors (POEM) and Common Heterogeneous Integration and IP Reuse Strategies (CHIPS) programs.

Now concluded, the DARPA POEM program sought to develop photonic technologies that could be integrated within embedded microprocessors to enable seamless, energy-efficient, high-capacity communications within and between the microprocessor and dynamic random access memory (DRAM).

Ayar Labs' work under POEM helped generate the first TeraPHY optical I/O chiplet.

Researchers also leveraged low-power signaling standards and chiplet packaging processes developed by Intel under the DARPA CHIPS program.

To help address skyrocketing design costs and increase system flexibility, CHIPS is working to develop an ecosystem of discrete modular, reusable IP block that can be assembled into systems using various integration technologies.

Critical to this effort was the establishment of a common interface standard, which Intel supplied via the Advanced Interface Bus (AIB).

AIB is a publicly available, open interface standard that enables Intel and other silicon IP providers working under the program to easily build chiplets that can inter-operate with each other.

The PIPES team used the AIB interface standards to integrate the MCM and in-package optics.

As PIPES progresses, the Intel team will continue to advance performance of the integrated technologies.

Through the next phases of the program, all PIPES researchers will focus on enabling aggregate signaling rates to 100 Tbps and beyond, maturing various photonics technologies, and meeting demanding metrics for efficiency, latency, and bandwidth density.

*Number 13*

## Proliferated Commercial Satellite Constellations, Implications for National Security

By Matthew A. Hallex and Travis S. Cottom


The falling costs of space launch and the increasing capabilities of small satellites have enabled the emergence of radically new space architectures—proliferated constellations made up of dozens, hundreds, or even thousands of satellites in low orbits.

Commercial space actors—from tiny startups to companies backed by billions of dollars of private investment— are pursuing these new architectures to disrupt traditional business models for commercial Earth observation and satellite communications.

The success of these endeavors will result in new space-based services, including global broadband Internet coverage broadcast from orbit and high-revisit overhead imagery of much of the Earth's surface.

The effects of proliferated constellations will not be confined to the commercial sector.

The exponential increase in the number of satellites on orbit will shape the future military operating environment in space.

The increase in the availability of satellite imagery and communications bandwidth on the open market will also affect the operating environment in the ground, maritime, and air domains, offering new capabilities that can address hard problems facing the U.S. military, such as tracking mobile targets, operating in the Arctic, or providing resilient space support in the face of growing counterspace threats.

These trends will also create new challenges as adversaries ranging from Great Power competitors to hostile nonstate actors gain cheap access to space capabilities and the emergence of space-based Internet reshapes the cyber battlespace.

This article discusses some of the proposed commercial proliferated constellations being developed in the United States and abroad and

explores the potential effects of proliferated constellations on the space, terrestrial, and cyber domains.

It identifies the multidomain challenges and opportunities these trends create for the warfighter and proposes steps that the Department of Defense (DOD) and the broader national security community can take to prepare.

To read more (page 23/132):
https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97.pdf

*Number 14*

# Advisory: COVID-19 exploited by malicious cyber actors



This is a joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

## Introduction

This advisory provides information on exploitation by cyber criminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic.

It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

## COVID-19 exploitation

An increasing number of malicious cyber actors are exploiting the current COVID-19 pandemic for their own objectives.

In the UK, the NCSC has detected more UK government branded scams relating to COVID-19 than any other subject.

Although, from the data seen to date, the overall levels of cyber crime have not increased both the NCSC and CISA are seeing a growing use of COVID-19 related themes by malicious cyber actors.

At the same time, the surge in home working has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPNs), amplifying the threat to individuals and organisations.

APT groups and cyber criminals are targeting individuals, small and medium businesses and large organisations with COVID-19 related scams and phishing emails.

This advisory provides you with an overview of COVID-19 related malicious cyber activity.

It offers practical advice that individuals and organisations can follow to reduce the risk of being affected.

The IOCs provided within the accompanying .csv and .stix files of this advisory are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this advisory does not seek to catalogue all COVID-19 related malicious cyber activity. You should remain alert to increased activity relating to COVID-19 and take proactive steps to protect yourself and your organisation.

## Summary of attacks

APT groups and cyber criminals are exploiting the COVID-19 pandemic as part of their cyber operations.

These cyber threat actors will often masquerade as trusted entities.

Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised.

Their goals and targets are consistent with long-standing priorities such as espionage and information operations.

Cyber criminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cyber criminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months.

Threats observed include:

• Phishing, using the subject of coronavirus or COVID-19 as a lure
• Malware distribution using coronavirus or COVID-19 themed lures
• Registration of new domain names containing coronavirus or COVID-19 related wording
• Attacks against newly (and often rapidly) deployed remote access or remote working infrastructure.

## Social engineering techniques

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action.

These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

• Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.

o For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install 'CovidLock' ransomware on their device.

• Open a file (such as an email attachment) which contains malware.

o For example, email subject lines contain COVID-19 related phrases such as 'Coronavirus Update' or '2019-nCov: Coronavirus outbreak in your city (Emergency).'


*Figure 1 – UK Government themed SMS phishing*

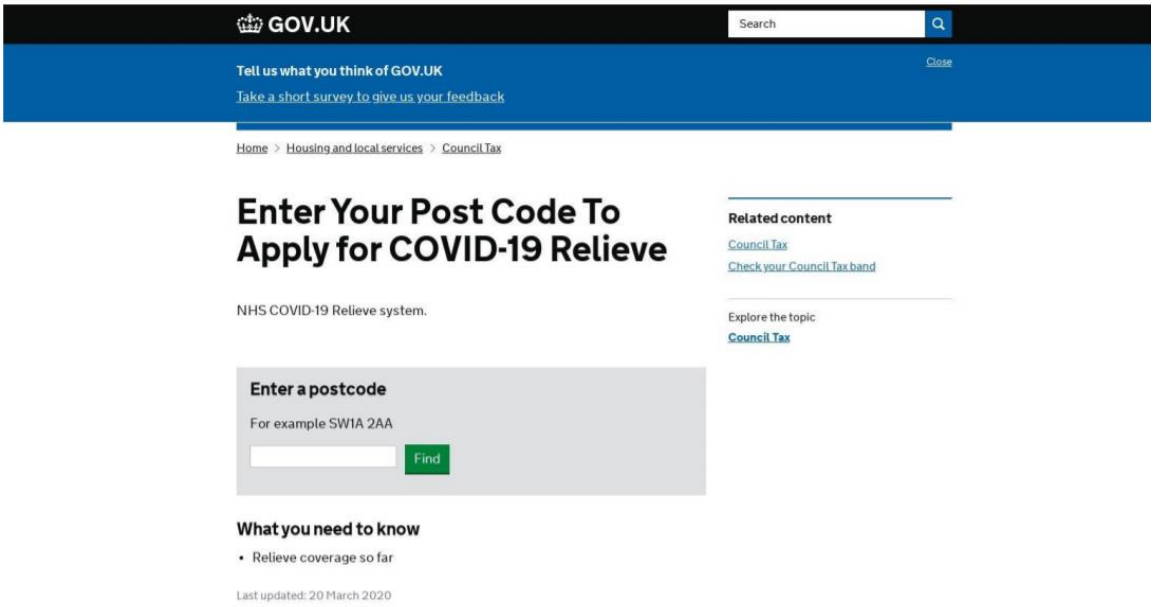
To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with 'Dr.' in their title.

In several examples, actors send phishing emails that contain links to a fake email login page.

Other examples purport to be from an organisation's human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus or COVID-19 related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf."

Note: A non-exhaustive list of IOCs related to this activity is provided within the accompanying .csv and .stix files linked to this advisory.




To read more:
https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

*Number 15*

U.S. Attorney Scott Brady and Pennsylvania Attorney General Josh Shapiro

## Zoom-Bombing and Hacking Teleconferences During Coronavirus Pandemic

Scott W. Brady, United States Attorney for the Western District of Pennsylvania, and Pennsylvania Attorney General Josh Shapiro today warned against hacking teleconferences during the coronavirus pandemic. The Western Pennsylvania COVID-19 Task Force will investigate, disrupt and prosecute such hacking.

Many Pennsylvania residents have turned to video-teleconferencing platforms, such as Zoom, to stay connected during the COVID-19 pandemic. Unfortunately, as the FBI has reported, there has been a rise in so-called "Zoom-bombing," or video hacking across the United States, where uninvited hackers disrupt conferences and online classrooms with pornographic images, hate images and/or threatening language.

These attacks have also targeted religious communities, minority groups, and vulnerable populations, such as Alcoholics Anonymous meetings. Some hackers have planned coordinated attacks through websites and social media, including Discord and Instagram, in violation of the terms of use. Pennsylvanians have seen several instances of such hacking within the past week.

Western Pennsylvania's chief federal, state, and local law enforcement officials are joining together to warn that anyone who hacks into a teleconference can be charged with state or federal crimes.

Charges may include: disrupting a public meeting, computer intrusion, using a computer to commit a crime, hate crimes, fraud, or transmitting threatening communications. When hackers work together on coordinated attacks, they can also be charged with conspiracy. All of these charges are punishable by fines and imprisonment.

U.S. Attorney Brady said, "Hackers are disrupting business and community meetings for sport and targeting specific groups, including addiction recovery meetings, in order to mock, harass and interfere with treatment.

This is another low point in this crisis. We are better than this. DOJ will use all of our resources to find, expose and prosecute these low-lifes."

"At a time when people need internet conferencing technology to do essential business or to connect with loved ones, it's vital that we make these platforms safe from hackers," Attorney General Josh Shapiro said. "People need confidence in the services they are relying upon during this emergency. Through my Office's partnership with the Western Pennsylvania COVID-19 Fraud Task Force, we will be able to investigate and prosecute hackers."

"The COVID-19 pandemic has led to a spike in businesses and employees teleworking to communicate and share information over the internet," said Acting FBI Pittsburgh Special Agent in Charge Eugene Kowel. "Cyber criminals see this as an easy way to take advantage of vulnerable members of our community and to exploit telework software vulnerabilities to obtain sensitive information.

The FBI encourages users to safeguard their user information and prevent these malicious cyber actors from eavesdropping or stealing sensitive information. We ask anyone with information about criminal activities, especially those exploiting the disruptions caused by the Coronavirus, to contact us."

"Over the course of the next several weeks, the United States Secret Service's primary investigative priorities will be to mitigate any efforts by criminals that target citizens for cyber-enabled crimes and identity theft as it relates to COVID-19 scams," said Tim Burke, Special Agent in Charge, United States Secret Service Pittsburgh Field Office.

"In doing so, we at the Secret Service are grateful to be joining our fellow law enforcement partners on the COVID-19 Fraud Task Force. Together, the COVID-19 Task Force will enable us to focus our resources to uncover, investigate, and prevent these crimes more effectively in a unified front."

"Every community and their leadership are appreciative of the efforts that all of the Federal agencies are putting forth in addressing the issues of Zoom-bombing," added Bruce A. Fromlak, West View Borough Chief of Police and President of the Western Pennsylvania Chiefs of Police Association.

"As we conduct business each and every day we are presented with new challenges. This is clearly a new challenge however this too will be dealt with in cooperation with all of our law enforcement partners and professional law enforcement organizations. We will approach and address

all malicious attacks in an expeditious and professional manner in order to bring any and all unscrupulous individuals to justice."

As individuals continue the transition to online lessons and meetings, law enforcement recommends exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconferencing threats:

• Do not make the meeting or classroom public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control which guests are admitted.

• Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.

• Manage screen sharing options. In Zoom, change screen sharing to "Host Only."

• Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

• Understand the features of your specific teleconference platform, including how to close a conference call in the middle and how to kick out people who are disrupting. Zoom has posted these steps on their blog.

• Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

If you were a victim of a teleconference hijacking, or any cyber-crime for that matter, report it to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/default.aspx.

For more information regarding teleconference hijacking: https://www.ic3.gov/media/2020/200401.aspx.

## 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.*