April 2019, cyber risk and compliance in Switzerland

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

Dear readers and friends,

I am pleased to learn that the Cyber Defence Campus (CYD) of the Federal Department of Defence, Civil Protection and Sport (DDPS) is very well designed. It focuses on early detection and observation of current developments in the cyberworld, and development of action strategies.

The CYD campus is one of several initiatives of the national strategy for the protection of Switzerland against cyber risks (NCS) that were launched to more effectively counter the current challenges of the cyberworld. Under the leadership of armasuisse Science and Technology, experts from the DDPS, industry and universities have joined hands to develop broad expertise in all areas relevant to cyber issues.

The CYD campus officially commenced operation in January 2019, and it works closely with the Eidgenössische Technische Hochschule (ETH) in Zurich and the École polytechnique fédérale de Lausanne (EPFL). Industry and international partners are also integrated in the activities.

The services of the CYD campus are constantly being expanded in order to offer the full range of DDPS services as a competence centre. It will take a while for the campus to be fully effective for the DDPS. The competences and expertise will be built up gradually over the next two years. The initial focus is on areas such as cybersecurity, artificial intelligence and data analysis.

Malvertising (malicious advertising) is a very interesting attack method, used by state sponsored attack groups and criminals. It is based on the behavioural patterns of persons visiting specific web sites.

Intelligence agencies have teams of agents, psychologists and psychiatrists that study the behaviour of individuals online, their motivation, their

perceptions, and the means by which they take risks to satisfy their curiosity and needs.

Experts understand that online porn addiction is closely tied to guilt, shame, negative feelings that stem from moral or religious beliefs, that is often followed by inability to resist, excitement in the hope of finding something interesting, and then disappointment until the next effort.

During this upsetting loop, online porn addicts feed their hope clicking on advertisements.

Intelligence agencies know how to deploy sophisticated psychological control techniques matched to the vulnerabilities they have detected in online visitors, in order to manipulate, apply pressure, and induce a person to click on their advertisements.

How it works? Well, this is just one out of many approaches.

Step 1 – The state-sponsored group, using fraudulent identities and intermediaries, buys advertising traffic from pornographic websites. Now they can post advertisements.

Step 2 – When users click on the ads, they are redirected to websites hosting highly-sophisticated exploits and tools, including the Angler Exploit Kit (AEK).

Users with any vulnerabilities in their browsers or computers can be infected with a malicious payload.

Step 3 – Here we have deception and some income. In some cases, the malicious payload will lock the user's browser. Once locked, we have a computer infected with ransomware.

Alternatively, users will be blackmailed to pay the ransom demand to avoid disclosure of the "evidence" attackers have for their online behaviour. In other cases, the infected computer will be used as a member of a botnet.

So, it looks like they are criminals and hackers behind this attack.

Step 4 – Here we have the real attack. The computer is silently and secretly infected and there is no easy way to find the payload.

The user's data are transferred and studied, to be used to attack companies, banks, politicians, the government and the critical infrastructure. There are so many secrets hidden in files and emails stored in thousands of infected computers, that can be used for manipulation, blackmail and bribery.

Step 5 starts with the old carrot and stick approach. This is the real game for the intelligence agency behind the attack.

The UK's Centre for the Protection of National Infrastructure (CPNI) released in April 2013 a very important paper, about an important challenge, the insider threat.

You may ask, where is the point, this paper was released 6 years ago!

Revisiting previous approaches and trends is never a waste of time. On the contrary, you can understand better what works and what not, and how the business environment has been changed.

What motivates insider activity?

In the paper, three main types of insider behaviour are described:

- Deliberate insider: those who obtain employment with the deliberate intent of abusing their access.

- Volunteer/self-initiated insider: those who obtain employment without deliberate intent to abuse their access, but at some point personally decide to do so.

- Exploited/recruited insider: those who obtain employment without deliberate intent to abuse their access, but at some point are exploited or recruited by a third party to do so.

The last two types of insider behaviour described above are defined as 'opportunistic' due to the lack of deliberate targeting of employment.

The findings from this study suggest that the vast majority (76%) of insider cases assessed were self-initiated, 15% of cases were exploited or recruited by a third party, and "only 6% were as a result of deliberate infiltration".

Well, this *only 6%* is the real message for me, the number is large, and it is very scary. It can involve blackmail, bribery or both.

We continue with the paper:

Primary motivation

The research demonstrated that the reasons why people undertake insider activity are complex and multifaceted. It is relatively common for insiders to have more than one motivation for their activity, with a third of the cases

in the study being identified with more than one motivating factor.

The range of primary motivations was identified as:

- Financial gain (47% of cases).
- Ideology (20% of cases).
- Desire for recognition (14% of cases).
- Loyalty to friends/family/country (14% of cases).
- Revenge (6% of cases).

This demonstrates that although financial gain was the single most common primary motivation, ideology, a desire for recognition and loyalty (to friends/family/country) were also quite common motivations.

Although revenge against the employer was noted as a primary motivator in only 6% of cases, general disaffection with the employing organisation continued to be a contributory factor in many of the cases assessed.

The research showed that in many insider cases there was an element of disaffection displayed by the employee.

This ranged from being the main reason for the employee deciding to commit an insider act, to simply being disengaged from their employer and therefore not feeling committed to their organisation.

The research identified a clear pattern in the relationship between primary motivation and type of insider incident.

- Ideology and desire for recognition were closely linked to unauthorised disclosure of sensitive information. Ideology was the primary motivation for 40% of unauthorised disclosures and desire for recognition accounted for 22%.

- Financial gain was most closely linked to process corruption or giving access to assets. Financial gain was the primary motivation for 83% of process corruption cases and for 63% of facilitation of access to assets.

- Cases involving loyalty were fairly evenly split between unauthorised disclosure and process corruption.

- For those motivated by revenge, the cases were split between unauthorised disclosure and sabotage.

Personality traits

The study examined the importance of a range of personality factors

among the cases that were reviewed in depth. For the purposes of this study, personality was defined as the characteristics of the individual relating to how they respond to situations and interact with others.

The personality factors listed below were considered to be of particular interest (and predictive of case type) when significant signs were shown that had a clear and negative impact on work and/or colleagues:

- Immature (e.g. lacks life experience, is naïve and requires excessive guidance, has difficulty making life decisions);

- Low self-esteem (e.g. lacks confidence, is extremely dependent on recognition and praise, struggles to cope well with adversity, setbacks and difficult tasks);

- Amoral and unethical (e.g. lacks moral values or personal integrity, acts in an unscrupulous manner and shows no remorse, engages in unethical behaviour);

- Superficial (e.g. lacks a sense of identity and is hard to get to know, provokes a range of different opinions among people in the workplace);

- Prone to fantasising (e.g. believes they are engaged in activities that have no basis in reality, likes to create the impression that they are engaged in something special);

- Restless and impulsive (e.g. requires constant stimulation and cannot tolerate boredom, needs or seeks instant gratification and does whatever feels good in the moment, shifts from one thing to another);

- Lacks conscientiousness (e.g. does not comply with rules, neglects responsibilities and is unconcerned with duties and obligations, shows poor attention to detail and demonstrates poor judgement, shows a lack of focus);

- Manipulative (e.g. uses charm to get their own way and is very persuasive, nurtures relationships and manipulates others to serve their own self-interest, tends to adopt whatever position or attitude will result in getting their own way);

- Emotionally unstable (e.g. is prone to exaggerated mood swings, overreacts to problems, complains about unimportant or trivial things);

- Evidence of psychological or personality disorders.

An insider is someone who (knowingly or unknowingly) misuses legitimate access to commit a malicious act or damage their employer.

These days, most insider acts involve IT exploitation termed "Cyber Insider".

CPNI has been engaging with industry and academia through a broad range of research initiatives that aim to improve IT monitoring capabilities to identify insider precursors and behaviour; raising awareness in employer and employee communities about insider threats; establish methods for designing IT and policies to deter staff from committing insider acts; designing IT and work practices to block insider acts.

U.S. Senators Chris Van Hollen (D-Md.) and Marco Rubio (R-Fla.) reintroduced the *Defending Elections from Threats by Establishing Redlines (DETER)* Act.

The legislation, which gained strong momentum last Congress, sends a clear message to foreign actors seeking to disrupt elections.

Risk and compliance professionals are very interested in the definition of "election and campaign infrastructure": "information and communications technology and systems used by or on behalf of—

(A) the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, equipment for the secure transmission of election results, and other systems; or

(B) a principal campaign committee or national committee with respect to strategy or tactics affecting the conduct of a political campaign, including electronic communications, and the information stored on, processed by, or transiting such technology and systems."

I also find very interesting the approach of Section 204, *SENSE OF CONGRESS ON STRATEGY ON COORDINATION WITH EUROPEAN UNION:*

"It is the sense of Congress that, not later than 180 days after the date of the enactment of this Act, the President should submit to the appropriate congressional committees and leadership a strategy on how the United States will—
(1) work in concert with the European Union and member countries of the European Union to deter interference by the Government of the Russian

Federation in elections; and

(2) coordinate with the European Union and member countries of the European Union to enact legislation similar to this Act.

Background

Reporting Requirements

The Director of National Intelligence (DNI) must issue to Congress a determination on whether any foreign government has interfered in that election within 60 days after every federal election.

The DNI must also provide identify any senior Russian political figure or oligarch that knowingly contributed to interference in a United States election.

Actions That Will Elicit Retaliation

A foreign government, or an agent acting on its behalf, cannot undertake the following actions with the intent to influence an election's outcome:

- purchase advertisements to influence an election, including online ads
- use social and traditional media to spread information to Americans under a false identity
- hack and release or modify election and campaign infrastructure, including voter registration databases and campaign emails
- block or otherwise hinder access to elections infrastructure, such as websites providing information on polling locations

Russia-Specific Sanctions

If the DNI determines that the Kremlin has once again interfered in an American federal election, the bill mandates a set of severe sanctions that must be implemented within 30 days of the DNI's determination.

This includes sanctions on major sectors of the Russian economy, including finance, energy, and defense.

Every senior Russian political figure or oligarch, identified by the DNI in his determination to Congress, will be blacklisted from entering the United States and will have their assets blocked.

The Administration is also required to work with the European Union to enlist their support in adopting a sanctions regime to broaden the impact.

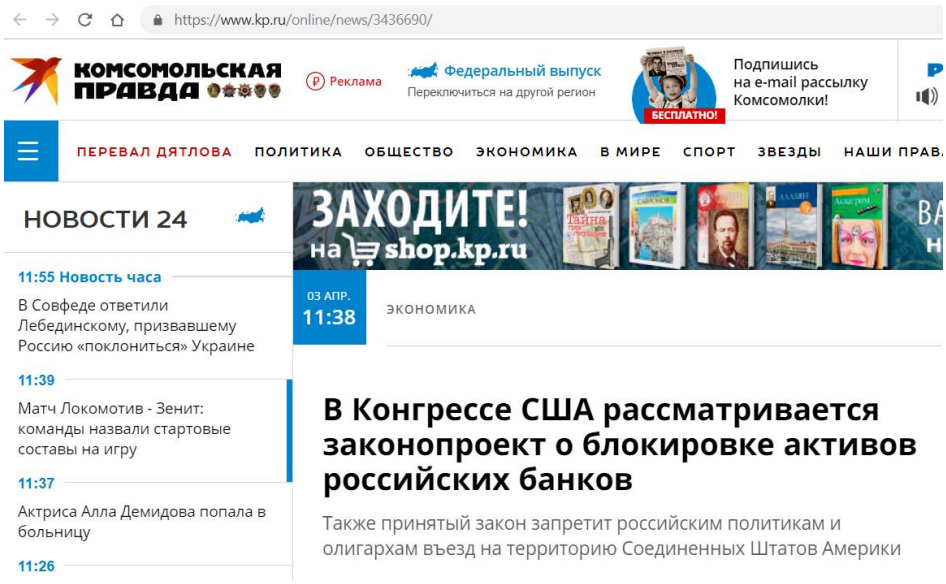
Preparing for Other Potential Attacks

The DNI has identified China, Iran, and North Korea as our other major foreign government cyber threats, and they may also seek to exploit American vulnerabilities in the next election cycle.

The Administration should present Congress with a strategy preventing interference in our elections for each of these countries and any other foreign state of significant concern.

The draft:
https://www.rubio.senate.gov/public/_cache/files/848643fd-db7a-447a-8db0-aca2e080f555/CA616C85336870AEF1D5DC78D3980515.20190403-vanhollen-rubio-deter-act-as-introduced.pdf

I have spent some time using Google translate (Russian to English) to understand the Russian point of view.



For example, we read at the title above “В Конгрессе США рассматривается законопроект о блокировке активов российских банков” that is translated by google “The US Congress is considering a bill to block the assets of Russian banks.”

Another interesting development On March 26, President Donald J. Trump signed the Executive Order on Coordinating National Resilience to Electromagnetic Pulses.

This is the first-ever comprehensive whole-of-government policy to build resilience and protect against electromagnetic pulses, or EMPs, which are temporary electromagnetic signals that can disrupt, degrade, and damage technology and critical infrastructure systems across large areas.

The strategy also reflects a consensus Intelligence Community assessment of the EMP threat posed by our nation's adversaries. Primarily focused on Departmental activities, the DHS strategy recognizes the importance of continued close collaboration with federal, state, local, tribal, and territorial decision-makers, sector-specific agencies, and private sector critical infrastructure owner-operators.

"Electromagnetic pulse" (EMP) is a burst of electromagnetic energy. EMPs have the potential to negatively affect technology systems on earth and in space.

A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of Earth.

A geomagnetic disturbance (GMD) is a type of natural EMP driven by a temporary disturbance of Earth's magnetic field resulting from interactions with solar eruptions.

Both HEMPs and GMDs can affect large geographic areas.

Assessments of the risks to civilian critical infrastructure from electromagnetic incidents are intrinsically difficult to produce due to the rarity—or complete absence—of actual events, as well as the fundamental complexity of predicting real-world interactions between electromagnetic pulses and thousands of diverse infrastructure installations.

I remember a joke. Why actuaries recommend selling more life insurance policies to 100-year olds? Because, according to actuarial tables, very few of them die each year. The moral of the story: We cannot model, understand well, or calculate the impact and the likelihood of tail risks.

Owners and operators of critical infrastructure systems have significant uncertainty regarding risks posed by major electromagnetic events, and mitigation techniques that would address current vulnerabilities or increase resilience.

These uncertainties make it difficult to evaluate the return on investments made in preparedness actions and protection measures.

Read more at Number 1 below. 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_2019.pdf

Number 1 (Page 13)

Secretary Nielsen Statement on Executive Order to Protect the U.S. from Electromagnetic Pulse Attacks

On March 26, President Donald J. Trump signed the Executive Order on Coordinating National Resilience to Electromagnetic Pulses, the first-ever comprehensive whole-of-government policy to build resilience and protect against electromagnetic pulses, or EMPs, which are temporary electromagnetic signals that can disrupt, degrade, and damage technology and critical infrastructure systems across large areas.

Number 2 (Page 24)

Interpol reviews its rules for the international exchange of criminal data

A legal framework that allows police worldwide to share details on crimes and criminals effectively in line with international standards

Interpol has launched a review of its Rules on the Processing of Data (RPD) to ensure they continue to meet the needs of international police cooperation in a digital world.

Number 3 (Page 26)

DARPA Seeks to Make Scalable On-Chip Security Pervasive

Program to focus on addressing the economic and technical challenges associated with incorporating scalable defense mechanisms into chip designs

For the past decade, cybersecurity threats have moved from high in the software stack to progressively lower levels of the computational hierarchy, working their way towards the underlying hardware.

The rise of the Internet of Things (IoT) has driven the creation of a rapidly growing number of accessible devices and a multitude of complex chip designs needed to enable them.

Number 4 (Page 30)

Data exposed by banking app security flaws

National Cyber Security Centre

Vulnerabilities have been found in the mobile applications of 30 financial service providers.

The report, by cyber security company Arxan, revealed that source code, back-end accesses and sensitive data are at risk after a researcher download various apps from the Google Play store.

Number 5 (Page 31)

Avoiding the Crack of Doom

New imaging technique reveals how mechanical damage begins at the molecular scale.

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

Just as a journey of 1,000 miles begins with a single step, the deformations and fractures that cause catastrophic failure in materials begin with a few molecules torn out of place. This in turn leads to a cascade of damage at increasingly larger scales, culminating in total mechanical breakdown.

That process is of urgent interest to researchers studying how to build high-strength composite materials for critical components ranging from airplane wings and wind-turbine blades to artificial knee joints.

Number 1

Secretary Nielsen Statement on Executive Order to Protect the U.S. from Electromagnetic Pulse Attacks

On March 26, President Donald J. Trump signed the Executive Order on Coordinating National Resilience to Electromagnetic Pulses, the first-ever comprehensive whole-of-government policy to build resilience and protect against electromagnetic pulses, or EMPs, which are temporary electromagnetic signals that can disrupt, degrade, and damage technology and critical infrastructure systems across large areas.

"EMPs pose a potential threat to our nation's critical infrastructure, and this executive order will advance our national goal of increased resilience across all infrastructure sectors. DHS remains committed to working with our interagency partners to ensure a more resilient, prepared America by reducing the risk of EMP events. DHS is grateful for the president's leadership on this critical issue and continued commitment to protecting our country and keeping Americans safe," said Homeland Security Secretary Kirstjen M. Nielsen.

The executive order outlines DHS' lead role in implementing the following activities:

- Provide timely information on credible EMP threats and events to stakeholders;

- Take a risk-informed approach to understand and enhance resilience to the effects of EMP across all critical infrastructure sectors, including coordinating the identification of national critical functions and prioritization of associated critical infrastructure at greatest risk to the effects of EMP;

- Coordinate response to and recovery from the effects of EMP on critical infrastructure;

- Consider EMP scenarios as a factor in preparedness exercises;

- Conduct R&D to better understand and more effectively model the effects of EMP on national critical functions, and then develop technologies and guidelines to protect this critical infrastructure;

- Maintain survivable means to provide necessary emergency information to the public during and after an EMP event; and

- Develop quadrennial EMP risk assessments, with the first risk assessment delivered within 1 year of this order.

The executive order will foster increased resilience to EMP events through better data gathering, testing, risk assessments, and private sector coordination.

It directs departments and agencies to coordinate and streamline efforts, while fostering an environment that promotes private sector innovation to strengthen our critical infrastructure.

DHS last year announced the Strategy for Protecting and Preparing the Homeland against Threats from Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD), which laid out a clear vision and an approach for DHS to take to protect critical infrastructure and prepare to respond and recover from potentially catastrophic electromagnetic incidents.

The strategy also reflects a consensus Intelligence Community assessment of the EMP threat posed by our nation's adversaries. Primarily focused on Departmental activities, the DHS strategy recognizes the importance of continued close collaboration with federal, state, local, tribal, and territorial decision-makers, sector-specific agencies, and private sector critical infrastructure owner-operators.

Before the Executive Order:
https://www.dhs.gov/sites/default/files/publications/18_1009_EMP_GMD_Strategy-Non-Embargoed.pdf

Executive Order on Coordinating National Resilience to Electromagnetic Pulses

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. An electromagnetic pulse (EMP) has the potential to disrupt, degrade, and damage technology and critical infrastructure

systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs.

Sec. 2. Definitions. As used in this order:

(a) "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(b) "Electromagnetic pulse" is a burst of electromagnetic energy. EMPs have the potential to negatively affect technology systems on Earth and in space. A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of Earth. A geomagnetic disturbance (GMD) is a type of natural EMP driven by a temporary disturbance of Earth's magnetic field resulting from interactions with solar eruptions. Both HEMPs and GMDs can affect large geographic areas.

(c) "National Critical Functions" means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
(d) "National Essential Functions" means the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency, such as an EMP that adversely affects the performance of Government.

(e) "Prepare" and "preparedness" mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. These terms include the prediction and notification of impending EMPs.

(f) A "Sector-Specific Agency" (SSA) is the Federal department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those

identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

Sec. 3. Policy. (a) It is the policy of the United States to prepare for the effects of EMPs through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement.

The Federal Government must provide warning of an impending EMP; protect against, respond to, and recover from the effects of an EMP through public and private engagement, planning, and investment; and prevent adversarial events through deterrence, defense, and nuclear nonproliferation efforts. To achieve these goals, the Federal Government shall engage in risk-informed planning, prioritize research and development (R&D) to address the needs of critical infrastructure stakeholders, and, for adversarial threats, consult Intelligence Community assessments.

(b) To implement the actions directed in this order, the Federal Government shall promote collaboration and facilitate information sharing, including the sharing of threat and vulnerability assessments, among executive departments and agencies (agencies), the owners and operators of critical infrastructure, and other relevant stakeholders, as appropriate.

The Federal Government shall also provide incentives, as appropriate, to private-sector partners to encourage innovation that strengthens critical infrastructure against the effects of EMPs through the development and implementation of best practices, regulations, and appropriate guidance.

Sec. 4. Coordination. (a) The Assistant to the President for National Security Affairs (APNSA), through National Security Council staff and in consultation with the Director of the Office of Science and Technology Policy (OSTP), shall coordinate the development and implementation of executive branch actions to assess, prioritize, and manage the risks of EMPs. The APNSA shall, on an annual basis, submit a report to the President summarizing progress on the implementation of this order, identifying gaps in capability, and recommending how to address those gaps.

(b) To further the Federal R&D necessary to prepare the Nation for the effects of EMPs, the Director of OSTP shall coordinate efforts of agencies through the National Science and Technology Council (NSTC). The Director of OSTP, through the NSTC, shall annually review and assess the R&D needs of agencies conducting preparedness activities for EMPs, consistent with this order.

Sec. 5. Roles and Responsibilities. (a) The Secretary of State shall:

(i) lead the coordination of diplomatic efforts with United States allies and international partners regarding enhancing resilience to the effects of EMPs; and

(ii) in coordination with the Secretary of Defense and the heads of other relevant agencies, strengthen nuclear nonproliferation and deterrence efforts, which would reduce the likelihood of an EMP attack on the United States or its allies and partners by limiting the availability of nuclear devices.

(b) The Secretary of Defense shall:

(i) in cooperation with the heads of relevant agencies and with United States allies, international partners, and private-sector entities as appropriate, improve and develop the ability to rapidly characterize, attribute, and provide warning of EMPs, including effects on space systems of interest to the United States;

(ii) provide timely operational observations, analyses, forecasts, and other products for naturally occurring EMPs to support the mission of the Department of Defense along with United States allies and international partners, including the provision of alerts and warnings for natural EMPs that may affect weapons systems, military operations, or the defense of the United States;

(iii) conduct R&D and testing to understand the effects of EMPs on Department of Defense systems and infrastructure, improve capabilities to model and simulate the environments and effects of EMPs, and develop technologies to protect Department of Defense systems and infrastructure from the effects of EMPs to ensure the successful execution of Department of Defense missions;

(iv) review and update existing EMP-related standards for Department of Defense systems and infrastructure, as appropriate;

(v) share technical expertise and data regarding EMPs and their potential effects with other agencies and with the private sector, as appropriate;

(vi) incorporate attacks that include EMPs as a factor in defense planning scenarios; and

(vii) defend the Nation from adversarial EMPs originating outside of the United States through defense and deterrence, consistent with the mission and national security policy of the Department of Defense.

(c) The Secretary of the Interior shall support the research, development, deployment, and operation of capabilities that enhance understanding of variations of Earth's magnetic field associated with EMPs.

(d) The Secretary of Commerce shall:

(i) provide timely and accurate operational observations, analyses, forecasts, and other products for natural EMPs, exclusive of the responsibilities of the Secretary of Defense set forth in subsection (b)(ii) of this section; and

(ii) use the capabilities of the Department of Commerce, the private sector, academia, and nongovernmental organizations to continuously improve operational forecasting services and the development of standards for commercial EMP technology.

(e) The Secretary of Energy shall conduct early-stage R&D, develop pilot programs, and partner with other agencies and the private sector, as appropriate, to characterize sources of EMPs and their couplings to the electric power grid and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners.

(f) The Secretary of Homeland Security shall:

(i) provide timely distribution of information on EMPs and credible associated threats to Federal, State, and local governments, critical infrastructure owners and operators, and other stakeholders;

(ii) in coordination with the heads of any relevant SSAs, use the results of risk assessments to better understand and enhance resilience to the effects of EMPs across all critical infrastructure sectors, including coordinating the identification of national critical functions and the prioritization of associated critical infrastructure at greatest risk to the effects of EMPs;

(iii) coordinate response to and recovery from the effects of EMPs on critical infrastructure, in coordination with the heads of appropriate SSAs;

(iv) incorporate events that include EMPs as a factor in preparedness scenarios and exercises;

(v) in coordination with the heads of relevant SSAs, conduct R&D to better understand and more effectively model the effects of EMPs on national critical functions and associated critical infrastructure — excluding Department of Defense systems and infrastructure — and

develop technologies and guidelines to enhance these functions and better protect this infrastructure;

(vi) maintain survivable means to provide necessary emergency information to the public during and after EMPs; and

(vii) in coordination with the Secretaries of Defense and Energy, and informed by intelligence-based threat assessments, develop quadrennial risk assessments on EMPs, with the first risk assessment delivered within 1 year of the date of this order.

(g) The Director of National Intelligence shall:

(i) coordinate the collection, analysis, and promulgation, as appropriate, of intelligence-based assessments on adversaries' capabilities to conduct an attack utilizing an EMP and the likelihood of such an attack; and

(ii) provide intelligence-based threat assessments to support the heads of relevant SSAs in the development of quadrennial risk assessments on EMPs.

(h) The heads of all SSAs, in coordination with the Secretary of Homeland Security, shall enhance and facilitate information sharing with private-sector counterparts, as appropriate, to enhance preparedness for the effects of EMPs, to identify and share vulnerabilities, and to work collaboratively to reduce vulnerabilities.

(i) The heads of all agencies that support National Essential Functions shall ensure that their all-hazards preparedness planning sufficiently addresses EMPs, including through mitigation, response, and recovery, as directed by national preparedness policy.

Sec. 6. Implementation. (a) Identifying national critical functions and associated priority critical infrastructure at greatest risk.

(i) Within 90 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security. The Secretary of Homeland Security shall update this list as necessary.

(ii) Within 1 year of the identification described in subsection (a)(i) of this section, the Secretary of Homeland Security, in coordination with the

heads of other agencies as appropriate, shall, using appropriate government and private-sector standards for EMPs, assess which identified critical infrastructure systems, networks, and assets are most vulnerable to the effects of EMPs. The Secretary of Homeland Security shall provide this list to the President, through the APNSA. The Secretary of Homeland Security shall update this list using the results produced pursuant to subsection (b) of this section, and as necessary thereafter.

(b) Improving understanding of the effects of EMPs.

(i) Within 180 days of the identification described in subsection (a)(ii) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall review test data — identifying any gaps in such data — regarding the effects of EMPs on critical infrastructure systems, networks, and assets representative of those throughout the Nation.

(ii) Within 180 days of identifying the gaps in existing test data, as directed by subsection (b)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of SSAs and in consultation with the Director of OSTP and the heads of other appropriate agencies, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps. The heads of agencies identified in the plan shall implement the plan in collaboration with the private sector, as appropriate.

(iii) Within 1 year of the date of this order, and as appropriate thereafter, the Secretary of Energy, in consultation with the heads of other agencies and the private sector, as appropriate, shall review existing standards for EMPs and develop or update, as necessary, quantitative benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure.

(iv) Within 4 years of the date of this order, the Secretary of the Interior shall complete a magnetotelluric survey of the contiguous United States to help critical infrastructure owners and operators conduct EMP vulnerability assessments.

(c) Evaluating approaches to mitigate the effects of EMPs.

(i) Within 1 year of the date of this order, and every 2 years thereafter, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, and in consultation with the Director of OSTP, the heads of other appropriate agencies, and private-sector partners as

appropriate, shall submit to the President, through the APNSA, a report that analyzes the technology options available to improve the resilience of critical infrastructure to the effects of EMPs. The Secretaries of Defense, Energy, and Homeland Security shall also identify gaps in available technologies and opportunities for future technological developments to inform R&D activities.

(ii) Within 180 days of the completion of the activities directed by subsections (b)(iii) and (c)(i) of this section, the Secretary of Homeland Security, in coordination with the heads of other agencies and in consultation with the private sector as appropriate, shall develop and implement a pilot test to evaluate available engineering approaches for mitigating the effects of EMPs on the most vulnerable critical infrastructure systems, networks, and assets, as identified in subsection (a)(ii) of this section.

(iii) Within 1 year of the date of this order, the Secretary of Homeland Security, in coordination with the heads of relevant SSAs, and in consultation with appropriate regulatory and utility commissions and other stakeholders, shall identify regulatory and non regulatory mechanisms, including cost recovery measures, that can enhance private-sector engagement to address the effects of EMPs.

(d) Strengthening critical infrastructure to withstand the effects of EMPs.

(i) Within 90 days of completing the actions directed in subsection (c)(ii) of this section, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy and in consultation with the heads of other appropriate agencies and with the private sector as appropriate, shall develop a plan to mitigate the effects of EMPs on the vulnerable priority critical infrastructure systems, networks, and assets identified under subsection (a)(ii) of this section.

The plan shall align with and build on actions identified in reports required by Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure). The Secretary of Homeland Security shall implement those elements of the plan that are consistent with Department of Homeland Security authorities and resources, and report to the APNSA regarding any additional authorities and resources needed to complete its implementation. The Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy, shall update the plan as necessary based on results from the actions directed in subsections (b) and (c) of this section.

(ii) Within 180 days of the completion of the actions identified in subsection (c)(i) of this section, the Secretary of Defense, in consultation with the Secretaries of Homeland Security and Energy, shall conduct a

pilot test to evaluate engineering approaches used to harden a strategic military installation, including infrastructure that is critical to supporting that installation, against the effects of EMPs.

(iii) Within 180 days of completing the pilot test described in subsection (d)(ii) of this section, the Secretary of Defense shall report to the President, through the APNSA, regarding the cost and effectiveness of the evaluated approaches.

(e) Improving response to EMPs.

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, in coordination with the heads of appropriate SSAs, shall review and update Federal response plans, programs, and procedures to account for the effects of EMPs.

(ii) Within 180 days of the completion of actions directed by subsection (e)(i) of this section, agencies that support National Essential Functions shall update operational plans documenting their procedures and responsibilities to prepare for, protect against, and mitigate the effects of EMPs.

(iii) Within 180 days of identifying vulnerable priority critical infrastructure systems, networks, and assets as directed by subsection (a)(ii) of this section, the Secretary of Homeland Security, in consultation with the Secretaries of Defense and Commerce, and the Chairman of the Federal Communications Commission, shall provide the Deputy Assistant to the President for Homeland Security and Counterterrorism and the Director of OSTP with an assessment of the effects of EMPs on critical communications infrastructure, and recommend changes to operational plans to enhance national response and recovery efforts after an EMP.

Sec. 7. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,
March 26, 2019.

Number 2

Interpol reviews its rules for the international exchange of criminal data

A legal framework that allows police worldwide to share details on crimes and criminals effectively in line with international standards

Interpol has launched a review of its Rules on the Processing of Data (RPD) to ensure they continue to meet the needs of international police cooperation in a digital world.

The RPD are the only existing legal instrument with a global scope regulating the international exchange of criminal data.

The RPD enable 194 countries to share data via INTERPOL's Information System in line with international standards, including the rights to privacy and data protection.

The INTERPOL Working Group on the Processing of Information held its first meeting on 20 and 21 March in Lyon, France, to lay the groundwork for its review of the RPD over the coming years.

Delegates from 36 countries in Africa, the Americas, Asia and Europe took part in meeting along with legal experts and national practitioners in the area of international police cooperation.

With international policing practices and technologies evolving rapidly, the purpose of the review is to ensure the RPD meet countries' needs and keep pace with developments – such as big data technologies, open-source intelligence, the increasing interconnectivity of systems, and the use of data for crime prevention purposes such as screening of travellers – while ensuring individuals' rights and privacy are respected.

The current RPD were adopted by INTERPOL's member countries during the General Assembly meeting in 2011 and went into force the following year.

But INTERPOL has a long history in the area of data protection due to its role of coordinating the exchange of data through its police information systems. The review is part of a process of continuous reassessment of the Organization's regulations, policies and procedures.
During the meeting, the Working Group reviewed the current set of RPD and were briefed on strategic projects under development which could

potentially affect how INTERPOL and its member countries share and use data.

The Working Group will report on the progress of its review of the RPD at the INTERPOL General Assembly in October in Santiago, Chile.

More about Interpol's legal documents:
https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents

Number 3

DARPA Seeks to Make Scalable On-Chip Security Pervasive

Program to focus on addressing the economic and technical challenges associated with incorporating scalable defense mechanisms into chip designs

For the past decade, cybersecurity threats have moved from high in the software stack to progressively lower levels of the computational hierarchy, working their way towards the underlying hardware.

The rise of the Internet of Things (IoT) has driven the creation of a rapidly growing number of accessible devices and a multitude of complex chip designs needed to enable them.

With this rapid growth comes increased opportunity for economic and nation-state adversaries alike to shift their attention to chips that enable complex capabilities across commercial and defense applications.

The consequences of a hardware cyberattack are significant as a compromise could potentially impact not millions, but billions of devices.

Despite growing recognition of the issue, there are no common tools, methods, or solutions for chip-level security currently in wide use.

This is largely driven by the economic hurdles and technical trade-offs often associated with secure chip design.

Incorporating security into chips is a manual, expensive, and cumbersome task that requires significant time and a level of expertise that is not readily available in most chip and system companies.

The inclusion of security also often requires certain trade-offs with the typical design objectives, such as size, performance, and power dissipation.

Further, modern chip design methods are unforgiving – once a chip is designed, adding security after the fact or making changes to address newly discovered threats is nearly impossible.

“Today, it can take six to nine months to design a modern chip, and twice as long if you want to make that same design secure,” said Serge Leef, a program manager in DARPA’s Microsystems Technology Office (MTO).

"While large merchant semiconductor companies are investing in in-house personnel to manually incorporate security into their high-volume silicon, mid-size chip companies, system houses, and start-ups with small design teams who create lower volume chips lack the resources and economic drivers to support the necessary investment in scalable security mechanisms, leaving a majority of today's chips largely unprotected."

To ease the burden of developing secure chips, DARPA developed the Automatic Implementation of Secure Silicon (AISS) program. AISS aims to automate the process of incorporating scalable defense mechanisms into chip designs, while allowing designers to explore economics versus security trade-offs and maximize design productivity.

The objective of the program is to develop a design tool and IP ecosystem – which includes tool vendors, chip developers, IP licensers, and the open source community – that will allow security to be inexpensively incorporated into chip designs with minimal effort and expertise, ultimately making scalable on-chip security pervasive.

Leef continued, "The security, design, and economic objectives of a chip can vary based on its intended application. As an example, a chip design with extreme security requirements may have to accept certain tradeoffs. Achieving the required security level may cause the chip to become larger, consume more power, or deliver slower performance.

Depending on the application, some or all of these tradeoffs may be acceptable, but with today's manual processes it's hard to determine where tradeoffs can be made."

AISS seeks to create a novel, automated chip design flow that will allow the security mechanisms to scale consistently with the goals of the design.

The design flow will provide a means of rapidly evaluating architectural alternatives that best address the required design and security metrics, as well as varying cost models to optimize the economics versus security tradeoff.

The target AISS system – or system on chip (SoC) – will be automatically generated, integrated, and optimized to meet the objectives of the application and security intent.

These systems will consist of two partitions – an application specific processor partition and a security partition implementing the on-chip security features.

This approach is novel in that most systems today do not include a security partition due to its design complexity and cost of integration.

By bringing greater automation to the chip design process, the burden of security inclusion can be profoundly decreased.

While the threat landscape is ever evolving and expansive, AISS seeks to address four specific attack surfaces that are most relevant to digital ASICs and SoCs. These include side channel attacks, reverse engineering attacks, supply chain attacks, and malicious hardware attacks.

"Strategies for resisting threats vary widely in cost, complexity, and invasiveness.

As such, AISS will help designers assess which defense mechanisms are most appropriate based on the potential attack surface and the likelihood of a compromise," said Leef.

In addition to incorporating scalable defense mechanisms, AISS seeks to ensure that the IP blocks that make up the chip remain secure throughout the design process and are not compromised as they move through the ecosystem.

As such, the program will also aim to move forward provenance and integrity validation techniques for preexisting design components by advancing current methods or inventing novel technical approaches.

These techniques may include IP watermarking and threat detection to help validate the chip's integrity and IP provenance throughout its lifetime.

AISS is part of the second phase of DARPA's Electronics Resurgence Initiative (ERI) – a five-year, upwards of $1.5 billion investment in the future of domestic, U.S. government, and defense electronics systems.

Under ERI Phase II, DARPA is exploring the development of trusted electronics components, including the advancement of electronics that can enforce security and privacy protections.

AISS will help address this mission through its efforts to enable scalable on-chip security.

DARPA holds a Proposers Day on April 10, 2019 at the DARPA Conference Center, located at 675 North Randolph Street, Arlington, Virginia 22203, to provide more information about AISS and answer questions from potential proposers.

For details about the event, including registration requirements, please visit:
https://www.fbo.gov/index?s=opportunity&mode=form&id=6770487d820ee13f33af67b0980a7d73&tab=core&_cview=0

Additional information will be available in the forthcoming Broad Agency Announcement, which will be posted to www.fbo.gov

Number 4

Data exposed by banking app security flaws

Vulnerabilities have been found in the mobile applications of 30 financial service providers.

The report, by cyber security company Arxan, revealed that source code, back-end accesses and sensitive data are at risk after a researcher download various apps from the Google Play store.

The report:
https://www.arxan.com/resources/downloads/aite-research-financial-mobile-apps

The vulnerabilities noticed include insecure data storage, weak encryption and a lack of binary protections. The report has not named any of the apps in an effort to not increase additional risk, but it does highlight the importance of ensuring strong app development and security.

The NCSC has produced guidance discussing app development which can help organisations do more to help secure sensitive data.

The NCSC has created guidance for platform-specific application development and secure best practice for modern development teams at:
https://www.ncsc.gov.uk/collection/application-development

https://www.ncsc.gov.uk/collection/developers-collection

Number 5

Avoiding the Crack of Doom

New imaging technique reveals how mechanical damage begins at the molecular scale.

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

Just as a journey of 1,000 miles begins with a single step, the deformations and fractures that cause catastrophic failure in materials begin with a few molecules torn out of place. This in turn leads to a cascade of damage at increasingly larger scales, culminating in total mechanical breakdown.

That process is of urgent interest to researchers studying how to build high-strength composite materials for critical components ranging from airplane wings and wind-turbine blades to artificial knee joints.

Now scientists from the National Institute of Standards and Technology (NIST) and their colleagues have devised a way to observe the effects of strain at the single-molecule level by measuring how an applied force changes the three-dimensional alignment of molecules in the material.

The technique uses single-molecule, super-resolution optical microscopy, which can resolve objects in the range of 20 nanometers (billionths of a meter)—about one-tenth the size of what can be seen at the sharpest focus with a conventional optical microscope.

The new method examines a polymer doped with fluorescent molecules that emit light of one wavelength when they are illuminated with light of another wavelength. An image of the emitted light reveals not only a molecule's location, but also its orientation horizontally and vertically.

The super-resolution microscope, development of which won the 2014 Nobel Prize in Chemistry, has been widely employed for biomedical applications. "But we started wondering what you could do with it in the materials area," said NIST scientist J. Alexander Liddle.

"That is, how can we see what is happening at the molecular level at the very earliest stages of deformation or damage? If those mechanisms can be understood, researchers may be able to design better composite materials that can inhibit failure."

Composite materials are used throughout industry to increase strength and decrease weight. For example, half the material by weight in a Boeing 787 airframe is carbon fiber-reinforced plastic and other composites.

For many such materials, it is difficult to see the early onset of damage because there are no visible markers to track its effects.

To provide those markers in their experiment, the researchers used a very thin film of a polymer found in Lucite and Plexiglas that had been doped with thousands of fluorescent molecules. Initially, the polymer was unstressed, and the embedded fluorescent molecules were in completely random orientations in three dimensions.

Then the scientists applied force to the polymer, deforming it in a controlled specific direction. As the polymer was strained, the embedded fluorescent molecules were carried along with the deformation, losing their random orientation and lining up with the path of the damage.

That path was made visible by observing the pattern of emitted light from the embedded fluorescent molecules, which acted like a series of little flashlights pointing the way.

Prior to the experiment, the scientists used a mathematical model that predicted how light would look when emitted by molecules in different 3D alignments. When they illuminated the fluorescent molecules and made images of the emitted light, the results matched the model. After about 10,000 cycles of illumination, a telltale pattern emerged showing the extent of deformation.

“It’s sort of like a pointillist painting, where individual dots build up to form a shape,” Liddle said.

In addition to the technique’s clear relevance to the design of essential composite materials, there might also be applications in medicine.

“Let’s say you have a new bioimplant—for example, a knee replacement,” said Mitchell Wang, now at Northwestern University, who worked on the experiment while at NIST. “To make it biocompatible, it will likely be made of soft polymers, but you also want the device to have excellent mechanical properties. You want it to operate easily while also being stiff and tough. This technique could help inform design so the materials used have excellent mechanical strength.”

There are many avenues for future research. “This technique was a post-mortem study, in that we could view the damage in a material after it already happened,” Wang said. “The next step might be to learn how to perform this work in real time, to watch not only where the damage is happening, but when.”

Liddle's team is also developing an improved imaging technique. It involves making two simultaneous image sets—one on each side of the doped polymer. On one side, imaging is produced by the method described above. On the other, a separate lens gathers fluorescent light from the material and divides it into four different polarizations in individual channels. Because the polarization of the emitted light is affected by the orientation of the fluorescent molecules, "if you measure the ratios of the intensity in each channel, you can figure out which direction the molecule is pointing," Liddle said. "That would give us an independent measure of orientation."

In addition, the scientists hope to improve resolution by a factor of about five—allowing them to image areas as small as a few nanometers. This could be accomplished by increasing the brightness of the fluorescent molecules, perhaps by reducing their exposure to oxygen, which shuts off fluorescence.

Meanwhile, Liddle said, "it still amazes me that I can look at this little bright spot in a microscope and know within five or ten nanometers where it is and also know, within a few degrees, in which direction it's pointing."

In addition to NIST scientists, researchers at the University of Maryland NanoCenter contributed to the experiment and journal article.

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.