October 2019, cyber risk and compliance in Switzerland

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

Dear readers,

It is time to read the new semi-annual report (January – June 2019) of the Reporting and Analysis Centre for Information Assurance (MELANI), that addresses the most important cyberincidents of the first half of 2019, both in Switzerland and abroad.

According to MELANI, for more than two hours on 6 June 2019, a large proportion of European mobile phone traffic was diverted via China Telecom's infrastructure. The incident was caused by a BGP route leak at the Swiss data centre Safe Host, which accidentally redirected over 70,000 routes from the routing table to the Chinese internet service provider (ISP).

Route leaks lead to the diversion of data traffic via an unintended path, which can cause an overload or a black hole. As a result, data might not be transmitted and may be "dropped" (deleted) before it reaches its destination. Traffic analysis and eavesdropping are also possible.

Route leaks mostly arise from accidental misconfigurations. Instead of ignoring the BGP leak, China Telecom immediately took over the routes and redirected the traffic from a large number of European mobile phone networks to its own network. This went against filtering practices for the Border Gateway Protocol (BGP), which is used at ISP level to control the routing of data flows and prevent the spread of BGP leaks.

Among the European networks most affected were mobile phone operators in Switzerland (Swisscom), France (Bouygues Telecom, Numericable-SFR) and the Netherlands (KPN).

The redirection lasted for over two hours – a relatively long time according to experts. Global communications were also severely impaired; this was reflected in slow connectivity for users of the affected mobile networks.

Some servers were completely unavailable for users during this period. It is still unclear whether the redirection was deliberate, a technical fault or human error.

We can also read in the report that it is not just email accounts and credit card information that can be phished. Any online account is at risk. While a hacked Twitter account can be used to run a misinformation campaign discrediting the legitimate user, hacked Instagram profiles or YouTube accounts can also result in financial losses for the people affected.

The collected subscribers and followers are influencers' capital. If they lose control of their online presence, they have to start again and rebuild their community from scratch. Moreover, they are unable to upload any online content in the meantime, thereby losing a source of revenue.

Loss of control over an online account does not have repercussions just for famous people. More and more people live their lives at least partly on social media platforms. If they lose access to their Facebook account for example, they can indeed have problems maintaining their contacts, at least temporarily.

We can also read a very interesting analysis about ransomware. MELANI described the emergence of malware that blocks computers for blackmail purposes as early as eight years ago. That was one of the first versions of ransomware, which blocked the screen and displayed a message purportedly from the Federal Department of Justice and Police (FDJP).

The message claimed that a fine had to be paid because illegal material had allegedly been found on the computer. This type of malware was relatively harmless and could be removed in most cases by simply analysing the computer with an antivirus live CD.

Two years later, CryptoLocker was the first malware with an encryption function to hit the headlines. CryptoLocker encrypted files on both the hard disk and all locally connected media. A specific key was generated for each victim on a C2 server. This made data recovery more difficult than in the case of encryption Trojans that use a hard-coded and therefore extractable key.

CryptoLocker spread through infected email attachments (malspam) and drive-by infections (manipulated websites), or was downloaded via a dropper already installed on the device (independently executable program file). Propagation via droppers is currently widespread.

In 2018, the Taiwanese microchip manufacturer TSMC (Taiwan Semiconductor Manufacturing Company) experienced the loss of

productivity that can be caused by ransomware and persists until the systems affected by ransomware are restored. It had to stop production at several plants because of a WannaCry variant.

Ransomware attacks were generally not targeted until 2018. Only the SamSam group was known for targeted attacks. It used encryption Trojans largely against US organisations.

The emergence of Ryuk in 2018 marked the start of a form of ransomware apparently placed specifically within organisations from which high ransoms can be demanded.

Ryuk was discussed in the last semi-annual report and it has been very active also in 2019. Ransomware that is used in both a targeted and opportunistic manner likewise exists, e.g. GandCrab and Dharma.

To read the report:
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2019-1.html

---

According to Facebook, Libra is a “global currency and financial infrastructure”. The name Libra comes from the basic Roman measurement of weight.

Facebook wants to reach the 1.7 billion people around the world who do not have access to a bank account. But the effort is likely to run into regulatory hurdles and antitrust concerns.

Who will validate transactions on the Libra blockchain? The Libra Association, an independent, not-for-profit membership organization, headquartered in Geneva, Switzerland.

The association collaborates with the global community, and partners with policymakers to help further the Libra mission.

The Swiss authorities are following these developments very closely. In Switzerland, a project such as Libra can only be implemented with the authorisation of the Swiss Financial Market Supervisory Authority (FINMA).

On 11 September 2019, FINMA announced that the project, as currently planned, would be considered as a payment system and would require a corresponding authorisation. Such a system would automatically be subject to the Anti-Money Laundering Act.

Unlike the majority of cryptocurrencies, Libra is fully backed by a reserve of real assets. A basket of currencies and assets will be held in the Libra Reserve for every Libra that is created, building trust in its intrinsic value.

The Libra Blockchain is operated by a network of validator nodes. The evolution of the blockchain will be overseen by the Founding Members of the Libra Association, and each member will be responsible for running a validator node.

As the network grows and becomes more self-sustaining, the Libra Association will work to gradually transition to a permissionless mode of operation.

Read more at *number 1* below.

At *number 2* below you can read what Benoît Cœuré, Chair of the CPMI and Member of the Executive Board of the ECB said, at the hearing on "Digital currencies, focusing on Libra", at the Deutsche Bundestag in Berlin.

Is security the best friend, or the worst enemy of privacy?

Privacy is a human right, recognized in the UN Declaration of Human Rights. It relates to our freedom to control our personal information, and how it's used.

There is no privacy without security. Security implements privacy's choices, it is the interface layer between information and privacy.

Some people regard privacy and security as pretty much the same thing. Others believe that security is the worst enemy of privacy.

Carl Jung believed that the most intense conflicts, if overcome, leave behind a sense of security and calm that is not easily disturbed. It is just these intense conflicts and their conflagration which are needed to produce valuable and lasting results.

Cybersecurity risk and privacy risk are related but distinct concepts. Risk is defined in NIST SP 800-37 Revision 2 as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of:

(i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence."

For cybersecurity, risk is about threats—the exploitation of vulnerabilities by threat actors to compromise device or data confidentiality, integrity, or availability.

For privacy, risk is about problematic data actions—operations that process personally identifiable information (PII) through the information lifecycle to meet mission or business needs of an organization or "authorized" PII processing and, as a side effect, cause individuals to experience some type of problem(s).

Privacy and cybersecurity risk overlap with respect to concerns about the cybersecurity of PII, but there are also privacy concerns without implications for cybersecurity, and cybersecurity concerns without implications for privacy.

IoT devices generally face the same types of cybersecurity and privacy risks as conventional IT devices, though the prevalence and severity of such risks often differ.

For example, data security risks are almost always a significant concern for conventional IT devices, but for some IoT devices, there may not be data security risks because they do not have any data that needs protection.

Read more at number 5 below.

Edgar Allan Poe believed that *beauty* of whatever kind, in its supreme development, invariably excites the sensitive soul to tears. Saint Augustine has said that repentant tears wash out the stain of guilt.

Supervisors around the world have washed out the stain of guilt that followed the crisis of 2007, but perhaps they feel like crying again, as financial stress testing has become a *beauty contest,* according to Andrea Enria.

The presentation of Andrea Enria, Chair of the Supervisory Board of the ECB with title "The future of stress testing – realism, relevance and resources", is great. He said:

"But the realism of the exercise is also challenged because it easily turns into a "beauty contest": banks direct their efforts to "model the stress away" in order to look good to supervisors and investors.

And the experience from the first rounds of European stress tests shows that banks indeed often try to compensate losses in the adverse scenario. They do so by either being overly optimistic when estimating their income

in the adverse scenario or by being very positive on what management can achieve in turbulent market conditions.

We also see banks conspiring to game stress tests, often with the help of external advisers. Data are collected from banks ahead of their submission to supervisors, and each bank is informed of its position vis-à-vis its peers.

This helps them to align before and during the exercise in order to collectively adjust the results and minimise the impact of the stress scenario. We see this, we don't like it, and we will not tolerate it."

He continued:

"Imagine we decided to relax constraints in the bottom-up approach. Banks would be free to depart from a common methodology and scenario to better reflect their individual business models and risk profiles. The results of the stress test would become more realistic and more relevant for banks, which is good.

However, supervisors would have a hard time using the results of such an exercise to determine capital buffers in a consistent way across banks. They would need to invest more time and energy in quality assurance, which would require additional resources.

So, what should we do about it? Well, there are voices arguing that supervisors should focus more on top-down stress tests, as is done in the United States. Thus, they would run the exercise with their own models and fully control the consistency of the results.

But then, much less information would be provided to the markets. After all, banks would not accept the publication of very granular risk parameters which would not reflect their own risk management practices.

I think that the root of the problem lies in the fact that we are trying to do too much with too little. If we aim to achieve several goals, some of which conflict with each other, and if we aim to serve different customers, the stress test is bound to disappoint all of them."

I liked his introduction to financial stress testing:

"In 1628, the Vasa – the pride of the Swedish navy – was the most powerful warship in the Baltics. Until she sank about half an hour into her maiden voyage, that is. So, what happened? Well, nothing special when it comes to sailing ships: the wind simply picked up.

The problem was that the Vasa's design was rather unstable. She had been

built for the shallow waters around Stockholm, so not too much of the ship was below the waterline and a lot of weight was concentrated in her upper structures.

Thus, when the wind picked up, it pushed the ship so far over on its port side that water poured in through open gunports. And that was the end of the Vasa – and a huge embarrassment for the King of Sweden, Gustavus Adolphus.

Now, why am I telling you the story of the Vasa? In my view, it shows how beneficial it is to spend a moment or two thinking about what might happen if the wind picks up.

This is true when it comes to building ships and, in a sense, it is also true when it comes to managing banks. How will lenders fare in a storm? Are they stable enough to weather a storm? Or do they need additional weight below the waterline, in the form of more capital.

This idea sounds straightforward, doesn't it? Yet, it is only recently that stress tests for banks have entered the picture. It was the IMF that started such exercises as part of its regular Financial Sector Assessment Programs. But it took another 20 years before stress tests would become a key tool for banking supervisors.

In 2009, the United States used stress tests as a means to fight the financial crisis; Europe followed suit in 2010. Since then, stress tests have become a key instrument in the supervisory toolbox.

So, let us take a closer look at the evolution of stress testing and its objectives, and how it might need to be adapted in the future."

Read more at number 12 below. Welcome to our monthly newsletter.

Best regards,

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

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 14)

Update on the Libra project

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

On 18 June 2019, Facebook announced the creation of a new cryptocurrency, Libra, managed by a Geneva-based association, the Libra Association.

Number 2 (Page 16)

Introductory remarks to the Committee on the Digital Agenda of the Deutscher Bundestag

Benoît Cœuré, Chair of the CPMI and Member of the Executive Board of the ECB, at the hearing on the topic of "Digital currencies, focusing on Libra", Deutscher Bundestag, Berlin.

“The traditional bank-based payments ecosystem is being disrupted from below by tech start-ups and from above by well-established big techs - firms that have a large digital footprint but whose core business models have so far been confined to non-financial activities.”

Number 3 (Page 19)

National Cyber Security Strategies - Interactive Map

enisa
European Network and Information Security Agency

ENISA is supporting the EU Member States since 2012 to develop, implement and evaluate their National Cyber Security Strategies (NCSS). Since 2017, all EU Member States have published their own NCSS.

Number 4 (Page 20)

New REvil ransomware attributed to GandCrab Developers

National Cyber Security Centre

Back in May this year, the developers behind GandCrab Ransomware as a Service (RaaS) announced their "retirement", after claims they profited more than $2bn since January 2018. But this week, security researchers at Secureworks say they have discovered links between the thought-to-be-disbanded group and a strain of ransomware dubbed REvil, or Sodinokibi.

Number 5 (Page 21)

Before Connecting an IoT Device, Check Out a New NIST Report for Cybersecurity Advice

Revisiting a very important paper released during the summer. If you have not read it, you can find it below.

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

Seemingly every appliance we use comes in a version that can be connected to a computer network. But each gizmo we add brings another risk to our security and privacy.

Number 6 (Page 24)

Soldiers should safeguard against suspicious tweets

U.S.ARMY

The tweets surface innocently in Twitter feeds, often passing as legit news or normal social media posts. Often, Soldiers may not even know they have been fed disinformation.

Number 7 (Page 27)

Acting Secretary McAleenan at the CISA Cyber Summit

Homeland Security

"The expertise and years of experience that you bring to the table, and the way you work with partners and stakeholders in and out of government, make you a tremendous asset to the agency and the Department of Homeland Security mission.

Also, thank you to Secretary Esper for joining the Summit this afternoon, having our two Departments closely aligned in this effort is essential."

Number 8 (Page 33)

Extending free Windows 7 security updates to voting systems

Tom Burt, Corporate Vice President, Customer Security & Trust

Microsoft

Today, as part of Microsoft's Defending Democracy Program, we are announcing that we will provide free security updates for federally certified voting systems running Windows 7 through the 2020 elections, even after Microsoft ends Windows 7 support.

Number 9 (Page 36)

DEPARTMENT OF HOMELAND SECURITY STRATEGIC FRAMEWORK FOR COUNTERING TERRORISM AND TARGETED VIOLENCE

Homeland Security

The United States faces an increasingly complex, and evolving, threat of terrorism and targeted violence. As was the case sixteen years ago, at the U.S. Department of Homeland Security's founding, foreign terrorist organizations remain intent on striking the Homeland, whether through directed attacks or by inspiring susceptible individuals in the United States.

Number 10 (Page 39)

Scripting Engine Memory Corruption Vulnerability

Microsoft

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

Number 11 (Page 40)

Reinventing the Network Stack for Compute-Intensive Applications

DARPA seeks to create new networking approaches to accelerate distributed application performance by 100x

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Today, network interface hardware is hampering data ingest from the network to processing hardware. Additional factors, such as limitations in server memory technologies, memory copying, poor application design, and competition for shared resources, has resulted in network subsystems that are creating a bottleneck within the network stack and are throttling application throughput.

Number 12 (Page 43)

The future of stress testing – realism, relevance and resources

Keynote speech by Andrea Enria, Chair of the Supervisory Board of the ECB, at the European Systemic Risk Board (ESRB) Annual Conference

In 1628, the Vasa – the pride of the Swedish navy – was the most powerful warship in the Baltics. Until she sank about half an hour into her maiden voyage, that is. So what happened? Well, nothing special when it comes to sailing ships: the wind simply picked up.

Number 13 (Page 51)

European Cybersecurity Month 2019 is launched

October marks the kick-off of the European Cybersecurity Month (ECSM), coordinated by the European Union Agency for Cybersecurity (ENISA), the European Commission and supported by the Member States.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

This campaign will focus on expanding awareness about cybersecurity to citizens across Europe.

Number 14 (Page 54)

Espionage

CPNI
Centre for the Protection of National Infrastructure

The potential impact of successful State-sponsored espionage against the UK is both wide reaching and significant. The threat of espionage (spying) did not end with the collapse of Soviet communism in the early 1990s.

Espionage against UK interests still continues and is potentially very damaging. A number of foreign intelligence services (FIS) seek to gather intelligence on a broad range of subjects, including foreign policy, defence, financial, technological, industrial and commercial interests.

Number 15 (Page 60)

Revisiting an important paper

Kaleidoscope on the Internet of Toys

Safety, security, privacy and societal insights

Stéphane Chaudron, Rosanna Di Gioia, Monica Gemo, Donell Holloway, Jackie Marsh, Giovanna Mascheroni, Jochen Peter, Dylan Yamada-Rice

This paper gives an insight into safety, security, privacy and societal questions emerging from the rise of the Internet of Toys.

These are Internet Connected Toys that constitute, along with the wave of other domestic connected objects, the Internet of Things, which has increased the ubiquity of the ICT within our everyday lives, bringing technology more than ever closer to ourselves and our children.

Number 1

Update on the Libra project

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

On 18 June 2019, Facebook announced the creation of a new cryptocurrency, Libra, managed by a Geneva-based association, the Libra Association.

Its members include major multinationals and non-governmental organisations. One of the association's central missions is to facilitate financial inclusion around the world. More generally, a project of this kind could accelerate payment traffic and reduce the costs involved.

Libra is based on blockchain technology and is one of the cryptocurrencies described as "stable coins": it is designed to limit its volatility as it is linked to a basket of currencies.

With regard to the Swiss authorities, they are following developments very closely. They are in close contact with the project initiators and are working in a coordinated manner both nationally and internationally.

Representatives of the State Secretariat for International Finance (SIF) and other Swiss authorities met with a US parliamentary delegation on 23 August 2019 in Bern to discuss, among other things, the Libra project.

On 10 September 2019, SIF also received US Under Secretary of the Treasury Sigal Mandelker.

The talks focused on the fight against money laundering and the financing of terrorism as well as on cryptocurrencies in general.

In Switzerland, a project such as Libra can only be implemented with the authorisation of the Swiss Financial Market Supervisory Authority (FINMA).

On 11 September 2019, FINMA announced that the project, as currently planned, would be considered as a payment system and would require a corresponding authorisation. Such a system would automatically be subject to the Anti-Money Laundering Act.

This would ensure that the highest international standards in the fight against money laundering are met.

You may visit:

https://finma.ch/en/news/2019/09/20190911-mm-stable-coins/

With regard to Libra, SIF has adopted the following position:

The choice of Geneva for the organisation's headquarters is a positive sign for Switzerland as an open and innovative economic and financial centre. Such innovative projects involve opportunities and risks that need to be proactively addressed.

The Federal Council attaches great importance to the fight against money laundering and other crimes. Switzerland's anti-money laundering and anti-terrorist financing system is technology-neutral and applies to virtual assets.

Given the global scope of the Libra project, coordination at the international level is essential. The Swiss authorities are seeking dialogue with foreign authorities and actively participating in the analysis of "stable coins" by relevant bodies, such as the Financial Stability Board.

To learn more: https://finma.ch/en/news/2019/09/20190911-mm-stable-coins/

Number 2

Introductory remarks to the Committee on the Digital Agenda of the Deutscher Bundestag

Benoît Cœuré, Chair of the CPMI and Member of the Executive Board of the ECB, at the hearing on the topic of "Digital currencies, focusing on Libra", Deutscher Bundestag, Berlin.

It is my pleasure to join you today to discuss the topic of digital currencies, focusing on Libra.

Payment systems have always been at the heart of finance but they have attracted heightened interest recently. Innovation is rampant, and new proposed solutions are testimony to the pervasive speed and scope of recent technological advances and their implications for our everyday lives.

The traditional bank-based payments ecosystem is being disrupted from below by tech start-ups and from above by well-established big techs - firms that have a large digital footprint but whose core business models have so far been confined to non-financial activities.

Despite progressive changes and improvements, the global payments system still faces two major challenges: access and cross-border retail payments. Globally, 1.7 billion adults remain outside the payments system, with no access to basic services, even though 1.1 billion of them have a mobile phone and one in four also have internet access (World Bank, 2018).

Payment accounts and e-wallets are gateways to additional financial services, such as credit and insurance, so a lack of access to them hampers financial inclusion more generally (Cœuré, 2019a).

Cross-border retail payments, on the other hand, are vital for global commerce and for migrants who send remittances home. Yet they are generally slower, more expensive and more opaque than domestic payments (CPMI, 2018). Sadly, the cost of cross-border remittances imposes the greatest burden on those who are least able to bear it.

A number of so-called "stablecoin" initiatives, backed by large technology or financial firms and built on blockchain technology, are designed to address at least one and, in the case of Libra, both of these failings.

Although private digital forms of money have been around for decades, these new initiatives have access to large networks of existing users and customers, which suggests that they could be the first to have a truly global footprint.

These initiatives raise formidable challenges across a broad range of policy domains. Of particular concern are the risks related to anti-money laundering and countering the financing of terrorism, as well as consumer and data protection, cyber resilience, fair competition and tax compliance.

Partly in response to these concerns, a working group has been mandated by G7 finance ministers and central bank governors to examine global "stablecoins" in more detail.

The group is expected to provide policy recommendations by the time of the IMF-World Bank Annual Meetings in October this year. The Financial Stability Board has also started looking into the regulatory implications of these initiatives and will report to G20 ministers and governors.

Depending on the jurisdiction, the risks that have been identified so far could be addressed by existing regulatory and supervisory regimes, with the fundamental approach being that regulatory answers should be internationally consistent and the principle of "same business, same risks, same rules" should be rigorously applied.

Some aspects may require novel approaches, however. In the European Union, for example, it is the role of the European Commission, together with Member States, the ECB and relevant authorities, to review whether the current framework is fit for purpose.

Significant work and further engagement with the public and authorities will be required before we can expect any potential global "stablecoin" arrangements to be approved by the relevant authorities (BIS, 2019).

"Stablecoin" initiatives also need to demonstrate a sound legal basis. The global nature of these initiatives means that potential conflicts of laws across jurisdictions need to be addressed. Ambiguity can make "stablecoin" arrangements vulnerable to a loss of confidence - an unacceptable risk in a global payments system with potentially systemic importance.
Given that many of the "stablecoins" target retail users, it is critical that the rights of coin holders and the obligations of issuers be clearly communicated and legally precise.

"Stablecoins" also rely on new entrants to the market operating nascent technology, which can potentially deliver new benefits to consumers but is largely untested in a real-world environment and on the scale required to run a global payments system. They are also being governed in new ways, using a distributed model. Consequently, their governance structures need to be well understood.

If "stablecoins" become widely used, they could also give rise to issues related to monetary policy transmission and financial stability (Cœuré, 2019b).

Where a "stablecoin" acts as a substitute for fiat currency, there may be the risk of the monetary sovereignty of countries being infringed. Furthermore, the transmission of monetary policy could be affected if "stablecoin"-denominated credit or overdraft extensions are provided.

Finally, financial stability will be affected if the assets underlying "stablecoin" arrangements are not managed in a sufficiently safe and prudent manner to ensure that coin holders have confidence that their coins are redeemable at par, in good times and in bad.

All things considered, Libra has undoubtedly been a wakeup call for central banks and policymakers. Global "stablecoin" initiatives are the natural result of rapid technological progress, globalisation and shifting consumer preferences.

The demand for fast, reliable and cheap cross-border payments is bound to grow further in coming years. Policymakers and central banks should respond to these challenges.

Thank you.

Note: The views expressed are not necessarily those of the CPMI, the Bank for International Settlements or the ECB.

Number 3

National Cyber Security Strategies - Interactive Map

ENISA is supporting the EU Member States since 2012 to develop, implement and evaluate their National Cyber Security Strategies (NCSS). Since 2017, all EU Member States have published their own NCSS.

The ENISA NCSS Interactive Map lists all the documents of National Cyber Security Strategies in the EU together with their strategic objectives and good examples of implementation. ENISA's goal is to create an info-hub with information provided by the Member States on their efforts to enhance national cybersecurity.

You may visit:
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Number 4

New REvil ransomware attributed to GandCrab Developers

Back in May this year, the developers behind GandCrab Ransomware as a Service (RaaS) announced their "retirement", after claims they profited more than $2bn since January 2018.

But this week, security researchers at Secureworks say they have discovered links between the thought-to-be-disbanded group and a strain of ransomware dubbed REvil, or Sodinokibi.

Researchers have noted "numerous characteristics" that would suggest the same developers were involved in the production of both GandCrab and REvil, including "nearly identical" coding.

Ransomware attacks are continuing to rise in number and sophistication. The NCSC has previously published guidance on how to protect your organisation from ransomware and, more recently, advice on how to effectively detect, respond to and resolve cyber incidents.

You may visit: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

https://www.ncsc.gov.uk/collection/incident-management

We've also produced a step-by-step guide on how individuals can recover an infected device at https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take

Number 5

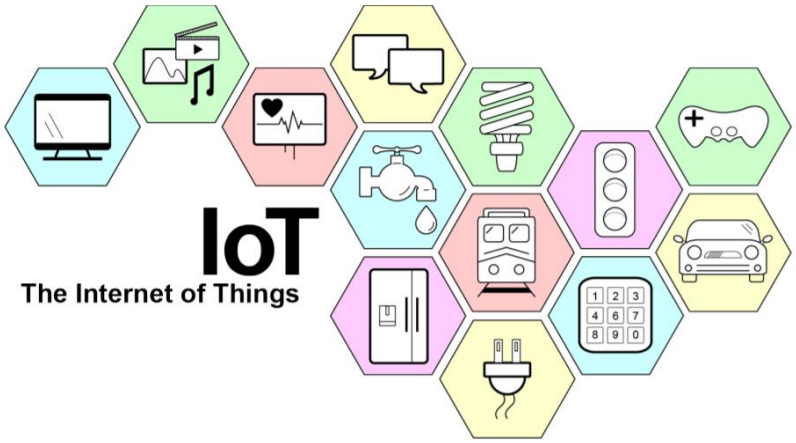
Before Connecting an IoT Device, Check Out a New NIST Report for Cybersecurity Advice

Revisiting a very important paper released during the summer. If you have not read it, you can find it below.

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

Seemingly every appliance we use comes in a version that can be connected to a computer network. But each gizmo we add brings another risk to our security and privacy.

So before linking your office's new printer or coffee maker to the internet of things (IoT), have a look at an informational report from the National Institute of Standards and Technology (NIST) outlining these risks and some considerations for mitigating them.



Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228) is the first in a planned series of documents NIST is developing to help IoT users protect themselves, their data and their networks from potential compromise.

Developed by the NIST Cybersecurity for IoT Program over more than two years of workshop discussions and interaction with the public, NISTIR 8228 is primarily aimed at federal agencies and other big organizations that are incorporating IoT devices into their workplace — organizations that may already be thinking about cybersecurity on a large-scale, enterprise level.

"The report is mainly for any organization that is thinking about security on the level of the NIST Cybersecurity Framework," said Mike Fagan, a NIST computer scientist and one of the authors of the report.

"It's targeted at the mode of thinking that an organization would have — more resources, more people, more ability, but also more risk of attack because of all those things. It's bad when a single house is attacked, but if a million bank account passwords are stolen, that has a much larger impact."

Larger organizations may already be using the Cybersecurity Framework and NIST SP 800-53 Rev. 5, two NIST resources that offer guidance for mitigating risk to information systems and the activities that involve them. NISTIR 8228 takes the security and privacy focus from these other documents and considers it in the context of IoT products, from thermostats to voice-operated devices, which may not have traditional interfaces such as a keyboard.

"An IoT device might even have no interface at all, or have no way to install security software," Fagan said. "But it still might connect to your network and be visible electronically to an enemy looking for a potential way in.

It's this kind of incongruency with expectations that we want to help an organization think through before they bring IoT devices onto their network."

The report is a companion document to the Cybersecurity Framework and SP 800-53 Rev. 5. However, NISTIR 8228 offers only advice; none of its contents are requirements under the Federal Information Security Management Act (FISMA).

After distinguishing IoT devices from conventional computers and outlining the type of risks they carry, the authors suggest three high-level risk mitigation goals:

- Protect device security, i.e., prevent an IoT device from being used to conduct attacks;

- Protect security of data, including personally identifiable information; and

- Protect individuals' privacy.

"IoT is still an emerging field," Fagan said. "Some challenges may vanish as the technology becomes more powerful. For now, our goal is awareness."

Specifics are around the corner, though. In the near future, NIST plans to release a core baseline document that aims to identify fundamental cybersecurity capabilities that IoT devices can include. The document will have all IoT devices in mind, including those for individual users and home networks.

"We plan to release a draft of the baseline document for public comment in July, and then we will hold a workshop on August 13 where we will gather feedback," Fagan said. "We'd like to help all IoT users be aware of the risks to their security and privacy and help them approach those risks with open eyes."

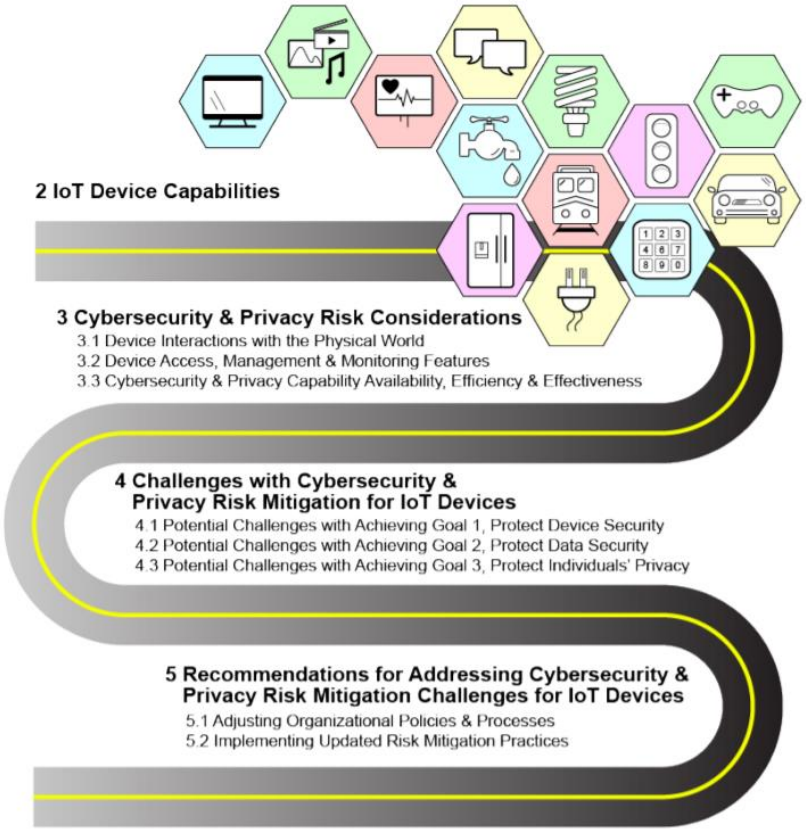


Figure 1: Topics Covered in This Publication

To read more:
https://csrc.nist.gov/publications/detail/nistir/8228/final

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

Number 6

Soldiers should safeguard against suspicious tweets

The tweets surface innocently in Twitter feeds, often passing as legit news or normal social media posts.

Often, Soldiers may not even know they have been fed disinformation. According to a Clemson University academic, Russian hackers apply disinformation tactics to spread divisive, political tweets to Soldiers and other Americans. Army leaders discussed the threat at an Association of the U.S. Army "Hot Topics" forum Monday on cyber and networks.

Army leaders want Soldiers to be aware of disinformation tweets and posts created by foreign agents, especially when perusing social media. Disinformation agents could be using duplicate or fraudulent accounts of military members and often pose as senior U.S. military leaders, according to experts.

Darren Linvill, communications professor at Clemson University, has sifted through millions of tweets by Russian, Chinese and Saudi accounts and said that Twitter ranks as the online tool foreign agents most frequently use to spread misinformation. Russian users in particular have grown skilled in the use of Twitter and can quickly gain followers, he said.

Linvill broke online disinformation in Twitter into two categories: offensive and defensive. While the majority of foreign agents use "defensive" tweets, often in response to negative news, the Russians primarily use "offensive" tweets to spread dissidence through the social media platform.

"They have decided it's in their best interest to mess with us, pushing the political conversations in this country to polarizing different directions," Linvill said. "It's fundamentally an offensive operation."

Col. Gittipong Paruchabutr, director of information operations, U.S. Army Special Operations Command, said the Army has taught identity management to help Soldiers protect themselves against fraudulent use of social media. He added the Army assigned specialized teams to monitor such activities. Linvill said the offensive tweets have not personally attacked any U.S. Soldiers but Russians have used tweets to attack Ukrainian military members.

Paruchabutr said Soldiers should remain wary of polarizing tweets.

"It's about awareness that these activities are happening at the Soldier level and more importantly how it affects the Soldier's families," he said. "We have to be cognizant that, even if it's not attacking Soldier X or unit Y, these accounts, these online activities are targeting general Americans and it further polarizes our divisions."

COUNTERING THE THREATS

To help combat disinformation and other cyber threats -- such as online hackers and cyberattacks -- the Army has been developing and fielding next-generation electronic warfare systems.

The Army has developed "I2CEWS" or intel, information, cyber, electronic warfare and space elements nested inside the Multi-Domain Task Force.

"That's the element that's intended to penetrate A2/AD [anti-access / area-denial technology] formations and disintegrate formations," said Brig. Gen. Richard Angle, deputy commanding general of operations, Army Cyber Command. "It's up. It's running. It's being exercised ... and it's doing some great work."

A2/AD refers to technology used by near-peer adversaries designed to deny freedom of movement to potential enemies, including U.S. forces.

The Army has also established the advanced tactical technology course, taught at Fort Bragg's John F. Kennedy Special Warfare Center and School. The course trains Soldiers to defend, inform and exploit within the digital terrain through advanced knowledge of computer systems and social media platforms.

The 30-day course trains Soldiers on basic digital force protection, targeting and sub-net target isolation and analysis. Soldiers who meet the prerequisites are eligible to take the course.

"There is a sense of urgency and need for speed," Angle said. "Because as we develop these concepts, we have to recognize this threat is here today, it's not theoretical."

To help advance the ability to counter against cyberattacks, Soldiers take part in cyber-themed exercises including a Cyber Blitz at Fort Dix, New Jersey. Cyber Blitz is an annual exercise co-hosted by the Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance and Reconnaissance -- or C5ISR -- Center, at Aberdeen Proving Ground, Maryland, and the U.S. Army Cyber Center of Excellence at Fort Gordon,

Georgia. It teaches Soldiers how to employ cyberspace electromagnetic activities across all aspects of Army doctrine, training and education.

U.S. Army Special Operations Command units now participate in combat training center rotations and warfighter exercises, where they are supported by Army Cyber formations in replicating near-peer information environments against U.S. internal formations, Paruchabutr said.

"This is an absolutely critical capability on how we look at ourselves," he said. "How do our formations look before we go into a combat training center because we know that the competition is here now; our enemies are looking at our formations across the United States."

In order to compete successfully in a congested and contested environment, Angle said that the Army must increase leader education and training development at all levels to change the mindset and the culture.

He added that exercises need to be revised with greater "depth" to fully synchronize the Army's new cyber capabilities to gain and maintain an advantage against adversaries.

"And that needs to be exercised in both conflict and competition scenarios and we have to force ourselves to operate it in congested and contested environments," he said.

Number 7

Acting Secretary McAleenan at the CISA Cyber Summit

Homeland Security

Thank you, Director Krebs, for the kind introduction, and thank you for your leadership of our nation's newest government agency, the Cybersecurity and Infrastructure Security Agency.

The expertise and years of experience that you bring to the table, and the way you work with partners and stakeholders in and out of government, make you a tremendous asset to the agency and the Department of Homeland Security mission.

Also, thank you to Secretary Esper for joining the Summit this afternoon, having our two Departments closely aligned in this effort is essential.

We appreciate the Secretary's and General Paul Nakasone's leadership and commitment to our nation's diverse and essential cyber missions.

I am excited to join you at the end of Day 2 for CISA's 2nd Annual National Cybersecurity Summit among our partners in the interagency, industry, and private sector.

I am fortunate to have made it here via Laredo, San Diego, and New York since Tuesday, but I thought it would be important to join this group to talk about DHS and the Administration's cybersecurity efforts.

I'd like to thank all of you in the audience, watching the live-stream, and of course – CISA and DHS professionals – for the work you do to protect our country and its critical infrastructure. Threats to the homeland and our national security are persistent and pervasive.

As our world becomes increasingly networked, it has acute impacts on homeland security—resulting in a landscape where a siloed sector and asset-specific approach is insufficient to defend against the threats we face.

Nation-state adversaries work to identify and exploit technological points of leverage for maximum injury to American critical infrastructure.

Bad actors are using cyber as a means to disrupt and sow discord in our democratic institutions, even going so far as to incite violence in our nation's disaffected against their fellow Americans.

And across industries and asset sectors, cyber attacks for financial gain are ever more common, requiring that we practice cyber hygiene at every level.

That is where CISA comes in.

Congress made the important move last year of recognizing the need in the U.S. Government for heightened efforts in cybersecurity, standing up CISA in November 2018. CISA has the unique and critical mission within the U.S. Government of protecting the Nation's critical infrastructure from physical and cyber threats.

But CISA's mission success will not be possible without extensive collaboration across government, industry and academia, as evidenced in this room today.

It is only by leveraging all available resources – federal, state, and local governments, business, industry, academia and international partners – that we will be able to counter and mitigate threats to our critical infrastructure.

This summit provides us the opportunity to capitalize on our initiatives, explore new ideas, and unify our defenses against state and non-state, criminal, and domestic threats to our nation's cyber infrastructure.

Our nation is stronger when we counter and mitigate threats with a collective defense.

In closing out today, I want to provide you with a high-level perspective on the importance of what you have discussed here over the past two days, and will be finishing out tomorrow. CISA's mission and functions, as well as its partners' roles in cyber and infrastructure security, are vitally important to our national security.

In less than a year, CISA has made noteworthy progress in their mission field as the Nation's risk advisor – and they are gearing up to address increasingly dynamic threats in 2020.

As the government agency responsible for building national resilience, the interagency community looks to CISA for strategic leadership in this arena. In August, CISA released its Strategic Intent to serve as the guide for CISA's leadership, workforce, and partners across government, industry, and academia in our unified effort of Defending Today and Securing Tomorrow.

Its five operational areas of focus, outlined by Director Krebs, reflect the top priorities of CISA in its mission space. These focus areas are:

- China, Supply Chain and 5G wireless;
- Soft Target Security;
- Government Network Protection;
- Industrial Control Systems; and
- Election Security.

DHS is committed to providing CISA with the support it needs to address these imminent risks facing our nation's critical infrastructure. CISA has already done a great deal in its short history to build our national resilience in these areas… and I want to briefly highlight a few of their efforts.

In December of 2018, CISA announced that malicious actors working on behalf of the Chinese government had been carrying out a campaign of cyberattacks that targeted Managed Service Providers (MSP), fitting a trend of threat actors targeting supply chains and trusted relationships. These attacks not only targeted MSPs, but also their customers on every continent across sectors, from finance and banking, to automotive, to telecommunications.

In response, CISA hosted a series of high-profile, public-facing webinars that addressed public concerns about Chinese malicious cyber activity that targeted MSPs. These substantive and informative webinars helped organizations manage their own risk, allowing us to take a step towards both defending today and securing tomorrow.

Furthermore, in January, CISA issued an emergency directive to all civilian federal executive branch agencies, requiring immediate actions to protect federal information and information systems against recent Domain Name System (DNS) infrastructure hijacking and tampering activities.

CISA analysts observed attackers using compromised credentials to redirect and intercept web and mail traffic across multiple federal agency servers and networks. CISA's leadership made it clear that a decisive, urgent response was needed as the actions posed a significant opportunity for harm to our critical infrastructure. Their directive ensured that federal agencies were prepared and not vulnerable to DNS infrastructure hijacking and tampering.

These are two examples among many of CISA's significant work in the last ten months. But—I'd like to hone in on one area of their ongoing work in particular that is highlighted by the Strategic Intent: election security.

It is DHS's mission to safeguard the American people, our homeland, and our values – and there are perhaps few more treasured national values than free and fair elections.

As 2016 showed, adversaries, including Russia, are targeting our democracy, seeking to disrupt the institution and turn Americans against one another. That election was a wake-up call for our nation's election security mission. And we've learned that greater collective vigilance is needed.

State and local election officials are standing on the front lines of a renewed conflict, defending our nation's election systems, against nation-states and criminal actors alike. I am committed to ensuring that that they do not stand alone.

I'm proud of the work that CISA has led, partnering with state and local election officials and the private sector to ensure that they are supported with assessments, resources, training, penetration testing, intelligence and analysis ahead of the 2020 elections.

CISA has taken an aggressive lead with "#Protect2020," a campaign to increase our partnership with state and local election officials, engage campaigns and political organizations, and enhance the general public's resilience against foreign disinformation campaigns designed to undermine our confidence in the elections process.

By being here, you have a unique opportunity to be a part of the conversation and the solution through the Protect 2020 breakout sessions. From the state of election cybersecurity from the front lines, to delving into the complexities of disinformation, together we can better understand the challenges. Together we can build in better defense and resilience.

CISA is currently working with all 50 states and thousands of local election jurisdictions to ensure the integrity, confidentiality, and availability of critical election systems and information.

We've hosted extensive tabletop exercises, ranging from the Tabletop the Vote series that rivals the scale of a federal election to exercises hosted down at the county and jurisdiction level.

We've developed and deployed new cybersecurity assessments to safeguard voting machines and secure e-pollbooks and election networks. We've developed guidance documents and established the Elections Infrastructure Information Sharing and Analysis Center.

And we host a security operations center during elections where we are in constant contact with election officials, partisan organizations, social media platforms, and election vendors.

It's this type of support that gives us confidence in the security measures being undertaken—confidence in 2018 and confidence going into 2020.

While we will continue our support to election officials we are also growing our support to the American public. We know that foreign actors will continue to attempt to undermine our democracy through disinformation campaigns.

DHS is working with federal partners, industry, and non-government organizations to build national resilience to foreign influence through education and awareness.

Some of you may have seen our pineapple product that challenged Americans to learn about disinformation campaigns while sharing their views on whether pineapple belongs on pizza… While I hesitate to take up an issue on the wrong side of Dwayne Johnson—the Rock—let me be clear on my stance on this—it absolutely does not.

DHS will continue to support the steps that CISA is taking to achieve their election security goals for 2020. At the end of the day, these goals should be collectively shared by us all – an attack on our nation's free and fair elections is an attack on our democracy itself, and on the American way of life.

In closing, I want to reemphasize how important CISA's efforts are within the Department of Homeland Security's mission. We value our partners across sectors who are working with us to defend our Nation's critical infrastructure.

Because neither any level of government, industry, the private sector, or individuals alone can effectively defend against all threats.

Instead, we must leverage the spectrum of resources available through CISA, industry sectors, and academia to reach our collective goals.

I join CISA in calling for your continued vigilance and efforts in the cyber arena.

If an organization hasn't invested in cybersecurity resources due to a lack of awareness, then let's work together to close that awareness gap and partner together. You will see measurable results from partnering with CISA.

And if an organization has mature cybersecurity protections, then I'd encourage them to assist with less mature organizations in their sectors and supply chains, to improve the cyber hygiene around them.

Cybersecurity is homeland security – and I want to thank you, again, for the opportunity to join you today. DHS is grateful for your continued work and collaboration in protecting the Homeland.

Number 8

Extending free Windows 7 security updates to voting systems

Tom Burt, Corporate Vice President, Customer Security & Trust

Microsoft

Today, as part of Microsoft's Defending Democracy Program, we are announcing that we will provide free security updates for federally certified voting systems running Windows 7 through the 2020 elections, even after Microsoft ends Windows 7 support.

I would like to share more on why we help customers move away from older operating systems and why we're making this unusual exception.

The Microsoft's Defending Democracy Program:
https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program/

We launched Windows 7 in 2009, the same year the Palm Pre launched, Twitter took off, mobile phone navigation was just coming to market, and floppy disks were still selling by the millions. Software built for that era cannot provide the same level of security as a modern operating system like Windows 10.

When we released Windows 7, we committed to supporting it for 10 years, and we've honored that commitment.

We've also reminded customers about this along the way including, most recently, in January and again in March.

This process is similar to how we've ended support for other operating systems in the past, and the majority of our customers have already made the move to Windows 10.

As we head into the 2020 elections, we know there is a relatively small but still significant number of certified voting machines in operation running on Windows 7.

We also know that transitioning to machines running newer operating systems in time for the 2020 election may not be possible for a number of reasons, including the lengthy voting machine certification process – a process we are working with government officials to update and make more agile.

Since we announced our Defending Democracy Program, we've focused on bringing the best of Microsoft's security products and expertise to political campaigns, parties, the election community and democracy-focused nongovernmental organizations.

This includes our AccountGuard service, which we offer at no additional cost, and ElectionGuard, which we're making available for free and open source.

As a next step in protecting the 2020 elections, the Defending Democracy Program will make extended security updates available for free to federally certified voting systems running Windows 7.

We will do this through the end of 2020, both in the United States and in other democratic countries, as defined by the EIU Democracy Index, that have national elections in 2020 and express interest.

We are also working with major manufacturers that have sold voting machines running Windows 7 to ensure any security updates provided to these systems are successful.

We are also announcing today that, as part of the Defending Democracy Program, we are proactively identifying and engaging election authorities that are Microsoft Azure customers to provide guidance and technical assistance in using the most advanced security features in Azure.

We provided this service ahead of the 2018 election cycle and will again ahead of the 2020 cycle.

If you are a government official overseeing 2020 elections and have questions about security updates for voting machines running Windows 7, or if you are an election official running elections-relevant workloads on Azure and would like help, please contact the Defending Democracy Team at Protect2020@microsoft.com.

We also encourage election authorities to upgrade Windows devices used to run their standard business operations to Windows 10.

These PCs are not subject to the certification requirements that are a major barrier to upgrading voting machines.

We offer Fast Track guidance to help election authorities upgrade these PCs to Windows 10, as well as other options.

To read more: https://blogs.microsoft.com/on-the-issues/2019/09/20/extending-free-windows-7-security-updates-to-voting-systems/

Number 9

DEPARTMENT OF HOMELAND SECURITY STRATEGIC FRAMEWORK FOR COUNTERING TERRORISM AND TARGETED VIOLENCE

The United States faces an increasingly complex, and evolving, threat of terrorism and targeted violence. As was the case sixteen years ago, at the U.S. Department of Homeland Security's founding, foreign terrorist organizations remain intent on striking the Homeland, whether through directed attacks or by inspiring susceptible individuals in the United States.

Today, though, the Nation also faces a growing threat from domestic actors inspired by violent extremist ideologies, as well as from those whose attacks are not ideologically driven.

Domestic threat actors often plan and carry out their acts of violence alone and with little apparent warning, in ways that limit the effectiveness of traditional law enforcement investigation and disruption methods.

We must confront these evolving challenges by building on existing best practices developed against foreign terrorist threats, identifying promising new approaches, and developing a strategic vision that provides a more holistic approach to preventing terrorism and targeted violence that originates here at home.

In an age of online radicalization to violent extremism and disparate threats, we must not only counter foreign enemies trying to strike us from abroad, but also those enemies, foreign and domestic, that seek to spur to violence our youth and our disaffected—encouraging them to strike in the heart of our Nation, and attack the unity of our vibrant, diverse American society.

The Department has experienced clear successes in its mission to thwart foreign terrorist enemies. We have denied them entry, stopping them at our border or even before they reach it.

We have integrated and supported the efforts of Federal, state, local, tribal, territorial, private sector, and international partners, gathering and sharing information and intelligence, and providing the resources they require to counter terrorism in their areas of responsibility.
We have strengthened our communities. As a Nation, we are more resilient than ever. Our ability to prevent foreign-origin attacks against the

Homeland is unmatched across the globe. These successes provide a roadmap for addressing the threat we face today.

This Strategic Framework outlines the Department's vision for reinvesting in programs and efforts that have enhanced our security, while incorporating key strategic changes that will allow us to address the threats we currently face.

In addition to addressing terrorism, this Strategic Framework encompasses targeted violence, such as attacks on schools, house of worship, public spaces, and transportation systems, and other forms of racially, ethnically, and religiously motivated violence that can overlap and intersect with terrorism.

The Strategy recognizes the critical role advances in technology have played in facilitating the spread, evolution, and interaction of violent ideologies and narratives of personal grievance, and the subsequent security implications, both for the Homeland and around the world.

Our Strategic Framework is crafted with the conviction that the Department must play a vital role in securing the privacy, civil rights, and civil liberties of Americans and others.

Privacy, civil rights, and civil liberties are essential. They should be cherished and safeguarded. This is designed to promote and preserve them. In addressing terrorism and targeted violence, we are steadfast that the role of the Department is to protect American communities, not to police thought or speech.

The Department of Homeland Security Strategy for Countering Terrorism and Targeted Violence is designed to implement the White House's 2017 National Security Strategy and 2018 National Strategy for Counterterrorism, as well as related national policy guidance.

While other departments and agencies have vital roles to play, this framework describes the Department's vision for addressing terrorism and targeted violence threatening the Homeland.

The goals, objectives, and priority actions promoted herein will also enhance the Department's ability to counter transnational criminal organizations, human traffickers, and other criminal threats.

The challenges facing our Nation are significant, but through a whole-of-society approach that empowers our citizens and our state, local, tribal, and territorial authorities, as well as our private sector, non-governmental, and community leaders, the Department of Homeland Security will

continue to adapt ahead of evolving threats, and will enhance the safety of our Nation.

To read the paper:
https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

Number 10

Scripting Engine Memory Corruption Vulnerability

Microsoft

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.

If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website, for example, by sending an email.

The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.

To read more: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

Number II

Reinventing the Network Stack for Compute-Intensive Applications

DARPA seeks to create new networking approaches to accelerate distributed application performance by 100x

Computing performance has steadily increased against the trajectory set by Moore's Law, and networking performance has accelerated at a similar rate. Despite these connected evolutions in network and server technology however, the network stack, starting with the network interface card (NIC) – or the hardware that bridges the network/server boundary – has not kept pace.

Today, network interface hardware is hampering data ingest from the network to processing hardware. Additional factors, such as limitations in server memory technologies, memory copying, poor application design, and competition for shared resources, has resulted in network subsystems that are creating a bottleneck within the network stack and are throttling application throughput.

"The true bottleneck for processor throughput is the network interface used to connect a machine to an external network, such as an Ethernet, therefore severely limiting a processor's data ingest capability," said Dr. Jonathan Smith, a program manager in DARPA's Information Innovation Office (I2O). "Today, network throughput on state-of-the-art technology is about 1014 bits per second (bps) and data is processed in aggregate at about 1014 bps. Current stacks deliver only about 1010 to 1011 bps application throughputs."

Addressing the bottleneck between multiprocessor servers and the network links that interconnect them is increasingly critical for distributed computing. This class of computing requires significant communication between computation nodes. It is also increasingly relied on for advanced applications such as deep neural network training and image classification.

To accelerate distributed applications and close the yawning performance gap, DARPA initiated the Fast Network Interface Cards (FastNICs) program. FastNICs seeks to improve network stack performance by a factor of 100 through the creation of clean-slate networking approaches. Enabling this significant performance gain will require a rework of the entire network stack – from the application layer through the system software layer, down to the hardware.

"There is a lot of expense and complexity involved in building a network stack – from maximizing connections across hardware and software to reworking the application interfaces. Strong commercial incentives focused on cautious incremental technology advances across multiple, independent market silos have dissuaded anyone from addressing the stack as a whole," said Smith.

To help justify the need for this significant overhaul, the FastNICs programs will select a challenge application and provide it with the hardware support it needs, operating system software, and application interfaces that will enable an overall system acceleration that comes from having faster NICs. Under the program, researchers will work to develop, implement, integrate, and validate novel, clean-slate network subsystems.

Part of FastNICs will focus on developing hardware systems to significantly improve aggregate raw server datapath speed. Within this research area, researchers will design, implement, and demonstrate 10 Tbps network interface hardware using existing or road-mapped hardware interfaces.

The hardware solutions must attach to servers via one or more industry-standard interface points, such as I/O buses, multiprocessor interconnection networks, and memory slots, to support the rapid transition of FastNICs technology. "It starts with the hardware; if you cannot get that right, you are stuck. Software can't make things faster than the physical layer will allow so we have to first change the physical layer," said Smith.

A second research area will focus on developing system software required to manage the FastNICs hardware resources. To realize 100x throughput gains at the application level, system software must enable efficient and parallel transfer of data between the network hardware and other elements of the system. FastNICs researchers will work to generate software libraries – all of which will be open source, and compatible with at least one open source OS – that are usable by various applications.

FastNICs will also explore applications that could be enabled by the multiple order of magnitude performance increases provided by the program-generated hardware. Researchers will aim to design and implement at least one application that demonstrates a 100x speedup when executed on the novel hardware/software stack, providing a validator for the program's primary objective.
There are two application areas of particular interest – distributed machine learning and sensors. Machine learning requires the harnessing of clusters – or large numbers of machines – so that all cores are employed for a single purpose, like analyzing imagery to help self-driving cars appropriately identify an obstacle in the road.

“Recent research has shown that by speeding up the network support, the entire distributed machine learning system can operate more quickly. With machine learning, the methods typically used involve moving data around, which creates delays. However, if you can move data more quickly between machines with a successful FastNICs result then you should be able to shrink the performance gap,” said Smith.

FastNICs will also explore sensor data from systems like UAVs and overhead imagers. An example application would be change detection where tagged images are used to train a deep learning system to recognize anomalies in a time series of image captures, such as the presence of a strange structure, or a sudden spurt in activity at facilities in an inexplicable location.

Change detection requires quick access to both current sensor data as well as the ability to rapidly access archives of data. FastNICs will provide a way of accelerating the acquisition of actionable intelligence from a mountain of data.

A FastNICs Broad Agency Announcement is currently posted on FedBizOpps.gov and includes program objectives, schedules, and metrics. More information is available here, https://www.fbo.gov/index?s=opportunity&mode=form&id=fb5cfba969669de12025ff1ce2c99935&tab=core&_cview=1

Number 12

The future of stress testing – realism, relevance and resources

Keynote speech by Andrea Enria, Chair of the Supervisory Board of the ECB, at the European Systemic Risk Board (ESRB) Annual Conference

In 1628, the Vasa – the pride of the Swedish navy – was the most powerful warship in the Baltics. Until she sank about half an hour into her maiden voyage, that is. So what happened? Well, nothing special when it comes to sailing ships: the wind simply picked up.

The problem was that the Vasa's design was rather unstable. She had been built for the shallow waters around Stockholm, so not too much of the ship was below the waterline and a lot of weight was concentrated in her upper structures.

Thus, when the wind picked up, it pushed the ship so far over on its port side that water poured in through open gunports. And that was the end of the Vasa – and a huge embarrassment for the King of Sweden, Gustavus Adolphus.

Now, why am I telling you the story of the Vasa? In my view, it shows how beneficial it is to spend a moment or two thinking about what might happen if the wind picks up.

This is true when it comes to building ships and, in a sense, it is also true when it comes to managing banks. How will lenders fare in a storm? Are they stable enough to weather a storm? Or do they need additional weight below the waterline, in the form of more capital.

This idea sounds straightforward, doesn't it? Yet, it is only recently that stress tests for banks have entered the picture. It was the IMF that started such exercises as part of its regular Financial Sector Assessment Programs. But it took another 20 years before stress tests would become a key tool for banking supervisors.

In 2009, the United States used stress tests as a means to fight the financial crisis; Europe followed suit in 2010. Since then, stress tests have become a key instrument in the supervisory toolbox. So let us take a closer

look at the evolution of stress testing and its objectives, and how it might need to be adapted in the future.

Goals and benefits of stress testing banks

The general goal of a stress test is quite simple: to assess how the ship would weather a storm and what shape it would be in afterwards. In terms of banks: how would the bank fare if the economy took a turn for the worse? Would it survive? And would it still be able to provide loans to help the economy recover?

Answering these questions has been the core intent of the stress tests since they were first introduced in Europe. But over time, they have also served other topical purposes.

Stress tests were used during the last financial crisis to gauge the size of the capital holes in bank balance sheets, and they were key elements in determining how much additional capital needed to be provided. This helped to reduce uncertainty and calm the markets – not least because some banks took upcoming stress tests as a cue to pre-emptively build up capital.

At the time, there was the difficult challenge of addressing the risks triggered by the sovereign debt crisis. And so the choice was made to provide extensive disclosure to the markets with a view to helping them correctly assess the risks of individual banks. This, in turn, helped to bring about more effective market discipline.

Then, in 2014, stress tests featured heavily in the comprehensive assessment that preceded the establishment of European banking supervision. Here, they helped to level the playing field for banks from 19 countries with different accounting rules and supervisory practices.

It was these stress tests, for instance, that first relied on the benefits of the Single Rulebook, which provides fully harmonised definitions of capital and non-performing loans as developed in the Capital Requirements Regulation and the EBA's standards.

Since then, stress tests have become a regular transparency and benchmarking exercise. But their focus has shifted. Rather than measuring the actual size of capital holes against a supervisory yardstick, stress tests now help us to spot vulnerabilities in banks. Also, the dialogue between supervisors and banks has become more important as the stress test is seen as a tool to strengthen banks' own risk management.
Ever since they were first used, stress tests have helped to make the banking sector more transparent. In Europe, disclosure has always been a

key feature of the exercise. Transparency helps to foster market discipline in parallel with supervisory judgement.

Over the years, stress tests have remained an important tool for supervisors. What we learn from them guides our Supervisory Review and Evaluation Process, or SREP. The stress test results are used, for instance, as a starting point when setting the Pillar 2 guidance, or P2G. Likewise, the insights we gain from stress tests can also inform other supervisory actions such as follow-up on-site missions or internal model investigations.

No matter which goals they have served, stress tests have so far proved very useful. But we have to acknowledge one thing: the attempt to align different, sometimes conflicting objectives has led to a fairly complex and resource-intensive exercise. And this, in turn, has led to a certain amount of discontent among supervisors and banks alike. So ten years after the crisis, and five years into European banking supervision, it is time to rethink the design of stress tests.

Rethinking stress tests: realism, relevance and resources

When discussing the future of stress tests in Europe, we can rely on three yardsticks to gauge how best to proceed: realism, relevance and resources. We need a stress test that paints a realistic picture of individual banks; we need a stress test that is relevant for supervisors, banks and markets alike; and we need a stress test that balances costs and benefits.

All these things are connected, of course. But for the sake of today's discourse, I'll try to disentangle them for you, starting with realism.

First, let's look at the methods we use to calculate the impact of the stress scenarios. Currently, we rely on a constrained bottom-up approach. Banks use their internal models to calculate how their capital positions would change in the stress scenario. However, we impose some constraints on these models. Static balance sheets are one of them: we assume that management would not attempt to mitigate the impact of the stress.

Such constraints act as safeguards. They discourage banks from engaging in a beauty contest where they strive to look good instead of real. They make the results of the stress tests easier to compare and more conservative. And they also make quality assurance less complex.

All this comes at the cost of realism, however. But what exactly does realism mean for an exercise that is based on hypothetical scenarios? To me, it means that the results of the stress test accurately reflect how the hypothetical stress would actually affect a bank's balance sheet. In other

words, if it rains on the economy, how would the water trickle down or pour into the balance sheet?

So, if we want to make stress tests more realistic, the constraints might be one of the levers to pull. We might ask, for instance, whether it is realistic to assume static balance sheets. And the banks do ask, believe me. Selectively relaxing the constraints would allow us to better account for bank-specific factors and management actions – and this would make results more realistic.

Also, constraints might be seen as being the main driver of the results, rather than a backstop to ensure their credibility. In this case, banks would tend to consider the exercise irrelevant from an internal risk management perspective. This view often makes banks reluctant to publish final results which do not reflect their own views on risks.

But the realism of the exercise is also challenged because it easily turns into a "beauty contest": banks direct their efforts to "model the stress away" in order to look good to supervisors and investors. And the experience from the first rounds of European stress tests shows that banks indeed often try to compensate losses in the adverse scenario. They do so by either being overly optimistic when estimating their income in the adverse scenario or by being very positive on what management can achieve in turbulent market conditions.

We also see banks conspiring to game stress tests, often with the help of external advisers. Data are collected from banks ahead of their submission to supervisors, and each bank is informed of its position vis-à-vis its peers. This helps them to align before and during the exercise in order to collectively adjust the results and minimise the impact of the stress scenario. We see this, we don't like it, and we will not tolerate it.

Naturally, realism is closely linked to the second point on my list: relevance. The more realistic the results are, the more relevant they should be. But the notion of relevance may differ according to the objective that the stress test aims to achieve.

For banks, the stress test might be most useful for risk management purposes when the methodology and the scenario are tailored to the specific business model and risk profile of each bank. Thus, the ideal would be to have a tailor-made stress test for each and every bank.

Supervisors, too, care about the ability of the stress test to capture the risk profile of each bank. But they also need the results as input when setting capital buffers – the Pillar 2 guidance. As this is an administrative measure, consistency across banks is crucial: each bank should be subject

to significant stress, which challenges its resilience and provides comparable input for the Supervisory Review and Evaluation Process.

Macroprudential authorities want to assess how resilient the system as a whole is. They want to see how a single shock that hits banks at a certain point in time would spread throughout the system and potentially hamper its ability to serve the economy.

Finally, there are the markets. For them, relevance is closely linked to transparency. In other words, does the stress test provide valuable additional information on individual banks? I believe that the European stress test is one of the most transparent in the world. We publish a huge amount of data bank by bank and based on common definitions.

But there is one thing that markets cannot see: the link between stress test results and supervisory action. While we are very transparent on the results, we remain quite opaque on how they translate into capital add-ons. I am very much aware that both banks and supervisors have concerns when it comes to enhancing transparency in this area. They are worried, for instance, that if stressed capital guidance as defined by supervisors was to be disclosed, it might be misunderstood. It might be seen as a rigid minimum requirement and not as a buffer to be used under stress.

But to be honest, I still think that we need to seriously consider disclosing Pillar 2 guidance at some point. This is particularly true in a bail-in world, where private investors and not taxpayers are supposed be first in line when it comes to picking up the bill following a crisis. More transparency on the supervisory outcome of stress tests would sustain their relevance for banks and markets alike. Stress tests must have clear consequences.

Let's now turn to the final item on my list: resources. A stress test is a complex exercise. As I've said before, it is extremely resource-intensive for both banks and supervisors. This might be justified as long as the tests produce realistic and relevant results. Still, we need to strike a balance between costs and benefits. And currently, the impression seems to be that the amount of resources deployed is quite high when set against the value of the information that is generated.

I believe that all stakeholders agree on the basic idea that if we want to take stress testing from infancy to maturity, we need to progress in all three dimensions. We need to make it more realistic, more relevant and less resource-intensive. Yet, views differ significantly as to the best way forward, even among supervisors. So how can we square the circle?

Squaring the circle – the way forward

Ladies and gentlemen, when discussing the future of stress testing in Europe, we must keep in mind that "the future" means post-2020; the upcoming stress test will certainly follow the current approach. Nevertheless, the time for debate has come. The report recently published by the European Court of Auditors on the European stress test provides important input into this debate.

So far, I have discussed three yardsticks that stake out the bounds of possible futures: realism, relevance and resources. While I've taken them one by one in my remarks today, in reality they're all linked. Unfortunately, these links sometimes take the form of trade-offs. Thus, there are many parts which we can arrange in different ways, depending on how we want to balance them.

Imagine we decided to relax constraints in the bottom-up approach. Banks would be free to depart from a common methodology and scenario to better reflect their individual business models and risk profiles. The results of the stress test would become more realistic and more relevant for banks, which is good. However, supervisors would have a hard time using the results of such an exercise to determine capital buffers in a consistent way across banks. They would need to invest more time and energy in quality assurance, which would require additional resources.

So what should we do about it? Well, there are voices arguing that supervisors should focus more on top-down stress tests, as is done in the United States. Thus, they would run the exercise with their own models and fully control the consistency of the results. But then, much less information would be provided to the markets. After all, banks would not accept the publication of very granular risk parameters which would not reflect their own risk management practices.

I think that the root of the problem lies in the fact that we are trying to do too much with too little. If we aim to achieve several goals, some of which conflict with each other, and if we aim to serve different customers, the stress test is bound to disappoint all of them.

So I wonder whether the time is ripe to consider some bolder solutions. Why not split the microprudential stress test into a bank view and a supervisory view? The bank view would stem from a largely unconstrained bottom-up approach. There would be no quality assurance, but banks would have to explain where and why they deviate from the constraints. This would allow each bank to account for its individual circumstances. And each bank would have an added incentive to invest in risk management. The stress test would become more realistic and more relevant as a result. It could provide useful, granular information to the markets.

At this point, some might argue that banks could get over-excited about the freedom they would gain, and that this could lead to a lack of conservatism. This is where the supervisory view comes in.

It would rely on a constrained bottom-up approach, and top-down models would be used to provide quality assurance for the results and focused benchmarking. So it would be very similar to the approach followed in 2018. However, some methodological constraints, including the static balance sheet assumption, could be relaxed somewhat to increase realism. Likewise, the exercise could be streamlined and thus become less resource-intensive.

First, there would be fewer quality assurance cycles, as there would be no need to align the bank view and the supervisory view.

Second, the outcome of the supervisory view would only be published in terms of capital depletion, making it less granular.

Third, some design features of the bank view and the supervisory view could be aligned, which would avoid duplicating efforts. This too would save resources. At first, top-down stress tests would continue to support quality assurance. But in the longer run, as accuracy and reliability improve, we might consider relying even more on top-down stress tests.

The bank view and the supervisory view would then be published next to each other so that markets could form their own view.

To sum up, splitting stress tests into two components could help make them more realistic and relevant without taking up more resources.

Conclusion

Stress tests have become an important tool for supervisors in the wake of the financial crisis. And in Europe, we have benefited greatly from their use. I am indeed a great believer in stress testing, but I do also see the need to refine the exercise and adapt it to the post-crisis world. I have outlined a few ideas for you today, but they are only ideas at this stage. Nevertheless, if we all agree that we need to make stress tests more realistic and relevant without becoming too burdensome, then it is these ideas that we need to discuss.

This brings us back to the Vasa. The twist in the story is that the captain did design a rudimentary stress test. To gauge the stability of the ship, he had 30 of his men run from one side of the deck to the other in order to make her roll. And roll she did. However, a representative of the King was

on board, and he stopped the test. His main concern was that the stress test itself might sink the ship.

My final message is that we should be open-minded in the conversation about the future of stress tests. And the bottom line is this: they should remain serious, challenging and credible exercises; they should help supervisors to ensure the safety and soundness of banks.

Thank you for your attention.

Number 13

European Cybersecurity Month 2019 is launched

October marks the kick-off of the European Cybersecurity Month (ECSM), coordinated by the European Union Agency for Cybersecurity (ENISA), the European Commission and supported by the Member States.

This campaign will focus on expanding awareness about cybersecurity to citizens across Europe.

The 2019 campaign focuses on different themes addressing the need for behavioural change and identifying opportunities to help users recognise the risks of new technologies.

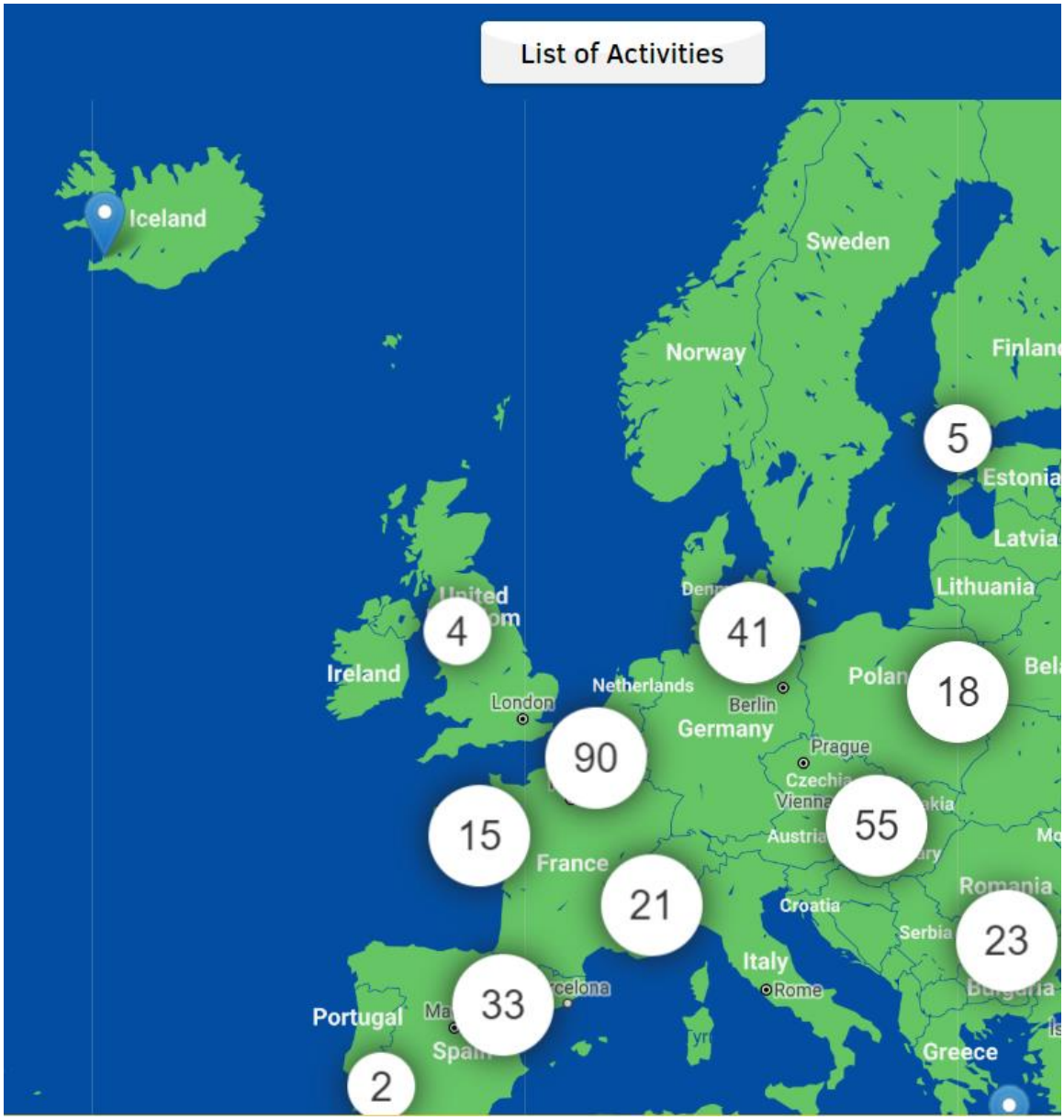
The first theme encompasses basic 'Cyber Hygiene', which uses the hygiene metaphor to inform about good cybersecurity habits that are part of everyone's daily routine. Having healthy cyber safety practices can provide users with more confidence using their devices, whether it's a computer, a smart phone, a wearable device or any other gadget that's connected to the internet. The key take-home message conveys that cyber hygiene is a habit you learn from a young age and remains a daily routine for life.

The second theme concentrates on 'Emerging Technology' and recognises the importance of keeping you and your new tech gadgets and devices secure. Technology is developing fast and it is important to question the security and privacy settings for your new purchases. For this theme, citizens will be guided around the topics they should be aware of when it comes to new technology.

European Commissioner for Digital Economy and Society Mariya Gabriel said: "Today we launch European Cybersecurity Month 2019, we are boosting awareness around online safety and the cybersecurity skills needed for the future. If we want to complete the Digital Single Market, it is essential we ensure EU citizens, particularly young people have the knowledge and skills to protect themselves online. It is our shared responsibility for all citizens to become responsible users of emerging technologies."

ENISA's Executive Director Udo Helmbrecht said: "Cyber threats are evolving at a rapid pace and human behaviour can play a fundamental role in how we stay cyber secure. Ensuring that all citizens are aware of online risks and have the tools to become more resilient and confident users is a key goal of European Cybersecurity Month. This October, we urge everyone

to stay alert with new technology and establish strong cyber hygiene habits."



Today to launch the campaign, ENISA has published a video that will provide citizens with simple awareness checks to undertake in their daily lives. Furthermore ENISA is organising an 'Ask Me Anything' session on Twitter on 30th September at 10:00 CET, for citizens and organisations to pose general cybersecurity questions on how to secure their devices to the EU Agency for Cybersecurity (ENISA).

Further European Cybersecurity Month information can be found on cybersecuritymonth.eu

What is CyberSecMonth?

Cybersecurity is a Shared Responsibility

ECSM is the EU's annual awareness campaign that takes place each October across Europe. The aim is to raise awareness of cybersecurity threats, promote cybersecurity among citizens and organizations; and provide resources to protect themselves online, through education and sharing of good practices.

LEARN MORE

enisa

STOP | THINK | CONNECT™

Staying secure online 2019 Campaign

Your Daily Cyber Routine - This year's campaign video is designed to: highlight the risks, demystify the remedies and suggest that the preventative actions required aren't as difficult or confusing as people might think. Share the video and invite friends and family to take some simple actions that can be make a big difference to your online safety.

Staying Safe with Tech - People are buying more and more tech gadgets to make their lives easier or just for fun. It's important to be aware of safety by asking these smart cyber questions before purchasing your next tech device.

Resources

Number 14

Espionage

CPNI
Centre for the Protection of National Infrastructure

The potential impact of successful State-sponsored espionage against the UK is both wide reaching and significant.

The threat of espionage (spying) did not end with the collapse of Soviet communism in the early 1990s.

Espionage against UK interests still continues and is potentially very damaging. A number of foreign intelligence services (FIS) seek to gather intelligence on a broad range of subjects, including foreign policy, defence, financial, technological, industrial and commercial interests.

What is espionage?

Most governments rely on a range of information being gathered to guide their decisions. This is not the same as espionage.

Espionage is the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). It may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power.

Open information gathering

The gathering of publicly available information is a routine activity of diplomatic staff, military attachés and trade delegations.

They use open sources such as the media, conferences, diplomatic events and trade fairs, and through open contact with host government representatives.

This enables them to monitor political, economic and military developments in their host country and brief their own governments.

Foreign representatives thereby help their governments to shape their foreign, commercial and military policies. This type of work is not harmful to our national interests. In fact, it often helps us to build good relationships with other nations.

Why espionage is damaging

Espionage focuses on gathering non-public information through covert means. Classified information is kept secret in the first place because its disclosure might harm national security, jeopardise the country's economic well-being or damage international relations. Its sensitivity makes it necessary for us to protect it but also makes it attractive to spies.

If this information is obtained by those with no right to access it, serious damage can be caused. For instance:

- other countries seeking technical details of weapons systems so that they can find ways of neutralising our military advantages.

- gathering information on key services such as gas, oil and transport which could enable terrorists to seriously damage these important economic targets.

- theft of classified technologies which could enable foreign companies to copy them, threatening both national security and jobs in the UK.

Targets of Espionage

In the past, espionage activity was typically directed towards obtaining political and military intelligence.

These targets remain of critical importance but in today's technology-driven world, the intelligence requirements of a number of countries are wider than before.

They now include communications technologies, IT, energy, scientific research, defence, aviation, electronics and many other fields. Intelligence services, therefore, are targeting commercial as well as government-related organisations. They sometimes do this on behalf of state-owned or sponsored companies in their own countries.

The UK is a high priority espionage target. Many countries actively seek UK information and material to advance their own military, technological, political and economic programmes.

The threat is not confined to within the UK itself. A foreign intelligence service operates best in its own country and therefore finds it easier to target UK interests at home, where they can control the environment and take advantage of any perceived vulnerabilities. The most capable foreign intelligence services are able to operate all over the world.

What information are spies looking for?

Intelligence agencies are directed by their governments to focus their attention on specific priorities. State agencies, the military and companies working on sensitive technologies are prime targets for foreign espionage.

Intelligence services working against the UK tend to focus on gaining a number of different types of secret information:

Military secrets

These will include technical information about weapons, details of where troops are located, information on defences and so on. This can be especially useful to an enemy country in wartime. It can help an enemy to find weak points or launch surprise attacks. It can also be useful to terrorists, as it can help them to pick out targets and weak points.

Industrial secrets

These will include information on companies' products and plans. Spies are especially interested in details of new inventions that may have a military or commercial use. Examples include communications technologies, computers, genetics, aviation, lasers, optics and electronics. Such secrets may also help give some countries an economic or military advantage.

Information of interest could extend from manufacturing processes and research programmes through to negotiating positions, financial transactions and longer-term strategy developments. All of which can help provide other countries with an economic advantage or enable foreign companies to establish a market lead using UK innovation.

In addition, previous incidences of the theft or release of sensitive information have been instigated by competitors, media organisations, activist groups, past employees and even existing staff - the consequences of which are no less costly, embarrassing or disruptive to the organisation that was targeted.

Political secrets

These will include confidential information on political and security affairs, negotiating positions, sensitive economic information and details of policy developments. Foreign governments could use such information to gain advantage in areas such as international relations and intelligence operations.

Targeting dissidents

Some foreign governments also target dissident movements and individuals that they see as a threat to their control at home. The UK's long tradition of political tolerance has meant that many foreign dissidents have made their homes here over the years – most famously the Russian revolutionaries Lenin and Trotsky – but this has also prompted the sometimes hostile interest of foreign intelligence services and this continues to the present day.

How is espionage conducted?

Spies working for states fall into two categories: intelligence officers and agents.

Intelligence officers

Intelligence officers are members of intelligence services. They will be highly trained in espionage techniques and the use of agents. They may operate openly, declaring themselves as representatives of foreign intelligence services to their host nation, or covertly under the cover of other official positions such as diplomatic staff or trade delegates.

Some intelligence officers may operate under non-official cover to conceal the fact that they work for an intelligence service - posing as a business person, student or journalist for example. In some cases they may operate in "deep cover" under false names and nationalities. Such spies are dubbed "illegals" because they operate without any of the protections offered by diplomatic immunity.

Agents

In the UK, an agent, more formally known as a "covert human intelligence source", is someone who secretly provides information to an intelligence officer. They will probably not be a professional "spy" but may have some basic instruction in espionage methods. An agent may be motivated by a wide variety of personal or ideological factors.

Differences in terminology

Confusion often arises between what is meant by an officer and an agent. Other countries use the same terminology in different ways. In the United States, for instance, an agent is a member of an intelligence or security agency such as the FBI or CIA. Such agencies call a covert human intelligence source an "informant" rather than an "agent."

How intelligence officers and agents operate

Intelligence officers seek to gather covert intelligence directly and to recruit agents to obtain intelligence on their behalf.

The methods used by intelligence officers vary widely, and are often limited only by their ingenuity.

They will often take advantage of the latest technology, using it to eavesdrop, tap telephone calls and communicate secretly. However, the human relationship between intelligence officers and their agents remains a key element of espionage.

Foreign intelligence services typically seek to establish networks of agents whom they can use over a sustained period of time, so that they can obtain a reliable flow of information.

Agents operate by exploiting trusted relationships and positions to obtain sensitive information.

They may also look for vulnerabilities among those handling secrets. They may be aware of flaws in their organisation's security that they can exploit.

Cyber espionage

Espionage activity is also carried out in cyberspace. Foreign intelligence services increasingly use the Internet and cyber techniques to conduct espionage against UK interests.

Cyber can be an attractive method of intelligence gathering for several reasons:

- It can be more cost-effective than traditional means;

- Its remote nature means that those involved have an extra layer of deniability;

- The volume of data that can be stolen is potentially immense.

Cyber also negates the need for a human agent as information gathering can be done remotely, without an intelligence officer needing to leave their desk, let alone their country.

As we become more reliant on the internet in our everyday lives the threat from cyber espionage will only increase. To that end the Government has

published a UK Cyber Security Strategy. This will help the UK to retain its balance of advantage in cyberspace.

You may visit: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

For more information on how to protect against cyber threat, see the National Cyber Security Centre website - https://www.ncsc.gov.uk/

More information about the espionage threat can be found on the MI5 website at https://www.mi5.gov.uk/counter-espionage

Number 15

Revisiting an important paper

Kaleidoscope on the Internet of Toys

Safety, security, privacy and societal insights

Stéphane Chaudron, Rosanna Di Gioia, Monica Gemo, Donell Holloway, Jackie Marsh, Giovanna Mascheroni, Jochen Peter, Dylan Yamada-Rice

This paper gives an insight into safety, security, privacy and societal questions emerging from the rise of the Internet of Toys.

These are Internet Connected Toys that constitute, along with the wave of other domestic connected objects, the Internet of Things, which has increased the ubiquity of the ICT within our everyday lives, bringing technology more than ever closer to ourselves and our children.

What changes and challenges will 24/7 Internet connected devices, and Connected Toys in particular, bring to our society? What precautionary measures do parents, teachers, health care professionals, and also industry partners and policymakers, need to take in order to protect our children's play, safety, security, privacy and social life? Based on which considerations? In which timeframe?

The paper offers a kaleidoscope of six experts' views on the Internet of Toys, each exploring the topic and raising questions from a specific angle, as follows: Public and industrial discourse; Safety, security and privacy concerns; Social robot-children interactions; Quantified-self of the Childhood; Nature of Play and, finally, Possible benefits of higher collaboration between research and the Internet Connected Toy Industry.

Introduction

Modern ICT offers formidable opportunities and possible new benefits to citizens and society. The rise of domestic Internet connected devices increases the ubiquity of ICT, embedding it further within our everyday lives, and bringing it closer to ourselves more than ever, 24/7.

Internet connected objects (known as the 'Internet of Things') are increasingly coming into our homes, with objects such as watches, fridges, toothbrushes, or coffee machines, turning our houses into Smart Houses.

Among the newly connected familiar objects are also Internet connected toys that parents today are starting to choose for their children.

Internet connected toys can offer new, important opportunities for play, learning, health and educational support, thanks to their interactive and personalised features, but they also raise questions about safety, security, privacy, trust and other fundamental rights of children.

Indeed, Internet connected toys, as is the case with any other connected device, may record personal information regarding our children's lives, and then use and share the data.

In a time of concerns about internet safety, security and privacy and social change, it seems crucial to take a step back, pose questions and look at these connected toys, characterised as the 'Internet of Toys', from various angles.

To read more:
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf

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.