*October 2020, cyber risk and compliance in Switzerland*

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

Dear readers,

During its meeting on 5 October 2020, the Swiss Federal Council Cyber Committee adopted the report on the progress made in implementing the national strategy for the protection of Switzerland against cyber-risks (NCS).

The 2018-2022 NCS specifies the strategic goals for protecting against cyber-risks. Implementation is going to plan and is largely supported by players from the cantons, the business community, universities, and the general public.

As the federal competence centre, the National Cybersecurity Centre (NCSC) is responsible for coordinated NCS implementation and regularly prepares a report on the state of implementation on behalf of the NCS Steering Committee.

The report covers the current implementation status as of the first quarter of 2020. A third of the 247 milestones defined in the implementation plan have already been reached.

*Progress made in promoting research and training*

The implementation of most of the milestones is planned for the second half of the NCS 2018-2022 period and must be completed by the end of 2022.

There are delays concerning 23 milestones. The competent bodies have explained the delays to the Steering Committee and plausibly demonstrated that they can be made up.

Concrete progress has been made in various areas of action. For example, an important milestone in the promotion of research and training was reached with the opening of the Cyber Defence Campus (CYD Campus) at

the two Federal Institutes of Technology, ETHZ and EPFL, as well as in Thun. Regarding prosecution, coordination in the area of combating cybercrime has been improved.


*Support for SMEs and the general public*

Small and medium-sized enterprises (SMEs) are now an NCS target group too.

Accordingly, cyber-risk support for them is being established and expanded. For example, a guide for SMEs has been prepared together with representatives from the business community.

Furthermore, the National Contact Point commenced operations in the NCSC on 1 January 2020.

It receives cyberincident reports from the general public and businesses, analyses them and forwards them to the competent bodies.

Those who submit reports are given recommendations on the action to be taken.

Since the adoption of the 2018-2022 NCS, the Federal Council has also decided on and implemented the Confederation's new organisation in the area of cyber-risks.

The Ordinance on Protecting against Cyber-Risks in the Federal Administration, which has been in force since 1 July 2020, creates the legal basis and governs cooperation both within the Federal Administration and with the cantons, businesses and academia.

To learn more:
https://www.newsd.admin.ch/newsd/message/attachments/63347.pdf

---

On 19 October 2020, the Swiss Federal Department of Finance (FDF) initiated the consultation on the blanket ordinance in the area of blockchain. It will run until 2 February 2021.

On 25 September 2020, the Swiss Parliament unanimously adopted the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT), thereby amending specific provisions in ten existing federal acts.

This has further improved the framework conditions for Switzerland to become a leading, innovative and sustainable location for blockchain and DLT companies.

A blanket ordinance is now planned to incorporate the legislative amendments voted by Parliament into law at federal ordinance level.

The consultation of the cantons, parties and other interested groups will run until 2 February 2021.

It is expected that the Federal Council will bring the amendments to the acts and ordinances into force on 1 August 2021.

However, it is planned that the amendments to the Financial Services Act and the Financial Institutions Act that were adopted by Parliament as part of the DLT bill will enter into force earlier.

These amendments limit the ombudsman affiliation requirement for specific financial service providers.

To read more:
https://www.newsd.admin.ch/newsd/message/attachments/63329.pdf

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

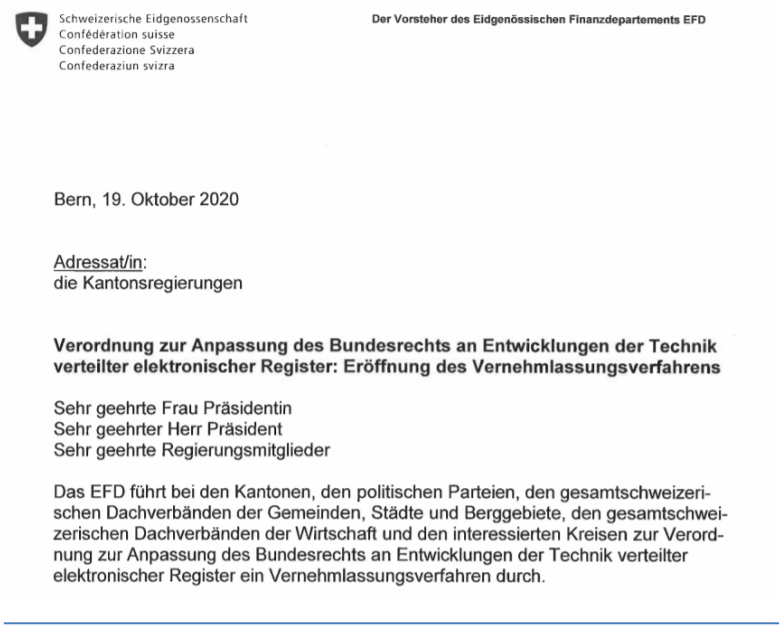
Eidgenössisches Finanzdepartement EFD

Bern, 19. Oktober 2020

**Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register**

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

https://www.newsd.admin.ch/newsd/message/attachments/63334.pdf



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Vorsteher des Eidgenössischen Finanzdepartements EFD

Bern, 19. Oktober 2020

Adressat/in:
die Kantonsregierungen

**Verordnung zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register: Eröffnung des Vernehmlassungsverfahrens**

Sehr geehrte Frau Präsidentin
Sehr geehrter Herr Präsident
Sehr geehrte Regierungsmitglieder

Das EFD führt bei den Kantonen, den politischen Parteien, den gesamtschweizerischen Dachverbänden der Gemeinden, Städte und Berggebiete, den gesamtschweizerischen Dachverbänden der Wirtschaft und den interessierten Kreisen zur Verordnung zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register ein Vernehmlassungsverfahren durch.

I have just read the *Internet Organized Crime Threat Assessment (IOCTA) of 2020*. This is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime.

It provides a unique law enforcement focused assessment of emerging challenges and key developments in the area of cybercrime.

According to the assessment, continuing innovative developments of recent years, criminals are *offering full digital user profiles* in order to bypass advanced fraud prevention tools.

In keeping up with e-commerce merchants increasingly employing analytics checking a user's identity against device fingerprints and several other metrics, criminals have moved to *obtaining and selling* these digital profiles to commit fraud.

Taken from machines compromised in a botnet, they are used in order to make purchases using the compromised computer pretending to be a returning customer, using the same browser settings and victim's card credentials.

After the fraud, many victims erase the evidence themselves, following Windows security guidance to restore to the last known configuration after having been compromised by the botnet, effectively removing all traces of the intrusion.

This use of botnets to bypass sophisticated fraud prevention tools reflects a recurrent theme in the fight against cybercrime – as security measures are heightened, criminals come up with novel ways to continue their illicit activities.

There has been an increase in the provision of digital and cybercrime elements on the *Darkweb*. Personal data, access to compromised systems, as well as services catering malware, ransomware, and DDoS attacks, are all elements prevalent for the facilitation of cybercrime.

*Document and proof of identity services* have also increased on the Darkweb. Perpetrators generally use identity and document services to support citizenship claims and other applications, obtaining lines of credit to set up a business, open untraceable bank accounts, proof of residence, to commit insurance fraud, purchase illicit items and other uses.

There has been a shift in the offering of *legitimate-looking counterfeit passports* to "legal or registered" passports, which can pass several authentication tests, with criminals offering registered passport services.

Trend Micro Inc. has explained that the increase of global immigrants and the increasing adoption of e-passports is a likely driver behind this trend.

Additionally, some Darkweb sites also promote money laundering and instructions for users on how to use cryptocurrencies for money laundering.

Users can find drug listings in massive volume on the Darkweb; however, these do not necessarily reach priority-levels in terms of impact.

More impactful, dangerous drugs, such as fentanyl, opioids and heroin are still significantly present on the Darkweb, although listings are smaller in number.

Europol has observed an increasing trend of top organised crime groups having a presence on the Darkweb dealing drugs, which is likely due to an effort to expand their distribution mechanisms.

As noted in IOCTA 2019, drug dealers may also be running multiple monikers on the Darkweb which makes it difficult to prioritise within the drug topic.

Additionally, the COVID-19 pandemic crisis seemed to have the most effect on the supply chains regarding drug trade compared to other crime. This has now stabilised and the situation has returned to normal, with an anticipated growth on the horizon.

Finally, the distribution of firearms has become significantly more fragmented. After the takedown of the Berlusconi marketplace by Italian law enforcement, which used to be the go-to place for firearms on the Darkweb, firearms have emerged on different marketplaces.

Firearms are also available on OpenBazaar, although the scale of supply is unconfirmed. Some shops are also selling firearms from the United States.

The ability for individuals to purchase firearms on the Darkweb has become increasingly difficult, due to recent law enforcement successes in catching individuals purchasing firearms illegally.

The diverse products and services vary in their level of impact and their ability to facilitate more serious forms of crime.

The supply of these goods on the Darkweb poses a significant threat in the EU. Furthermore, the geographic nature of the threat is also diversifying.

The Hydra market – the largest darknet marketplace serving Russia and neighbouring countries – has recently advertised an impending publication of a new, secure encrypted market platform, which they aim to open to the English-speaking community.

Such a development would arguably make Darkweb investigations more difficult for law enforcement in the future and poses a significant threat to the EU. Read more at number 6 below.

The role of *stress testing* has rapidly evolved and grown in importance after 2009 in most jurisdictions. Stress testing is now a critical element of risk management in the financial sector, and a core tool for banking, insurance, securities supervisors and macroprudential authorities.

A stress testing exercise alerts management and supervisory authorities to unexpected adverse outcomes arising from a wide range of risks, and provides an indication of the financial resources that might be needed to absorb losses.

In 2020, after the COVID crisis, we have some interesting developments from the European Banking Authority (EBA). After postponing the EU-wide stress test to 2021 (in order to allow banks to focus on and ensure continuity of their core operations), the Board of Supervisors of the ECB agreed on an additional EU-wide *transparency exercise* to be carried out, with the aim of providing updated information on banks' exposures and asset quality to market participants.

*Which is the difference between a transparency exercise and a stress test?*

Transparency exercises are purely disclosure exercises where only supervisory reporting data on a bank by bank level is published, and no shocks are applied (as it is the case for stress tests).

Transparency exercises are conducted by the EBA on a regular basis at the EU-wide level and cover the largest EU banks *at their highest level of consolidation*.

Both exercises aim at promoting market and supervisory discipline and providing transparency on banks' exposures, so as to address any uncertainties that may still remain.

The transparency exercise is a mean through which the EBA disseminates bank-by-bank information on a wide sample of EU banks in a consistent and comparable way.

In stress testing we follow Ovid's advice: "Perfer et obdura, dolor hic tibi proderit olim" (be patient and tough, someday this pain will be useful to you)". In transparency exercises, which are conducted by the EBA, banks have some more time to focus of the outcomes of the COVID crisis and focus on what must be done today.

Read more at number 10 below.

It is hard to believe that we must discuss with boards of directors terms like *mixers, tumblers,* and *chain hopping*. *Jurisdictional arbitrage* is again on the table, but this is an old concept.

In 2018, the US Attorney General established a *Cyber-Digital Task Force* within the U.S. Department of Justice, to evaluate the impact that advances in technology have had on law enforcement's ability to keep citizens safe.

I have just read the excellent *Report of the Attorney General's Cyber Digital Task Force*.

According to the report, the acceptance of *anonymity enhanced cryptocurrencies (AEC)* such as Monero, Dash, and Zcash—by MSBs and darknet marketplaces, has increased the use of this type of virtual currency.

Because AECs use non-public or private blockchains, use of these cryptocurrencies may undermine the AML/CFT controls used to detect suspicious activity by MSBs and other financial institutions, and may limit or even negate a business's ability to conduct AML/CFT checks on customer activity and to satisfy BSA requirements.

Some AECs, however, offer features, such as public view keys, that potentially can facilitate the fulfilment of AML/CFT obligations, depending upon the implementation of such features.

The Department considers the use of AECs to be a high-risk activity that is indicative of possible criminal conduct. In most circumstances, the Department does not liquidate seized or forfeited AECs, as doing so allows them to re-enter the stream of commerce for potential future criminal use. Companies that choose to offer AEC products should consider the increased risks of money laundering and financing of criminal activity and should evaluate whether it is possible to adopt appropriate AML/CFT measures to address such risks.

AECs are often exchanged for other virtual assets like bitcoin, which may indicate a cross-virtual-asset layering technique for users attempting to conceal criminal behavior. This practice is commonly referred to as *"chain hopping"*.

*"Mixers" and "tumblers"* are entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination.

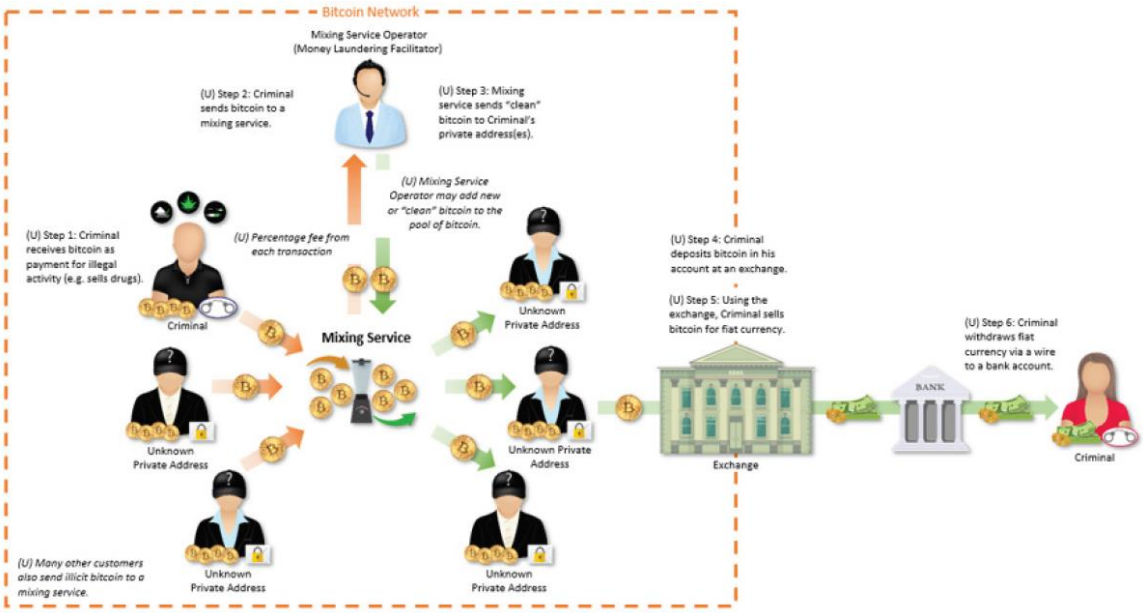
For a fee, a customer can send cryptocurrency to a specific address that is controlled by the mixer.

The mixer then commingles this cryptocurrency with funds received from other customers before sending it to the requested recipient address.

Websites or companies offering mixing or tumbling services are engaged in money transmission, and therefore are MSBs subject to the BSA and other similar international regulations.

In addition to facing BSA liability for failing to register, conduct AML procedures, or collect customer identification, operators of these services can be criminally liable for money laundering because these mixers and tumblers are designed specifically to conceal or disguise the nature, the location, the source, the ownership, or the control of a financial transaction.

Chain hopping is frequently used by individuals who are laundering proceeds of virtual currency thefts. Chain hopping is often viewed as a potential way to obfuscate the trail of virtual currency by shifting the trail of transactions from the blockchain of one virtual currency to the blockchain of another virtual currency.




Because of the global and cross-border nature of transactions involving virtual assets, the lack of consistent AML/ CFT regulation and supervision over VASPs across jurisdictions—and the complete absence of such regulation and supervision in certain parts of the world—is detrimental to the safety and stability of the international financial system.

This inconsistency also impedes law enforcement's ability to investigate, prosecute, and prevent criminal activity involving or facilitated by virtual assets.

For example, illicit financial flows denominated in virtual assets may move to companies and exchanges in jurisdictions where authorities lack regulatory frameworks requiring the generation and retention of records necessary to support investigations.

Read more at Number 13 below.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

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

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

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

*Number 1 (Page 14)*

## The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails

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

*Number 2 (Page 17)*

## New cyberattacks targeting U.S. elections

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

*Number 3 (Page 22)*

## Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

THE UNITED STATES DEPARTMENT of JUSTICE

*Number 4 (Page 28)*

## Worldwide Threats to the Homeland

Christopher Wray, Director, Federal Bureau of Investigation, Statement Before the House Homeland Security Committee, Washington, D.C.

*Number 5 (Page 39)*

## UEFI Secure Boot Customization

National Security Agency, Cybersecurity Technical Report

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

*Number 6 (Page 42)*

## INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020

*Number 7 (Page 48)*

## Homeland Threat Assessment, October 2020

*Number 8 (Page 51)*

## Cloud Security: The way forward?

*Number 9 (Page 52)*

## Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development: A Shared Vision for Driving Technological Breakthroughs in Artificial Intelligence

*Number 10 (Page 55)*

## EBA launches EU-wide transparency exercise

*Number 11 (Page 59)*

## Report on risks and vulnerabilities in the EU financial system

*Number 12 (Page 63)*

## FOREIGN ACTORS AND CYBERCRIMINALS LIKELY TO SPREAD DISINFORMATION REGARDING 2020 ELECTION RESULTS


*Number 13 (Page 66)*

## Report of the Attorney General's Cyber Digital Task Force

*Number 14 (Page 72)*

## UK National Sentenced to Prison for Role in "The Dark Overlord" Hacking Group

Defendant Conspired to Steal Sensitive Personally Identifying Information from Victim Companies and Release those Records on Criminal Marketplaces unless Victims Paid Bitcoin Ransoms

THE UNITED STATES DEPARTMENT of JUSTICE

*Number 15 (Page 74)*

## Russian Hacker Sentenced to Over 7 Years in Prison for Hacking into Three Bay Area Tech Companies

THE UNITED STATES ATTORNEY'S OFFICE
NORTHERN DISTRICT of CALIFORNIA

*Number 1*

## The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails

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

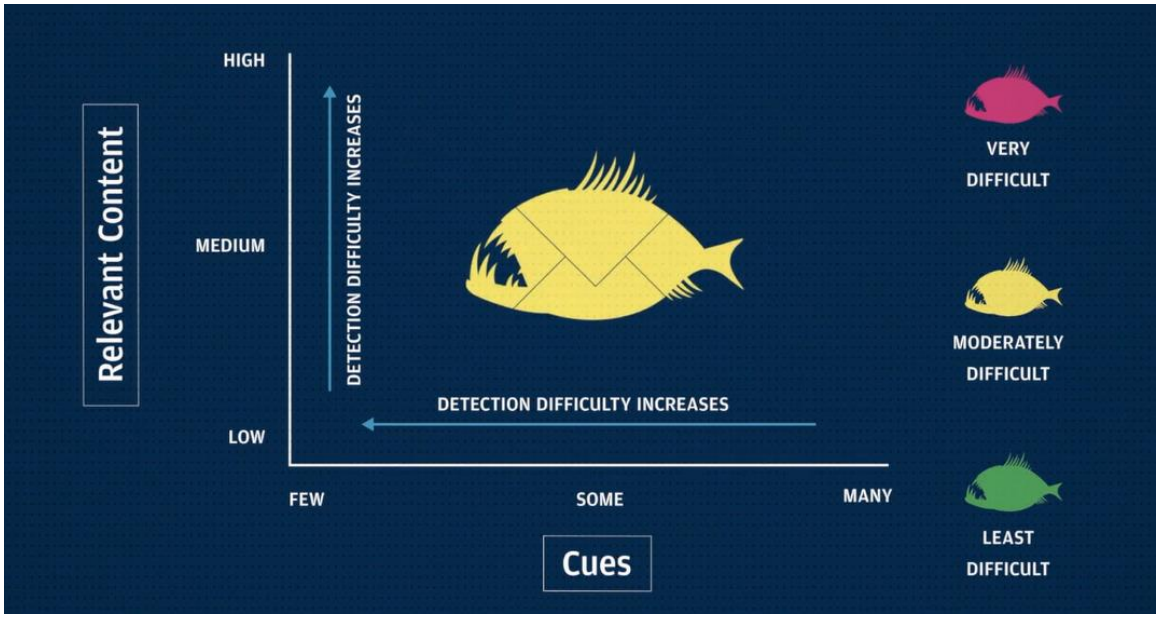
Researchers at the National Institute of Standards and Technology (NIST) have developed a new method called the Phish Scale that could help organizations better train their employees to avoid a particularly dangerous form of cyberattack known as phishing.

By 2021, global cybercrime damages will cost $6 trillion annually, up from $3 trillion in 2015, according to estimates from the 2020 Official Annual Cybercrime Report by Cybersecurity Ventures.

One of the more prevalent types of cybercrime is phishing, a practice where hackers send emails that appear to be from an acquaintance or trustworthy institution.

A phishing email (or phish) can tempt users with a variety of scenarios, from the promise of free gift cards to urgent alerts from upper management.

If users click on links in a phishing email, the links can take them to websites that could deposit dangerous malware into the organization's computers.




Many organizations have phishing training programs in which employees receive fake phishing emails generated by the employees' own organization

to teach them to be vigilant and to recognize the characteristics of actual phishing emails.

Chief information security officers (CISOs), who often oversee these phishing awareness programs, then look at the click rates, or how often users click on the emails, to determine if their phishing training is working.

Higher click rates are generally seen as bad because it means users failed to notice the email was a phish, while low click rates are often seen as good.

However, numbers alone don't tell the whole story. "The Phish Scale is intended to help provide a deeper understanding of whether a particular phishing email is harder or easier for a particular target audience to detect," said NIST researcher Michelle Steves. The tool can help explain why click rates are high or low.

The Phish Scale uses a rating system that is based on the message content in a phishing email. This can consist of cues that should tip users off about the legitimacy of the email and the premise of the scenario for the target audience, meaning whichever tactics the email uses would be effective for that audience. These groups can vary widely, including universities, business institutions, hospitals and government agencies.

The new method uses five elements that are rated on a 5-point scale that relate to the scenario's premise. The overall score is then used by the phishing trainer to help analyze their data and rank the phishing exercise as low, medium or high difficulty.

The significance of the Phish Scale is to give CISOs a better understanding of their click-rate data instead of relying on the numbers alone.

A low click rate for a particular phishing email can have several causes: The phishing training emails are too easy or do not provide relevant context to the user, or the phishing email is similar to a previous exercise. Data like this can create a false sense of security if click rates are analyzed on their own without understanding the phishing email's difficulty.

By using the Phish Scale to analyze click rates and collecting feedback from users on why they clicked on certain phishing emails, CISOs can better understand their phishing training programs, especially if they are optimized for the intended target audience.

The Phish Scale is the culmination of years of research, and the data used for it comes from an "operational" setting, very much the opposite of a laboratory experiment with controlled variables. "As soon as you put people into a laboratory setting, they know," said Steves. "They're outside

of their regular context, their regular work setting, and their regular work responsibilities. That is artificial already. Our data did not come from there."

This type of operational data is both beneficial and in short supply in the research field. "We were very fortunate that we were able to publish that data and contribute to the literature in that way," said NIST researcher Kristen Greene.

As for next steps, Greene and Steves say they need even more data. All of the data used for the Phish Scale came from NIST. The next step is to expand the pool and acquire data from other organizations, including nongovernmental ones, and to make sure the Phish Scale performs as it should over time and in different operational settings. "We know that the phishing threat landscape continues to change," said Greene. "Does the Phish Scale hold up against all the new phishing attacks? How can we improve it with new data?" NIST researcher Shaneé Dawkins and her colleagues are now working to make those improvements and revisions.

Detailed steps for the DIY tool are listed in the methods section of the paper.

In the meantime, the Phish Scale provides a new way for computer security professionals to better understand their organization's phishing click rates, and ultimately improve training so their users are better prepared against real phishing scenarios.

Information on the Phish Scale is published in a research article appearing in the current issue of the Journal of Cybersecurity. You may visit: https://academic.oup.com/cybersecurity/article/6/1/tyaa009/5905453

For additional background information about the development of the Phish Scale, you may visit: https://csrc.nist.gov/projects/usable-cybersecurity/research-areas/phishing

*Number 2*

## New cyberattacks targeting U.S. elections

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

In recent weeks, Microsoft has detected cyberattacks targeting people and organizations involved in the upcoming presidential election, including unsuccessful attacks on people associated with both the Trump and Biden campaigns, as detailed below.

We have and will continue to defend our democracy against these attacks through notifications of such activity to impacted customers, security features in our products and services, and legal and technical disruptions.

The activity we are announcing today makes clear that foreign activity groups have stepped up their efforts targeting the 2020 election as had been anticipated, and is consistent with what the U.S. government and others have reported.

We also report here on attacks against other institutions and enterprises worldwide that reflect similar adversary activity.

We have observed that:

- Strontium, operating from Russia, has attacked more than 200 organizations including political campaigns, advocacy groups, parties and political consultants

- Zirconium, operating from China, has attacked high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community

- Phosphorus, operating from Iran, has continued to attack the personal accounts of people associated with the Donald J. Trump for President campaign

The majority of these attacks were detected and stopped by security tools built into our products.

We have directly notified those who were targeted or compromised so they can take action to protect themselves. We are sharing more about the details of these attacks today, and where we've named impacted customers, we're doing so with their support.

What we've seen is consistent with previous attack patterns that not only target candidates and campaign staffers but also those they consult on key issues.

These activities highlight the need for people and organizations involved in the political process to take advantage of free and low-cost security tools to protect themselves as we get closer to election day.

At Microsoft, for example, we offer AccountGuard threat monitoring, Microsoft 365 for Campaigns and Election Security Advisors to help secure campaigns and their volunteers.

More broadly, these attacks underscore the continued importance of work underway at the United Nations to protect cyberspace and initiatives like the Paris Call for Trust and Security in Cyberspace.

*Strontium*

Strontium is an activity group operating from Russia whose activities Microsoft has tracked and taken action to disrupt on several previous occasions.

It was also identified in the Mueller report as the organization primary responsible for the attacks on the Democratic presidential campaign in 2016.

Microsoft's Threat Intelligence Center (MSTIC) has observed a series of attacks conducted by Strontium between September 2019 and today.

Similar to what we observed in 2016, Strontium is launching campaigns to harvest people's log-in credentials or compromise their accounts, presumably to aid in intelligence gathering or disruption operations.

Many of Strontium's targets in this campaign, which has affected more than 200 organizations in total, are directly or indirectly affiliated with the upcoming U.S. election as well as political and policy-related organizations in Europe.

These targets include:

- U.S.-based consultants serving Republicans and Democrats;

- Think tanks such as The German Marshall Fund of the United States and advocacy organizations;

- National and state party organizations in the U.S.; and

- The European People's Party and political parties in the UK.

Others that Strontium targeted recently include businesses in the entertainment, hospitality, manufacturing, financial services and physical security industries.

Microsoft has been monitoring these attacks and notifying targeted customers for several months, but only recently reached a point in our investigation where we can attribute the activity to Strontium with high confidence.

MSTIC's investigation revealed that Strontium has evolved its tactics since the 2016 election to include new reconnaissance tools and new techniques to obfuscate their operations.

In 2016, the group primarily relied on spear phishing to capture people's credentials.

In recent months, it has engaged in brute force attacks and password spray, two tactics that have likely allowed them to automate aspects of their operations.

Strontium also disguised these credential harvesting attacks in new ways, running them through more than 1,000 constantly rotating IP addresses, many associated with the Tor anonymizing service.

Strontium even evolved its infrastructure over time, adding and removing about 20 IPs per day to further mask its activity.

We are also working with our customers to assist them in proactively hunting for these types of threats in their environments and have published additional detail and guidance on Strontium activity.

You may visit:
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

*Zirconium*

Zirconium, operating from China, has attempted to gain intelligence on organizations associated with the upcoming U.S. presidential election. We've detected thousands of attacks from Zirconium between March 2020 and September 2020 resulting in nearly 150 compromises. Its targets have included individuals in two categories.

First, the group is targeting people closely associated with U.S. presidential campaigns and candidates.

For example, it appears to have indirectly and unsuccessfully targeted the Joe Biden for President campaign through non-campaign email accounts belonging to people affiliated with the campaign.

The group has also targeted at least one prominent individual formerly associated with the Trump Administration.

Second, the group is targeting prominent individuals in the international affairs community, academics in international affairs from more than 15 universities, and accounts tied to 18 international affairs and policy organizations including the Atlantic Council and the Stimson Center.

Zirconium is using what are referred to as web bugs, or web beacons, tied to a domain they purchased and populated with content. The actor then sends the associated URL in either email text or an attachment to a targeted account.

Although the domain itself may not have malicious content, the web bug allows Zirconium to check if a user attempted to access the site. For nation-state actors, this is a simple way to perform reconnaissance on targeted accounts to determine if the account is valid or the user is active.

*Phosphorus*

Phosphorus is an activity group operating from Iran that MSTIC has tracked extensively for several years.

The actor has operated espionage campaigns targeting a wide variety of organizations traditionally tied to geopolitical, economic or human rights interests in the Middle East region.

Microsoft has previously taken legal action against Phosphorus' infrastructure and its efforts late last year to target a U.S. presidential campaign.

Last month, as part of our ongoing efforts to disrupt Phosphorus activity, Microsoft was again given permission by a federal court in Washington D.C. to take control of 25 new internet domains used by the Phosphorus. Microsoft has since taken control of these domains.

To date, we have used this method to take control of 155 Phosphorus domains.

Since our last disclosure, Phosphorus has attempted to access the personal or work accounts of individuals involved directly or indirectly with the U.S. presidential election.

Between May and June 2020, Phosphorus unsuccessfully attempted to log into the accounts of administration officials and Donald J. Trump for President campaign staff.

*Bolstering Cybersecurity*

We disclose attacks like these because we believe it's important the world knows about threats to democratic processes.

It is critical that everyone involved in democratic processes around the world, both directly or indirectly, be aware of these threats and take steps to protect themselves in both their personal and professional capacities.

We report on nation-state activity to our customers and more broadly when material to the public, regardless of the actor's nation-state affiliation.

We are taking extra steps to protect customers involved in elections, government and policymaking.

We'll continue to disclose additional significant activity in our efforts to defend democracy.

We also believe more federal funding is needed in the U.S. so states can better protect their election infrastructure.

While the political organizations targeted in attacks from these actors are not those that maintain or operate voting systems, this increased activity related to the U.S. electoral process is concerning for the whole ecosystem.

We continue to encourage state and local election authorities in the U.S. to harden their operations and prepare for potential attacks.

But as election security experts have noted, additional funding is still needed, especially as resources are stretched to accommodate the shift in COVID-19-related voting.

We encourage Congress to move forward with additional funding to the states and provide them with what they need to protect the vote and ultimately our democracy.

*Number 3*

## Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

THE UNITED STATES DEPARTMENT of JUSTICE

In August 2019 and August 2020, a federal grand jury in Washington, D.C., returned two separate indictments charging five computer hackers, all of whom were residents and nationals of the People's Republic of China (PRC), with computer intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong.

The intrusions, which security researchers have tracked using the threat labels "APT41," "Barium," "Winnti," "Wicked Panda," and "Wicked Spider," facilitated the theft of source code, software code signing certificates, customer account data, and valuable business information.

These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "crypto-jacking" schemes, the latter of which refers to the group's unauthorized use of victim computers to "mine" cryptocurrency.

Also in August 2020, the same federal grand jury returned a third indictment charging two Malaysian businessmen who conspired with two of the Chinese hackers to profit from computer intrusions targeting the video game industry in the United States and abroad.

Shortly thereafter, the U.S. District Court for the District of Columbia issued arrest warrants for the two businessmen.

On Sept. 14, 2020, pursuant to a provisional arrest request from the United States with a view to their extradition, Malaysian authorities arrested them in Sitiawan. The department appreciates the significant cooperation and assistance provided by the Government of Malaysia, including the Attorney General's Chambers of Malaysia and the Royal Malaysia Police.

In addition to arrest warrants for all of the charged defendants, in September 2020, the U.S. District Court for the District of Columbia issued seizure warrants that resulted in the recent seizure of hundreds of accounts, servers, domain names, and command-and-control (C2") "dead drop" web pages used by the defendants to conduct their computer intrusion offenses.

The FBI executed the warrants in coordination with other actions by several private-sector companies, which included disabling numerous accounts for violations of the companies' terms of service. In addition, in partnership with the department, Microsoft developed and implemented technical measures to block this threat actor from accessing victims' computer systems.

The actions by Microsoft were a significant part of the overall effort to deny the defendants continued access to hacking infrastructure, tools, accounts, and command and control domain names. In coordination with today's announcement, the FBI has also released a Liaison Alert System (FLASH) report that contains critical, relevant technical information collected by the FBI for use by specific private-sector partners.

"The department of Justice has used every tool available to disrupt the illegal computer intrusions and cyberattacks by these Chinese citizens," said Deputy Attorney General Jeffrey A. Rosen. "Regrettably, the Chinese communist party has chosen a different path of making China safe for cybercriminals so long as they attack computers outside China and steal intellectual property helpful to China."

"Today's charges, the related arrests, seizures of malware and other infrastructure used to conduct intrusions, and coordinated private sector protective actions reveal yet again the department's determination to use all of the tools at its disposal and to collaborate with the private sector and nations who support the rule of law in cyberspace," said Assistant Attorney General John C. Demers. "This is the only way to neutralize malicious nation state cyber activity."

"Today's announcement demonstrates the ramifications faced by the hackers in China but it is also a reminder to those who continue to deploy malicious cyber tactics that we will utilize every tool we have to administer justice," said FBI Deputy Director David Bowdich. "The arrests in Malaysia are a direct result of partnership, cooperation and collaboration. As the cyber threat continues to evolve larger than any one agency can address, the FBI remains committed to being an indispensable partner to our federal, international and private sector partners to stop rampant cyber crime and hold those carrying out these kind of actions accountable."

"The scope and sophistication of the crimes in these unsealed indictments is unprecedented. The alleged criminal scheme used actors in China and Malaysia to illegally hack, intrude and steal information from victims worldwide," said Michael R. Sherwin, Acting U.S. Attorney for the District of Columbia. "As set forth in the charging documents, some of these criminal actors believed their association with the PRC provided them free license to hack and steal across the globe. This scheme also contained a new and troubling cyber-criminal component – the targeting and utilization of gaming platforms to both defraud video game companies and launder illicit proceeds."

"The actions announced today reflect a years-long commitment by the FBI Washington Field Office to pursue the perpetrators of the computer intrusion campaigns described in the indictments, and to bring those perpetrators to justice," said Acting Assistant Director in Charge James A. Dawson, FBI Washington Field Office. "This case demonstrates the FBI's dedication to pursuing these criminals no matter where they are, and to whom they may be connected."

The August 2019 indictment charged Zhang Haoran, 35, and Tan Dailin, 35, with 25 counts of conspiracy, wire fraud, aggravated identity theft, money laundering, and violations of the Computer Fraud and Abuse Act ("CFAA"). The indictment charged Zhang and Tan with participating in a "Computer Hacking Conspiracy," which targeted high-technology and similar organizations.

The indictment also charged that, as an additional way to make money, Zhang and Tan participated in a "Video Game Conspiracy," through which Zhang and Tan, together with others, sought to make money by hacking video game companies, obtaining and otherwise generating digital items of value (e.g., video game currency), and then selling such items for profit.

In several instances, they used their unauthorized access to gaming company networks take action against other unrelated groups engaged in the same fraudulent generation of gaming artifacts, thereby attempting to eliminate the criminal competition.

One of the August 2020, indictments charged Jiang Lizhi, 35, Qian Chuan, 39, and Fu Qiang, 37, with nine counts of racketeering conspiracy, conspiracy to violate the CFAA, substantive violations of the CFAA, access device fraud, identity theft, aggravated identity theft, and money laundering.

The racketeering conspiracy pertained to the three defendants' conducting the affairs of Chengdu 404 Network Technology ("Chengdu 404"), a PRC company, through a pattern of racketeering activity involving computer

intrusion offenses affecting over 100 victim companies, organizations, and individuals in the United States and around the world, including in Australia, Brazil, Chile, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Singapore, South Korea, Taiwan, Thailand, and Vietnam.

The defendants also compromised foreign government computer networks in India and Vietnam, and targeted, but did not compromise, government computer networks in the United Kingdom.

In one notable instance, the defendants conducted a ransomware attack on the network of a non-profit organization dedicated to combating global poverty.

The defendants associated with Chengdu 404 employed sophisticated hacking techniques to gain and maintain access to victim computer networks. One example was the defendants' use of "supply chain attacks," in which the hackers compromised software providers and then modified the providers' code to facilitate further intrusions against the software providers' customers.

Another example was the hackers' use of C2 "dead drops," which are seemingly legitimate web pages that the hackers created, but which were surreptitiously encoded instructions to their malware. However, they also employed publicly available exploits and tools, including the following common vulnerabilities and exposures ("CVE"): CVE-2019-19781, CVE-2019-11510, CVE-2019-16920, CVE-2019-16278, CVE-2019-1652/CVE-2019-1653, and CVE-2020-10189.

The second August 2020 indictment charged Wong Ong Hua, 46, and Ling Yang Ching, 32, both Malaysian nationals and residents, with 23 counts of racketeering, conspiracy, identity theft, aggravated identity theft, access device fraud, money laundering, violations of the CFAA, and falsely registering domain names.

The indictment alleged that Wong and Ling conducted the affairs of Sea Gamer Mall, a Malaysian company founded by Wong, through a pattern of racketeering activity involving computer intrusion offenses targeting the video game industry in the United States, France, Japan, Singapore, and South Korea.

The indictment alleged that Wong and Ling worked with various hackers, including Zhang and Tan, to profit from the hackers' criminal computer intrusions at video game companies.

The indictment against Zhang and Tan charges the defendants with two counts of conspiracy to commit computer fraud, which carries a maximum

sentence of five years in prison; two counts of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; five counts of wire fraud, which carries a maximum sentence of 20 years in prison; nine counts of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; four counts of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; two counts of aggravated identity theft, which carries a mandatory sentence of two years in prison; and one count of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment against Jiang, Qian, and Fu charges the defendants with one count of racketeering conspiracy, which carries a maximum sentence of 20 years in prison; one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison; one count of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; one count of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; one count of threatening to damage a protected computer, which carries a maximum sentence of five years in prison; one count of access device fraud, which carries a maximum sentence of 10 years in prison; one count of identity theft, which carries a maximum sentence of five years in prison; one count of aggravated identity theft, which carries a mandatory sentence of two years in prison; and one count of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment against Wong and Ling charges the defendants with one count of racketeering conspiracy, which carries a maximum sentence of 20 years in prison; one count of racketeering, which carries a maximum sentence of 20 years in prison; three counts of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; five counts of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; five counts of furthering fraud by unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; two counts of access device fraud, which carries a maximum sentence of 10 years in prison; two counts of identity theft, which carries a maximum sentence of five years in prison; one count of aggravated identity theft, which carries a mandatory sentence of two years in prison; and three counts of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment also alleges false registration of domain names, which would increase the maximum sentence of imprisonment for money laundering to 27 years; the maximum sentence of imprisonment for unlawful access to a protected computer to 10 years instead of five years; the maximum sentence of imprisonment for intentional damage to a protected computer to 17 years instead of 10 years; and the mandatory

sentence of imprisonment for aggravated identity theft to four years instead of two years.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only; any sentencing's of the defendants will be determined by the assigned judge.

The investigation was conducted jointly by the U.S. Attorney's Office for the District of Columbia, the National Security Division of the Department of Justice, and the FBI's Washington Field Office.

The FBI's Cyber Division assisted in the investigation and, along with FBI's Cyber Assistant Legal Attachés and Legal Attachés in countries around the world, provided essential support. Numerous victims cooperated and provided valuable assistance in the investigation.

The department is also grateful to Microsoft, including Microsoft's Threat Intelligence Center (MSTIC) and Digital Crimes Unit (DCU), to Google, including its Threat Analysis Group (TAG), to Facebook, and to Verizon Media, including its Paranoids Advanced Cyber Threats Team, for the assistance they provided in this investigation.

Assistant U.S. Attorney Demian Ahn of the District of Columbia, Assistant U.S. Attorney Tejpal Chawla of the District of Columbia, and Trial Attorney Evan Turgeon of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case.

The Justice Department's Office of International Affairs provided critical assistance.

The details contained in the charging document are allegations. The defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

To read more: https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

*Number 4*

## Worldwide Threats to the Homeland

Christopher Wray, Director, Federal Bureau of Investigation, Statement Before the House Homeland Security Committee, Washington, D.C.

Good afternoon, Chairman Thompson, Ranking Member Rogers, and members of the committee. Thank you for the opportunity to appear before you today to discuss the current threats to the United States homeland. I am pleased to be here representing the nearly 37,000 dedicated men and women of the FBI.

While the COVID-19 pandemic has presented unique and unprecedented challenges to the FBI workforce, I am proud of their dedication to our mission of protecting the American people and upholding the Constitution. Hostile foreign actors, violent extremists, and opportunistic criminal elements have seized upon this environment. As a result, we are facing aggressive and sophisticated threats on many fronts.

Whether it is terrorism now moving at the speed of social media, or the increasingly blended threat of cyber intrusions and state-sponsored economic espionage, or malign foreign influence and interference or active shooters and other violent criminals threatening our communities, or the scourge of opioid trafficking and abuse, or hate crimes, human trafficking, crimes against children—the list of threats we are worried about is not getting any shorter, and none of the threats on that list are getting any easier.

## Counterterrorism

Preventing terrorist attacks remains the FBI's top priority. However, the threat posed by terrorism—both international terrorism (IT) and domestic violent extremism—has evolved significantly since 9/11.

The greatest threat we face in the homeland is that posed by lone actors radicalized online who look to attack soft targets with easily accessible weapons.

We see this lone actor threat manifested both within domestic violent extremists (DVEs) and homegrown violent extremists (HVEs), two distinct sets of individuals that generally self-radicalize and mobilize to violence on their own.

DVEs are individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government sentiment. HVEs are individuals who have been radicalized primarily in the United States, and who are inspired by, but not receiving individualized direction from, foreign terrorist organizations (FTOs).

Many of these violent extremists, both domestic and international, are motivated and inspired by a mix of ideological, sociopolitical, and personal grievances against their targets, which recently have more and more included large public gatherings, houses of worship, and retail locations.

Lone actors, who by definition are not likely to conspire with others regarding their plans, are increasingly choosing these soft, familiar targets for their attacks, limiting law enforcement opportunities for detection and disruption ahead of their action.

DVEs pose a steady and evolving threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism—such as perceptions of government or law enforcement overreach, sociopolitical conditions, racism, anti-Semitism, Islamophobia, misogyny, and reactions to legislative actions—remain constant.

As stated above, the FBI is most concerned about lone offender attacks, primarily shootings, as they have served as the dominant lethal mode for domestic violent extremist attacks. More deaths were caused by DVEs than international terrorists in recent years. In fact, 2019 was the deadliest year for domestic extremist violence since the Oklahoma City bombing in 1995.

The top threat we face from domestic violent extremists stems from those we identify as racially/ethnically motivated violent extremists (RMVE). RMVEs were the primary source of ideologically motivated lethal incidents and violence in 2018 and 2019 and have been considered the most lethal of all domestic extremists since 2001. Of note, the last three DVE attacks, however, were perpetrated by anti-government violent extremists.

The spate of attacks we saw in 2019 underscore the continued threat posed by DVEs and perpetrators of hate crimes. The FBI works proactively to prevent acts of domestic terrorism and hate crimes. For example, in November 2019, the Denver Joint Terrorism Task Force arrested Richard Holzer on federal charges of attempting to obstruct religious exercise by force using explosives.

This disruption is just one example of the strength of our Domestic Terrorism-Hate Crimes (DT-HC) Fusion Cell. Our Counterterrorism

Division (CTD) and Criminal Division (CID), working together, were able to prevent a potential terrorist attack before it occurred and, for the first time in recent history, make a proactive arrest on a hate crimes charge.

Through the DT-HC Fusion Cell, subject-matter experts from both CTD and CID work in tandem to innovatively use investigative tools and bring multiple perspectives to bear in combating the intersecting threats of domestic terrorism and hate crimes, preventing attacks and providing justice to victims.

We recognize that the FBI must be aware not just of the domestic violent extremism threat, but also of threats emanating from those responding violently to First Amendment-protected activities. In the past, we have seen some violent extremists respond to peaceful movements through violence rather than non-violent actions and ideas.

The FBI is involved only when responses cross from ideas and constitutionally protected protests to violence. Regardless of the specific ideology involved, the FBI requires that all domestic terrorism investigations be predicated based on activity intended to further a political or social goal, wholly or in part involving force, coercion, or violence, in violation of federal law.

HVEs and FTOs have posed a persistent threat to the nation and to U.S. interests abroad, while their tradecraft, tactics, and target sets have evolved. The international terrorism threat to the U.S. has expanded from sophisticated, externally directed FTO plots to include individual attacks carried out by HVEs who are inspired by designated terrorist organizations. As stated above, the FBI assesses HVEs are the greatest, most immediate international terrorism threat to the homeland.

These individuals are FTO-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized direction from FTOs. We, along with our law enforcement partners, face significant challenges in identifying and disrupting HVEs. This is due, in part, to their lack of a direct connection with an FTO, an ability to rapidly mobilize without law enforcement detection, and their frequent use of encrypted communications.

Many FTOs use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to violent terrorist messages. However, no group has been as successful at drawing people into its perverse ideology as ISIS, which has proven dangerously competent at employing such tools. ISIS uses traditional media platforms as well as widespread social media campaigns to propagate its ideology. Terrorists in ungoverned spaces—both physical and virtual—readily

disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause.

With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the U.S. either to travel to foreign lands or to conduct an attack on the homeland. Through the internet, terrorists anywhere overseas now have direct access to our local communities to target and recruit our citizens and spread their message faster than was imagined just a few years ago.

We remain concerned that groups such as the Islamic State of Iraq and ash-Sham (ISIS) and al Qaeda intend to carry out large-scale attacks in the U.S. Despite their territorial defeat in Iraq and Syria, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like-minded violent extremists.

The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who use messaging apps and participate in social networks. Ultimately, many of the individuals drawn to ISIS seek a sense of belonging.

Echoing other terrorist groups, ISIS has advocated lone offender attacks in Western countries. Recent ISIS videos and propaganda have specifically advocated attacks against soldiers, law enforcement, and intelligence community personnel.

As noted above, ISIS is not the only terrorist group of concern. Al Qaeda maintains its desire for large-scale, spectacular attacks. While continued counterterrorism pressure has degraded the group's Afghanistan-Pakistan senior leadership, in the near term, al Qaeda is more likely to focus on building its international affiliates and supporting small-scale, readily achievable attacks in key regions such as East and West Africa.

Simultaneously, over the last year, propaganda from al Qaeda leaders seeks to inspire individuals to conduct their own attacks in the U.S. and the West. For example, the December 2019 attack at Naval Air Station Pensacola demonstrates that groups such as al Qaeda continue to be interested in encouraging attacks on U.S. soil.

The FBI regularly reviews intelligence to ensure that we are appropriately mitigating threats from any place by any actor, and the possible violent responses and actions. We are sensitive to First Amendment-protected activities during investigative and intelligence efforts so as to ensure that our investigative actions remain aligned with our authorities and are

conducted with the appropriate protections in place for privacy and civil liberties.

As the threat to the United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our federal, state, local, tribal, and international partnerships.

The FBI uses all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence concerning the ongoing threat posed by violent extremists motivated by any ideology and desire to harm Americans and U.S. interests.

We continue to encourage information sharing, which is evidenced through our partnerships with many federal, state, local, and tribal agencies assigned to Joint Terrorism Task Forces around the country. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to help stay ahead of these threats.

## Election Security

In less than two months, Americans will exercise one of their most important and cherished freedoms: the right to vote in a democratic election. Our nation is confronting multi-faceted foreign threats seeking to both influence our national policies and public opinion and cause harm to our national dialogue.

The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

Foreign influence operations—which include covert, coercive, or corrupt actions by foreign governments to influence U.S. political sentiment or public discourse or interfere in our processes themselves—are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the internet, have changed the nature of the threat and how the FBI and its partners must address it.

This year's election cycle, amid the COVID-19 pandemic, provides ample opportunity for hostile foreign actors to conduct disinformation campaigns and foreign influence operations in an effort to mislead, sow discord, and, ultimately, undermine confidence in our democratic institutions and values and in our government's response to our current health crisis.

Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, the Foreign Influence Task Force (FITF) was established to identify and counteract malign foreign influence operations targeting the United States.

The FITF is led by the Counterintelligence Division and is composed of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions.

It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions and public confidence, develop a common operating picture, raise adversaries' costs, and reduce their overall asymmetric advantage.

The task force brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and—importantly—to be more agile.

Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had a number of instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia.

Utilizing lessons learned over the last year and half, the FITF is widening its aperture to confront malign foreign operations of China, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on election and foreign influence threats. We have also further refined our approach. All efforts are based on a three-pronged approach, which includes investigations and operations, information and intelligence sharing, and a strong partnership with the

private sector. Through the efforts of the FITF and lessons learned from both the 2016 and 2018 elections, the FBI is actively engaged in identifying, detecting, and disrupting threats to our elections and ensuring both the integrity of our democracy is preserved and the will of the American people is fulfilled.

Protecting policymakers is an important part of our efforts to combat malign foreign influence and protect our elections. As you are aware, the FBI and our interagency partners have been providing ongoing election security threat briefings to Congress. We will continue to do so throughout the fall and into the future, where there is actionable intelligence.

## Lawful Access

I want to turn now to an issue continuing to limit law enforcement's ability to disrupt these increasingly insular actors. We are all familiar with the inability of law enforcement agencies to access data, even with a lawful warrant or court order, due to "end-to-end" encryption.

Increasingly, device manufacturers and communications service providers have employed encryption in such a manner that only the users or parties to the communications can access the content of the communications or devices. This is known as end-to-end encryption.

This development has meant that, in recent years, the FBI has observed a decline in its ability to gain access to the content of both domestic and international terrorist communications due to the widespread adoption of encryption for internet traffic and the prevalence of mobile messaging apps using end-to-end encryption as default.

The FBI certainly recognizes how encryption increases the overall safety and security of the internet for users. But in fulfilling the FBI's duty to the American people to prevent acts of terrorism, this kind of end-to-end encryption creates serious challenges.

Accessing content of communications by, or data held by, known or suspected terrorists pursuant to judicially authorized, warranted legal process is getting more and more difficult.

The online, encrypted nature of radicalization, along with the insular nature of most of today's attack plotters, leaves investigators with fewer dots to connect.

As was evident in the December 9, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Alshamrani was able to

communicate using warrant-proof, end-to-end encrypted apps deliberately to evade detection by law enforcement.

It took the FBI several months to access information in his phones, during which time we did not know whether he was a lone wolf actor or whether his associates may have been plotting additional terrorist attacks.

If law enforcement loses the ability to detect criminal activity because communication between subjects—data in motion—or data held by subjects— data at rest—is encrypted in such a way making content inaccessible, even with a lawful order, our ability to protect the American people will be degraded.

Providers and law enforcement must continue to collaborate to explore possible technical solutions that would provide security and privacy to those using the internet while also contributing to the FBI's ability to complete its mission.

Despite the successes that result from the hard work of the men and women of the FBI, our Joint Terrorism Task Forces, and our partners across the government, terrorism continues to pose a persistent threat to the homeland and our interests overseas.

## China Threat

The greatest long-term threat to our nation's information and intellectual property and to our economic vitality is the counterintelligence and economic espionage threat from China. It is a threat to our economic security and by extension, to our national security.

As you have seen from the recent closure of the Chinese Consulate in Houston, this issue is not just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves.

Our adversaries' targets are our nation's core economic assets—our information and ideas, our innovation, our research and development, our technology. No country poses a broader, more severe threat to those assets than China. It is the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history. If you are an American adult, it is more likely than not that China has stolen your personal data.

In 2017, the Chinese military conspired to hack Equifax and made off with the sensitive personal information of 150 million Americans—we are talking nearly half of the American population and most American adults.

Our data is not the only thing at stake here—so is our health, livelihood, and security.

The FBI is opening a new China-related counterintelligence case approximately every 10 hours. Of the nearly 5,000 active FBI counterintelligence cases currently underway across the country, almost half are related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research. They are going after cost and pricing information, internal strategy documents, personally identifiable information—anything that can give them a competitive advantage.

It is important to be clear: This is not about the Chinese people as a whole, and certainly not about Chinese Americans as a group, but it is about the Chinese government and the Chinese Communist Party. Every year, the United States welcomes more than 100,000 Chinese students and researchers into this country.

For generations, people have journeyed from China to the United States to secure the blessings of liberty for themselves and their families—and our society is better for their contributions. So, when the FBI's refers to the threat from China, we mean the government of China and the Chinese Communist Party.

Confronting this threat effectively does not mean that we should not do business with the Chinese. It does not mean that we should not host Chinese visitors. It does not mean that we should not welcome Chinese students or coexist with China on the world stage. But it does mean that when China violates our criminal laws and international norms, we are not going to tolerate it, much less enable it.

The FBI and our partners throughout the U.S. government will hold China accountable and protect our nation's innovation, ideas, and way of life—with the help and vigilance of the American people.

## Cyber

With the advent of the COVID-19 pandemic, the nature of the cyber threat has become increasingly concerning. As more individuals telework and increasingly use the cloud, we encounter less secure networks. As a result, the scope of our cyber threats has changed, the impact has deepened, and many of the players have become more dangerous as we have become increasingly vulnerable.

We are still seeing hack after hack and breach after breach. We hear about it daily in the news.

The more we shift to the internet as the conduit and the repository for everything we use and share and manage, the more danger we are in.

Today we are worried about a wider-than-ever range of threat actors, from multinational cyber syndicates to nation-state adversaries. And we are concerned about a wider-than-ever gamut of methods continually employed in new ways, like the targeting of managed service providers—MSPs—as a way to access scores of victims by hacking just one provider.

China's Ministry of State Security (MSS) pioneered that technique and, as you saw in July, we indicted two Chinese hackers who worked with the Guangdong State Security Department of the MSS. These individuals conducted a hacking campaign lasting more than 10 years, targeting countries with high technology industries, to include the United States. The industries targeted included, among others, solar energy, pharmaceuticals, and defense.

Cyber crimes like these, directed by the Chinese government's intelligence services, threaten not only the United States but also every other country that supports fair play, international norms, and the rule of law, and they also seriously undermine China's desire to become a respected leader in world affairs.

Theft of intellectual property is not the only cyber threat presented by the People's Republic of China (PRC) government. They are also working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. All of them, and others, are working to simultaneously strengthen themselves and weaken the United States. And we are taking all these nation-state threats very seriously.

But as dangerous as nation-states are, we do not have the luxury of focusing on them alone. We also are battling the increasing sophistication of criminal groups that place many hackers on a level we used to see only among hackers working for governments.

The proliferation of malware as a service, where darkweb vendors sell sophistication in exchange for cryptocurrency, increases the difficulty of stopping what would once have been less-dangerous offenders. It can give a ring of unsophisticated criminals the tools to paralyze entire hospitals, police departments, and businesses with ransomware. Often the hackers themselves have not become much more sophisticated—but they are renting sophisticated capabilities, requiring us to up our game as we work to defeat them, too.

Hackers have not relented under the COVID-19 pandemic. On the contrary, they have attempted to compromise the computer systems of hospitals and medical centers to obtain patient financial data, medical records, and other information. In addition, such attacks on medical centers may lead to the interruption of computer networks and systems putting patients' lives at an increased risk when America faces its most dire health crisis in generations.

## Conclusion

Chairman Thompson, Ranking Member Rogers and members of the committee, thank you for the opportunity to testify today. I am now happy to answer any questions you might have.

*Number 5*

## UEFI Secure Boot Customization

National Security Agency, Cybersecurity Technical Report


Secure Boot is a boot integrity feature that is part of the Unified Extensible Firmware Interface (UEFI) industry standard.

Most modern computer systems are delivered to customers with a standard Secure Boot policy installed.

This document provides a comprehensive guide for customizing a Secure Boot policy to meet several use cases.

UEFI is a replacement for the legacy Basic Input Output System (BIOS) boot mechanism.

UEFI provides an environment common to different computing architectures and platforms.

UEFI also provides more configuration options, improved performance, enhanced interfaces, security measures to combat persistent firmware threats, and support for a wider variety of devices and form factors.

Malicious actors target firmware to persist on an endpoint.

Firmware is stored and executes from memory that is separate from the operating system and storage media.

Antivirus software, which runs after the operating system has loaded, is ineffective at detecting and remediating malware in the early-boot firmware environment that executes before the operating system.

Secure Boot provides a validation mechanism that reduces the risk of successful firmware exploitation and mitigates many published early-boot vulnerabilities.

Secure Boot is frequently not enabled due to issues with incompatible hardware and software. Custom certificates, signatures, and hashes should be utilized for incompatible software and hardware.

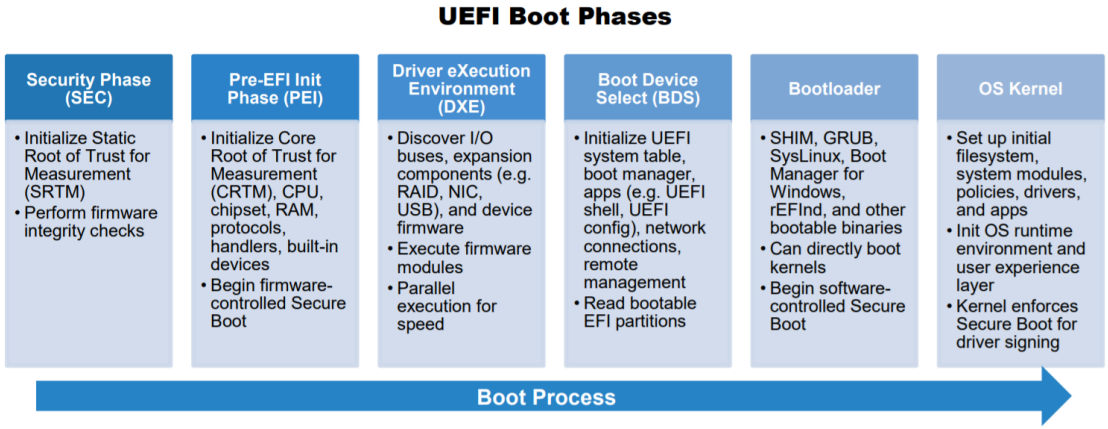



Figure 1 - An enumeration of UEFI firmware and software boot phases.

Secure Boot can be customized to meet the needs of different environments.

Customization enables administrators to realize the benefits of boot malware defenses, insider threat mitigations, and data-at-rest protections.

Administrators should opt to customize Secure Boot rather than disable it for compatibility reasons.

Customization may – depending on implementation – require infrastructures to sign their own boot binaries and drivers.

Recommendations for system administrators and infrastructure owners:

• Machines running legacy BIOS or Compatibility Support Module (CSM) should be migrated to UEFI native mode.

• Secure Boot should be enabled on all endpoints and configured to audit firmware modules, expansion devices, and bootable OS images (sometimes referred to as Thorough Mode).

• Secure Boot should be customized, if necessary, to meet the needs of organizations and their supporting hardware and software.

• Firmware should be secured using a set of administrator passwords appropriate for a device's capabilities and use case.

• Firmware should be updated regularly and treated as importantly as operating system and application updates.

• A Trusted Platform Module (TPM) should be leveraged to check the integrity of firmware and the Secure Boot configuration.

To read more: https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-SECURE-BOOT-CUSTOMIZATION-20200915.PDF/CTR-UEFI-SECURE-BOOT-CUSTOMIZATION-20200915.PDF

*Number 6*

## INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020

The IOCTA is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime.

It provides a unique law enforcement focused assessment of emerging challenges and key developments in the area of cybercrime.

We are grateful for the many contributions from our colleagues within European law enforcement community and to our partners in the private industry for their input to the report.

Combining law enforcement and private sector insights allows us to present this comprehensive overview of the threat landscape.

The data collection for the IOCTA 2020 took place during the lockdown implemented as a result of the COVID-19 pandemic.

Indeed, the pandemic prompted significant change and criminal innovation in the area of cybercrime.

Criminals devised both new modi operandi and adapted existing ones to exploit the situation, new attack vectors and new groups of victims.

The threat landscape over the last year described in the IOCTA 2020 contains many familiar main characters.

The starring roles in terms of priority threats went to the likes of social engineering, ransomware and other forms of malware.

Several interviewees captured the essence of the current state of affairs of the threat landscape by stating: cybercrime is an evolution, not a revolution.

As time passes, the cyber-element of cybercrime infiltrates nearly every area of criminal activity. Key elements mentioned in previous editions of the IOCTA that return this year merit more, rather than less, attention.

The repetition means the challenge still exists and has, in many cases, increased, underlining the need to further strengthen the resilience and response to well-known threats.

The IOCTA 2020 makes clear that the fundamentals of cybercrime are firmly rooted, but that does not mean cybercrime stands still.

Its evolution becomes apparent on closer inspection, in the ways seasoned cybercriminals refine their methods and make their artisanship accessible to others through crime as a service.

The COVID-19 crisis illustrated how criminals actively take advantage of society at its most vulnerable.

Criminals tweaked existing forms of cybercrime to fit the pandemic narrative, abused the uncertainty of the situation and the public's need for reliable information.

Across the board from social engineering to Distributed Denial of Service (DDoS) attacks and from ransomware to the distribution of child sexual abuse material (CSAM), criminals abused the crisis when the rest of society was trying to contain the situation.

The opportunistic behaviour of criminals during the pandemic, however, should not overshadow the overall threat landscape.

In many cases, COVID-19 caused an amplification of existing problems exacerbated by a significant increase in the number of people working from home.

This is perhaps most noticeable in the area of child sexual abuse and exploitation.

As in previous years, the amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has had serious consequences for the investigative capacity of law enforcement authorities.

In addition, livestreaming of child sexual abuse increased and became even more popular during the COVID-19 crisis; a recent case shows production also takes place in the EU.

Data compromise once more features as a central aspect throughout a number of threats. Both law enforcement and private sector representatives consistently report on social engineering among the top threats.

With regard to social engineering, in particular phishing, cybercriminals are now employing a more holistic strategy by demonstrating a high level of competency when exploiting tools, systems and vulnerabilities,

assuming false identities and working in close cooperation with other cybercriminals.

However, despite the trend pointing towards a growing sophistication of some criminals, the majority of social engineering and phishing attacks are successful due to inadequate security measures or insufficient awareness of users.

In particular, as attacks do not have to be necessarily refined to be successful.

The developments in the area of non-cash payment fraud over the past twelve months reflect the overall increase in sophistication and targeting of social engineering and phishing.

Fuelled by a wealth of readily available data, as well as a Cybercrime-as-a-Service (CaaS) community, it has become easier for criminals to carry out highly targeted attacks.

As a result, law enforcement and industry continue to identify well established frauds as a major threat.

Subscriber identity module (SIM) swapping is one of the new key trends this year, having caused significant losses and attracted considerable attention from law enforcement.

As a highly targeted type of social engineering attack, SIM swapping can have potentially devastating consequences for its victims, by allowing criminals to bypass text message-based (SMS) two factor authentication (2FA) measures gaining full control over their victims' sensitive accounts.

Business Email Compromise (BEC) continues to increase.

As criminals are more carefully selecting their targets, they have shown a significant understanding of internal business processes and systems' vulnerabilities.

At the same time, certain other forms of fraud have entered the spotlight due to the sheer number of victims they have generated.

The spread of online investment fraud all over Europe is not necessarily new but has generated increased law enforcement attention as victims at times lose their life savings to professional organised criminal groups that have incorporated cyber elements into their scams.

The clear majority of law enforcement respondents once again named ransomware as a top priority threat.

Although this point has been made in past editions of the IOCTA, ransomware remains one of the, if not the, most dominant threats, especially for public and private organisations within as well as outside Europe.

Considering the scale of damage that ransomware can inflict, victims also appear to be reluctant to come forward to law enforcement authorities or the public when they have been victimised, which makes it more difficult to identify and investigate such cases.

Criminals continued making their ransomware attacks increasingly targeted.

Ransomware has shown to pose a significant indirect threat to businesses and organisations, including in critical infrastructure, by targeting supply chains and third-party service providers.

Perhaps one of the most crucial developments is the new way of pressuring victims to pay by stealing and subsequently threatening to auction off victims' sensitive data.

Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases.

Criminals have converted some traditional banking Trojans into more advanced modular malware to cover a broader scope of functionality.

These evolved forms of modular malware are a top threat in the EU, especially as their adaptive and expandable nature makes them increasingly more complicated to combat effectively.

With a range of threat actors, this makes drawing general conclusions about particular threats challenging.

In areas ranging from social engineering and phishing, to ransomware and other forms of malware, law enforcement authorities witness a broad spectrum of threat actors.

These actors vary in terms of level of skill, capability and adaptability.

The top tier criminals manage to run their operations like a professional enterprise, whereas less sophisticated threat actors tend to rely on off-the-shelf materials to conduct their criminal activities.

The availability of the materials through CaaS, however, continues to make such activities accessible.

Moreover, across the board threat actors in different types of cybercrime demonstrate their resilience.

Perhaps more importantly, in areas such as the Darkweb, criminals have enhanced their cooperation and joined forces to provide a response to shared challenges.

This means they are able to make their business more robust and in particular incorporate better security solutions to ensure that law enforcement are unable to trace them.

Overall, cybercriminals are showing an improved level of operational security and proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies.

With cryptocurrencies, criminals also manage to complicate law enforcement's ability to trace payments connected to criminal activities.

To respond to the cybercrime challenges in a more effective manner, a number of key ingredients are essential.

First, information sharing is at the heart of any strategic, tactical and operational response regardless of the specific type of cybercrime.

Sharing information, which needs to be purposedriven and actionable, requires reliable coordination and cooperation from public and private partners.

At the same time, information sharing requires a legal framework and attitude that is sensitive to the timely exchange of information, which is crucial as cybercriminals can move their infrastructure within the blink of an eye.

This is particularly evident in the criminal abuse of the Darkweb, where short lifecycles of marketplaces influences law enforcement's ability to conduct investigations.

There is also the need to foster a culture of acceptance and transparency when organisations or individuals fall victim to cybercrime.

Re-victimising victims after a cyber-attack is counterproductive and a significant challenge, as law enforcement need companies and individuals who have been subject of a crime to come forward.

This can help resolve the challenges in reporting we currently face. Besides information sharing through enhanced coordination and cooperation, other key elements to include in an effective response are prevention and awareness and capacity building.

We can reduce the success rate of many forms of cybercrime by educating individuals and organisations in recognising criminal activity before they fall victim to it.

It is worth underlining the importance of the responsibility of industry in integrating security and privacy in their design as fundamental principles, instead of shaming end users as the weakest link.

Through capacity building, on the other hand, law enforcement across different crime areas will be able to understand and respond to the cyber-element of crimes.

Finally, taskforce work such as coordinating and de-conflicting law enforcement operational response, for which the Europol Joint Cybercrime Action Taskforce (J-CAT) platform is vital, continues to play a key role in the current cybercrime landscape.

The report: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

*Number 7*

## Homeland Threat Assessment, October 2020

Homeland Security

The Department of Homeland Security (DHS) is the first and last line of defense against the many threats facing our country.

Our ability to mitigate these threats is predicated on our ability to understand them and to inform the American people.

The DHS Homeland Threat Assessment (HTA) identifies the primary threats facing the United States of America at and inside our borders.

This Assessment draws upon all sources of information and expertise available to the Department, including from intelligence, law enforcement, and our operational components.

The purpose of the HTA is to provide the American people with an overview of the information collected and analyzed by DHS employees around the world and provided to the Secretary of Homeland Security.

The HTA is primarily informed by intelligence analysis prepared by the DHS Office of Intelligence and Analysis (I&A) and by the Component intelligence offices, which identified the leading security threats to the Homeland based on a review of all-source intelligence information and analysis.

Given the array of potential issues, I&A's scoped its analysis to focus on key threats covered by the intelligence elements of the Department, which expert analysts considered most likely and with the potential to significantly affect U.S. security.

The HTA was also informed by the expertise and insights of the Department's Operational Components, which assess and respond to threats on a daily basis, as well as the informed views of the DHS Office of Strategy, Policy, and Plans (PLCY), which leads threat identification and prevention activities.

This inaugural HTA presents a holistic look from across the Department and provides the American people with the most complete, transparent, and candid look at the threats facing our Homeland.

It breaks down the major threats to the Homeland in the following sections:

1. The Cyber Threat to the Homeland
2. Foreign Influence Activity in the Homeland
3. Threats to U.S. Economic Security
4. The Terrorist Threat to the Homeland
5. Transnational Criminal Organization Threats to National Security
6. Illegal Immigration to the United States
7. Natural Disasters

**OPPORTUNITY FOR CYBER ACTORS TO EXPLOIT COVID-19**

Both cybercriminals and nation-state cyber actors—motivated by profit, espionage, or disruption—will exploit the COVID-19 pandemic by targeting the U.S. healthcare and public health sector; government response entities, such as the U.S. Department of Health and Human Services and the Federal Emergency Management Agency; and the broader emergency services sector.

- Cybercriminals most likely will deploy ransomware for financial gain, whereas nation-state cyber actors might seek to capture insights into U.S. response plans and scientific information related to testing, therapeutics, and vaccine development.
- We expect that cybercriminals and nation-state cyber actors will target victims in the United States with COVID-19-themed spear-phishing e-mails, which we already have observed overseas. These e-mails appear to claim to be from official government sources, including the U.S. Centers for Disease Control and Prevention and the U.S. Department of State.

**FOREIGN INFLUENCE DEFINITIONS:**

Foreign Influence. Any covert, fraudulent, deceptive, or unlawful activity of foreign governments—or persons acting on their behalf—undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting U.S. democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives.

- Covert Influence: Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action.
- Overt Influence: Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda.
- Disinformation: A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests.
- Misinformation: Foreign use of false or misleading information. Misinformation is broader than disinformation because it targets a wide audience rather than a specific group.

To read more:
https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

*Number 8*

## Cloud Security: The way forward?

A survey completed by over 200 UK organisations, showed that moving to a cloud-based IT environment had saved them from collapse due to the increased demand for remote working availability as a result of the COVID-19 pandemic.

You may visit: https://www.centrify.com/about-us/news/press-releases/2020/cloud-adoption-has-saved-more-half-uk-businesses-covid-19

However, the pandemic has also highlighted the potential weaknesses in IT security, with more than half of the businesses polled seeing an increase in hijack attempts on employee accounts and impersonation attacks becoming harder to detect.

You may visit: https://www.mimecast.com/content/impersonation-attack/#:~:text=An%20impersonation%20attack%20is%20a,login%20credentials%20that%20attackers%20can

Further analysis from security experts has warned of the increased chance of remote workers falling victim to cyber attacks. This is largely due to inadequate security protection installed on personal devices and home broadband routers or workers becoming 'distracted' and clicking on harmful links.

The NCSC has further reading to help answer security concerns about moving to a cloud-based IT solution, guidance to help you determine how confident you can be that a cloud service is secure enough to handle your data and information to increase awareness about email security. You may visit: https://www.ncsc.gov.uk/blog-post/why-cloud-first-is-not-a-security-problem

*Number 9*

# Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development: A Shared Vision for Driving Technological Breakthroughs in Artificial Intelligence

The following declaration was released by the Governments of the United States of America and the United Kingdom of Great Britain and Northern Ireland during the September 25 inaugural meeting of the Special Relationship Economic Working Group.

*Begin Text*

Recognizing the benefits and opportunities artificial intelligence (AI) brings, and the importance of AI for our future economic growth, health and wellbeing, the protection of democratic values, and national security;

Desiring to harness AI technologies to empower our citizens, improve their quality of life, and promote a technology ecosystem that enables innovation to flourish by integrating AI into the economy;

Recognizing the value of shared best practice on public data sets to unlock AI innovation and exchanges of information on regulatory frameworks to remove barriers to innovation whilst commanding public confidence;

Recognizing the importance of collaboration in basic and early stage research and development (R&D), and the need to establish the research foundations for continued and future AI innovations and use;

Recognizing the importance of promoting trust and understanding in order to enable the adoption of AI and fully realize its potential;

Recognizing the importance of a capable R&D workforce and workforce development for AI-related technical skills, including apprenticeships, reskilling programs, computer science and STEM education — to empower and enable current and future generations of workers, and to improve the quality of life of our people;

Recognizing that public-private-partnerships bring value to and enrich the AI R&D enterprise, enhance technology commercialization, and create value for our citizens;

Building on the US-UK Science and Technology Agreement signed in September 2017, we intend to advance our shared vision and work towards an AI R&D ecosystem that embodies this approach by:

- Taking stock of and utilizing existing bilateral science and technology cooperation (e.g., the Memorandum of Understanding between the U.S. National Science Foundation and UK Research and Innovation on Research Cooperation) and multilateral cooperation frameworks;

- Recommending priorities for future cooperation, particularly in R&D areas where each partner shares strong common interest (e.g., interdisciplinary research and intelligent systems) and brings complementary challenges, regulatory or cultural considerations, or expertise to the partnerships;

- Coordinating as appropriate the planning and programming of relevant activities in these areas, including promoting researcher and student collaboration that could potentially involve national partners, the private sector, academia, and the scientific community to further our efforts by harnessing the value of public-private partnerships; and

- Promoting research and development in AI, focusing on challenging technical issues, and protecting against efforts to adopt and apply these technologies in the service of authoritarianism and repression.

We intend to establish a bilateral government-to-government dialogue on the areas identified in this vision and explore an AI R&D ecosystem that promotes the mutual wellbeing, prosperity, and security of present and future generations.

Signed in London and Washington on September 25, 2020, in two originals, in the English language.

*For the United States:*

The Honorable Michael J.K. Kratsios
Chief Technology Officer of the United States
The White House
*For the United Kingdom of Great Britain and Northern Ireland:*

The Right Honorable Alok Sharma, MP
Secretary of State

Department for Business, Energy, and Industrial Strategy
The Right Honorable Oliver Dowden, CBE MP
Secretary of State
Department for Digital, Culture, Media, and Sport

*End Text*

*Number 10*

## EBA launches EU-wide transparency exercise

The European Banking Authority (EBA) has launched its 7th annual EU-wide transparency exercise, with the objective of providing market participants with updated information on the financial conditions of EU banks as of June 2020, thus assessing the preliminary impact of the COVID-19 crisis on the sector.

The EBA expects to publish the results of this exercise at the beginning of December, along with the Risk Assessment Report.

This exercise will complement the information provided through the Spring EU-wide Transparency exercise of 8 June 2020, by disclosing data with reference date as of March and June 2020, thus shedding light on the preliminary impact of the ongoing crisis.

The EBA will release about one million data points, on average more than 7,000 data points for about 130 participating banks from 27 countries, including the United Kingdom.

The data will cover banks' capital positions, financial assets, financial liabilities, risk exposure amounts, sovereign exposures and asset quality.

The exercise will also include data on loans and advances subject to legislative and non-legislative moratoria, following the EBA Guidelines on Covid-19 measures reporting and disclosure.

## Spring 2020 EU-wide transparency exercise: Frequently Asked Questions

*1. What is a transparency exercise?*

The transparency exercise is a mean through which the EBA disseminates bank-by-bank information on a wide sample of EU banks in a consistent and comparable way.

Since its establishment in 2011, the EBA has promoted additional disclosure and transparency in the EU banking sector as a way to improve market discipline and restore confidence in EU banks.

*2. How often does the EBA release this data?*

The EBA conducts transparency exercises on an annual basis, usually in late Autumn in conjunction with the publication of the Risk Assessment Report.

*3. Why do we have a Spring exercise in 2020?*

The Spring 2020 EU-wide transparency exercise comes as an exceptional disclosure in response to the outbreak of COVID-19.

After postponing the EU-wide Stress Test to 2021, in order to allow banks to focus on and ensure continuity of their core operations, the Board of Supervisors agreed on an additional EU-wide transparency exercise to be carried out with the aim of providing updated information on banks' exposures and asset quality to market participants.

The EBA considers that the provision to market participants of continuous information on banks' exposures and asset quality is crucial, particularly in moments of increased uncertainty.

*4. How does it differ from a stress test?*

Transparency exercises are purely disclosure exercises where only supervisory reporting data on a bank by bank level is published, and no shocks are applied (as it is the case for stress tests).

Transparency exercises, just like stress tests, are conducted by the EBA on a regular basis at the EU-wide level and cover the largest EU banks at their highest level of consolidation.

Both exercises aim at promoting market and supervisory discipline and providing transparency on banks' exposures, so as to address any uncertainties that may still remain.

*5. What is the reference date of the Spring transparency exercise data?*

The reference dates for the data of the Spring 2020 Transparency exercise are September 2019 and December 2019.

*6. Does the data from transparency exercise shed light on the impact from Covid-19?*

The data included in the Spring 2020 exercise can serve a benchmark on the condition of the banking sector before the pandemic crisis and as a starting point for the analysis of the crisis impact.

The direct impact from Covid-19 on the banking sector will be more evident with the disclosure of 2020 data in the next Transparency exercises.

*7. How many banks are involved?*

The Spring 2020 EU-wide transparency exercise provides detailed bank-by-bank data for 127 banks from 27 countries of the European Union (EU) and the European Economic Area (EEA).

*8. Who will use this information?*

The information disclosed is expected to be extensively used by banks, market analysts, academics and international organizations in their assessments of EU banks, which will result in better understanding of and confidence in the EU banking sector.

*9. How is the transparency exercise related to the Risk Assessment Report (RAR)?*

The year-end EU-wide transparency exercise is usually published together with the Risk Assessment Report (RAR).

Instead, the Spring exercise is complemented with a booklet with key statistics on EU banks, which are based on a wider sample of banks.

*10.What kind of data is disclosed and which are the main changes in comparison with previous exercises?*

The disclosure templates are mostly in line with the ones used in the 2019 exercise. The most significant changes for this year's exercise derive from the disclosure of two additional templates, disclosing information related to Liabilities and exposures towards industry sectors (by NACE activities).

The templates for the Spring 2020 Sexercise cover the following areas: capital, leverage ratio, risk exposure amounts, profit and losses, assets, liabilities, market risk, credit risk, exposures to sovereign, non-performing exposures, forborne exposures and Breakdown of loans and advances to non-financial corporation.

All the templates are entirely populated with supervisory reporting data.

*11.How are capital increases, merges and acquisitions or any restructuring action on banks' balance sheets treated in the Spring 2020 EU-wide transparency exercise?*

The Spring 2020 EU-wide transparency exercise includes supervisory reporting data as of September 2019 and December 2019. Therefore, any banks' actions having an impact on their balance sheets happened after these reference dates are not considered in the exercise.

In case of major events, a footnote to the templates explains the impact of such events.

*12.In which format is the data being released?*

The EBA has developed a set of practical tools to help users navigate through the Spring 2020 EUwide transparency data.

These include interactive maps and aggregation tools, as well as a complete dataset in CSV format, which can be imported into any analytical software for analysis purposes.

The transparency dataset itself is stored in four different CSV files and shows all the bank-by-bank data contained in the transparency templates.

Each CSV file is related to a particular data category, reflecting the content of one or more transparency templates. The maps tool allows users visualizing and analysis data by country and by bank through maps.

To read more: https://eba.europa.eu/risk-analysis-and-data/eu-wide-transparency-exercise

*Number 11*

## Report on risks and vulnerabilities in the EU financial system


The outbreak of the Coronavirus has brought huge social disruptions and unprecedented economic challenges, with inevitable impact on the EU1 financial sector.

Valuation, liquidity, credit and solvency risks have increased across the board.

While liquidity positions of EU banks remained relatively strong, the EU investment fund industry faced a significant deterioration of asset liquidity in some segments combined with substantial outflows from investors in selected asset classes.

The pandemic has thus led to liquidity challenges in segments of the investment fund sector.

It has also further amplified profitability concerns for all financial sectors, and is expected to result in deteriorating asset quality in the EU banking sector. Moreover, the expected further prolonged low interest rate environment weighs on the profitability and solvency of financial institutions.

EU institutions for occupational retirement provision (IORPs) are also impacted by the pandemic and the prolonged low interest rate environment, which could lead to significant drops in the cover and funding ratios.

Uncertainties about the medium- and long term economic consequences of the COVID-19 pandemic are still very high, and lead to a fragile market environment going forward.

Financial markets are vulnerable to potential decoupling of financial market performance from underlying economic activity, raising questions about the sustainability of the market recovery.

A swift, coordinated supervisory response of the ESAs to the outbreak of the virus has contributed to address and mitigate implications on the EU financial sector, and is contributing to prevent fragmentation of the Single Market.
Usage of and dependency on information and communication technology (ICT) has further increased with the spread of the Coronavirus. Related

risks represent a key challenge for financial institutions and put sound ICT and security risk management high on the agenda.

Against this background, the Joint Committee of the ESAs advises national competent authorities (NCAs), financial institutions and market participants to take the following policy actions:

1. Given the high uncertainty regarding economic and market developments, financial institutions should be prepared for possible further market corrections and deterioration in financial market liquidity.

In this context, financial institutions and supervisors should take into account various scenarios and, for example, perform stress testing or sensitivity analyses in order to map the impact of potential shocks.

For the investment fund sector this should be complemented by continued monitoring of liquidity management tool adequacy and usage.

In addition, financial institutions cannot fully rely on their existing risk management frameworks, as they may not sufficiently take into account the unique characteristics of this crisis for managing their risks.

2. The impact of the crisis on bank asset quality is expected to be a key challenge going forward.

In the past few years, credit institutions in the EU have on average increased their exposures towards potentially riskier portfolios and, given the widespread impact of the crisis, average exposures to sectors most affected by the pandemic are high.

Banks are likely to face deteriorating asset quality with growing volumes of non-performing loans and rising cost of risk amid the prospective macroeconomic deterioration.

Banks and supervisors should properly assess the quality of loan portfolios and also consider in their preparations that widely introduced legislative and non-legislative loan moratoria, as well as further policy measures such as loan guarantee schemes, are of a temporary nature.

3. Given the overall uncertainty of the scale and duration of the crisis, it is important that the financial sector remains well-capitalised.

Financial institutions should ensure that the assessment of their capital positions is forward-looking and that it takes into account current uncertainties, following prudent dividend and other distribution policies, including variable remuneration.

At the same time, supervisors and banks should make use of the flexibility embedded in the existing regulatory framework, including to use capital and liquidity buffers to absorb losses, and thus to ensure continued lending to the economy.

4. Monetary policy responses to the crisis entail an even longer low interest rate environment. Supervisors and financial institutions need to accommodate a further prolonged "low-for-long" interest rate environment and its risks, including addressing overcapacities in the financial sector.

While low interest rates are important to support economic activity, they negatively impact bank profitability and remain the main risk for the life insurance and pension fund sector.

They contribute to the further build-up of valuation risks in securities markets through search-for-yield strategies, which underestimate risks, and have contributed to bank lending growth in riskier segments.

Notwithstanding the importance of continued lending in the crisis, banks should ensure sound lending practices and that risks are not mispriced, which should be monitored by supervisors.

5. It is key for financial institutions and their service providers to carefully manage their ICT and security risks, including when outsourcing ICT activities.

They should ensure that appropriate technologies and adequate resources are in place to address data integrity, business continuity and increasingly sophisticated cyber threats.

Institutions should also pay particular attention to a growing number and new forms of financial crime in this period of large economic turmoil.

Financial institutions should also ensure to be well-prepared for any disruptions they and their clients may face at the end of the UK's transition period agreed in the context of the UK withdrawal from the EU.

The ESAs are monitoring financial institutions' preparedness for the end of transitional period, when UK institutions will lose their passporting rights into the EU as of 1 January 2021.

Market participants should also be aware that a Free Trade Agreement (FTA) between the EU and UK that is currently being discussed would not eliminate most potential disruptions in the financial services sector, as the FTA will not address passporting rights.

Financial institutions must use the remainder of the transition period to finalise their preparations and adapt their business models accordingly.

Where relevant, the preparation should factor in situations in which no relevant equivalence decisions have been made by 31 December 2020.

To this end, financial institutions should ensure that their contingency planning minimises detriment to their customers, and should provide appropriate information to their customers regarding their preparations for the end of the transition period and availability and continuation of services offered to EU-based customers.

Financial institutions relocating from the UK to the EU need to ensure that they adhere to the establishment plans agreed with the relevant competent authorities in the EU as part of their authorisations.

Separately, it should be noted that in the area of central clearing, on 9 July 2020 the European Commission announced that a time-limited equivalence decision providing for the continued access of EU 27 institutions to UK central counterparties (CCPs) will be adopted in order to address possible financial stability risks.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/2020-67-report-on-risks-and-vulnerabilities.pdf

*Number 12*

## FOREIGN ACTORS AND CYBERCRIMINALS LIKELY TO SPREAD DISINFORMATION REGARDING 2020 ELECTION RESULTS


The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of the potential threat posed by attempts to spread disinformation regarding the results of the 2020 elections.

Foreign actors and cybercriminals could create new websites, change existing websites, and create or share corresponding social media content to spread false information in an attempt to discredit the electoral process and undermine confidence in U.S. democratic institutions.

State and local officials typically require several days to weeks to certify elections' final results in order to ensure every legally cast vote is accurately counted.

The increased use of mail-in ballots due to COVID-19 protocols could leave officials with incomplete results on election night.

Foreign actors and cybercriminals could exploit the time required to certify and announce elections' results by disseminating disinformation that includes reports of voter suppression, cyberattacks targeting election infrastructure, voter or ballot fraud, and other problems intended to convince the public of the elections' illegitimacy.

The FBI and CISA urge the American public to critically evaluate the sources of the information they consume and to seek out reliable and verified information from trusted sources, such as state and local election officials.

The public should also be aware that if foreign actors or cyber criminals were able to successfully change an election-related website, the underlying data and internal systems would remain uncompromised.

## RECOMMENDATIONS

- Seek out information from trustworthy sources, such as state and local election officials; verify who produced the content; and consider their intent.

- Verify through multiple reliable sources any reports about problems in voting or election results, and consider searching for other reliable sources before sharing such information via social media or other avenues.

- For information about final election results, rely on state and local government election officials.

- Report potential election crimes—such as disinformation about the manner, time, or place of voting—to the FBI.

- If appropriate, make use of in-platform tools offered by social media companies for reporting suspicious posts that appear to be spreading false or inconsistent information about election-related problems or results.

The FBI is responsible for investigating malign foreign influence operations and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions.

CISA is responsible for protecting the nation's critical infrastructure from physical and cyber threats.

The FBI and CISA provide services and information to uphold the security, integrity, and resiliency of the U.S. electoral processes.

## VICTIM REPORTING AND ADDITIONAL INFORMATION

The FBI encourages victims to report information concerning suspicious or criminal activity to their local field office (www.fbi.gov/contact-us/field). For additional assistance and best practices, and common terms, please visit the following websites:

Protected Voices: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

Election Crimes and Security: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security

#Protect2020: www.cisa.gov/protect2020

*Number 13*

## Report of the Attorney General's Cyber Digital Task Force

Innovation can drive a society forward. But innovation does not occur in a vacuum.

Public policy can establish background conditions that help the innovative spirit thrive—or create an environment in which that spirit is inhibited, or suppressed.

Even in societies where transformative scientific and technological advancements are achievable, public policy again plays a critical mediating role.

In the wrong hands, or without appropriate safeguards and oversight, these advancements can facilitate great human suffering.

Just ask the political enemies of authoritarian regimes that deploy surveillance tools Orwell never could have imagined.

Or, closer to home, listen to the child victims of unspeakable sexual exploitation whose images and livestreamed abuse are so easily transmitted across the internet.

Technological innovation and human flourishing are complementary concepts, but the former does not guarantee the latter.

Good public policy—and the fair and equitable enforcement of such policy—can help bring the two into alignment.

And even as too much regulation undoubtedly stifles innovation (and human flourishing, too), the absence of law's protections can endanger progress across both dimensions.

It takes careful consideration, and a deep and ongoing immersion in the facts, to understand when, and how, law should intervene.

Once law's empire has established its root in a particular domain, it requires equally careful consideration (and humility on the part of government officials) to ensure that regulation goes no further than is

required—that government action, in other words, reflects enforcement only of "those wise restraints that make us free."

*This Enforcement Framework*

In 2018, Attorney General Jeff Sessions established a Cyber-Digital Task Force within the U.S. Department of Justice to evaluate the impact that recent advances in technology have had on law enforcement's ability to keep our citizens safe.

Acknowledging the many ways in which technological advances "have enriched our lives and have driven our economy," the Attorney General also noted that "the malign use of . . . technolog[y] harms our government, victimizes consumers and businesses, and endangers public safety and national security."

The Task Force issued a comprehensive report later that year. That report identified particular threats currently confronting our society, ranging from transnational criminal enterprises' sophisticated cyber enabled schemes, to malign foreign influence operations, to efforts to compromise our nation's critical infrastructure.

The report also identified a number of emerging threats whose contours are still developing, and recommended further examination of their potential impact.

Specifically, the report recommended that "the Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use."

This Cryptocurrency Enforcement Framework represents the fruits of the Task Force's efforts.

At the outset, it bears emphasizing that distributed ledger technology, upon which all cryptocurrencies build, raises breathtaking possibilities for human flourishing.

These possibilities are rightly being explored around the globe, from within academia and industry, and from within governments— including our own.

It should be no surprise, for example, that researchers within the U.S. National Institute of Standards and Technology "have been investigating blockchain technologies at multiple levels: from use cases, applications and existing services, to protocols, security guarantees, and cryptographic mechanisms."

Or that the U.S. Department of Defense's recently-issued Digital Modernization Strategy specifically identifies blockchain technology as having "promise to provide increased effectiveness, efficiency, and security."

Or that the U.S. Food and Drug Administration recently released a detailed vision for how it plans to deploy blockchain for food safety-related purposes.

Or that—in the cryptocurrency space specifically—"the Federal Reserve is active in conducting research and experimentation related to distributed ledger technologies and the potential use cases for digital currencies," including by partnering with the Massachusetts Institute of Technology to "build and test a hypothetical digital currency oriented to central bank uses."

Without doubt, cryptocurrency represents a transformative way to store and exchange value. But as the following pages make clear, despite its relatively brief existence, this technology already plays a role in many of the most significant criminal and national security threats our nation faces.

As the Task Force has found, illicit uses of cryptocurrency typically fall into three categories:

(1) financial transactions associated with the commission of crimes;

(2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or

(3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself.

Part I of this Enforcement Framework examines in detail each of those categories. Our society is not powerless in the face of these threats.

As Part II demonstrates, the government has legal and regulatory tools available at its disposal to confront the threats posed by cryptocurrency's illicit uses.

Interagency partnership is critical for effectively leveraging those tools.

The Department of Justice has built strong working relationships with its regulatory and enforcement partners in the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the U.S. Department of the Treasury (including FinCEN, OFAC, and the IRS), among others, to enforce federal law in both its civil and criminal aspects.

We have actively participated in international regulatory and criminal enforcement efforts, as well. Those efforts are paying off.

The past year alone has witnessed the indictment and arrest of the alleged operator of the world's largest online child sexual exploitation market, involving an enforcement action that was coordinated with the disruption of that darknet market, the rescue of over 20 child victims, and the seizure of hundreds of thousands of dollars' worth of bitcoin; the largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns running into the millions of dollars involving Hamas's military wing, al-Qaeda, and ISIS; the first-ever imposition of economic sanctions for virtual-asset-related malicious cyber activity; and a novel (and successful) use of the federal securities laws to protect investors in the cryptocurrency space, resulting in the disgorgement of over $1.2 billion in ill-gotten gains in a single case. We expect these enforcement trends to continue.

This report concludes in Part III with a discussion of the ongoing challenges the government faces in cryptocurrency enforcement—particularly with respect to business models (employed by certain cryptocurrency exchanges, platforms, kiosks, and casinos), and to activity (like "mixing" and "tumbling," "chain hopping," and certain instances of jurisdictional arbitrage) that may facilitate criminal activity.


To read more: https://www.justice.gov/ag/page/file/1326061/download

**Figure 1: Systemic Attributes of Virtual Currency**

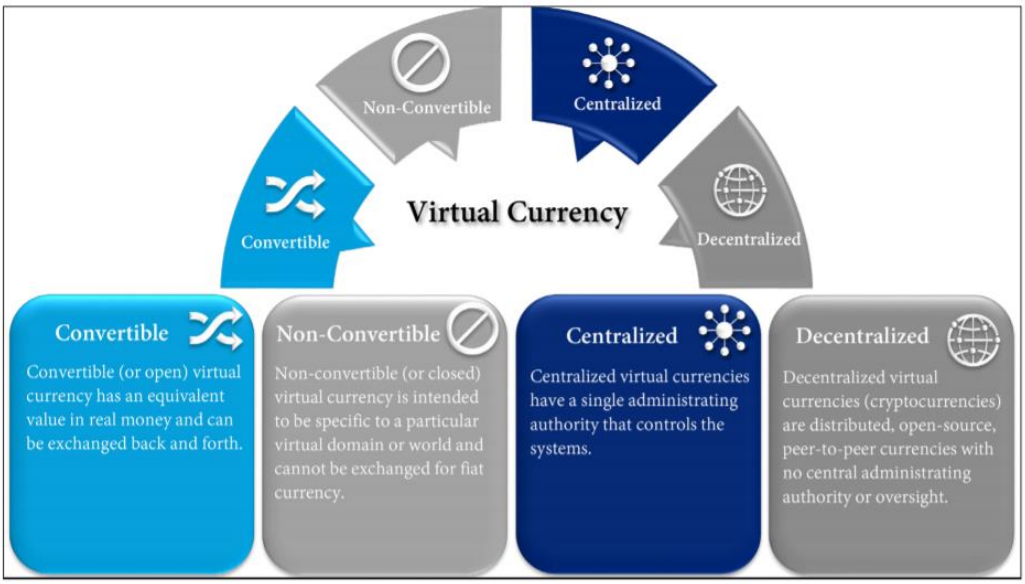



**Figure 2: Anatomy of a Cryptocurrency Transaction**

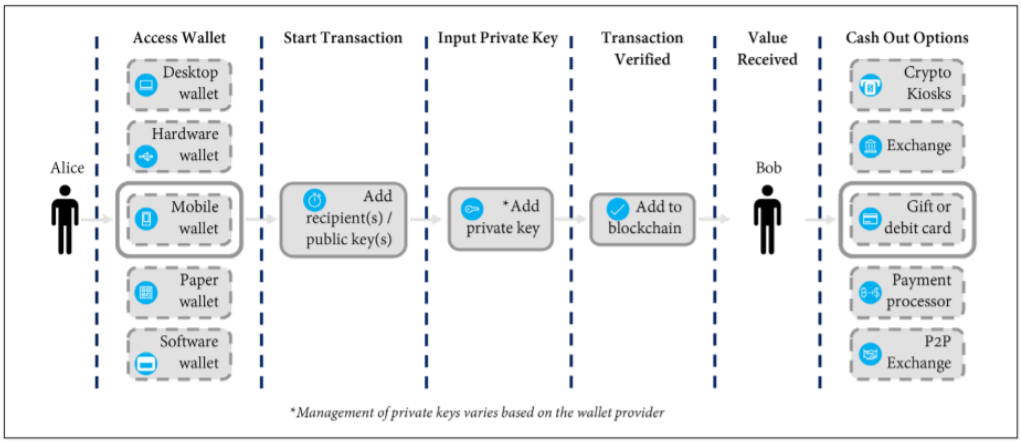
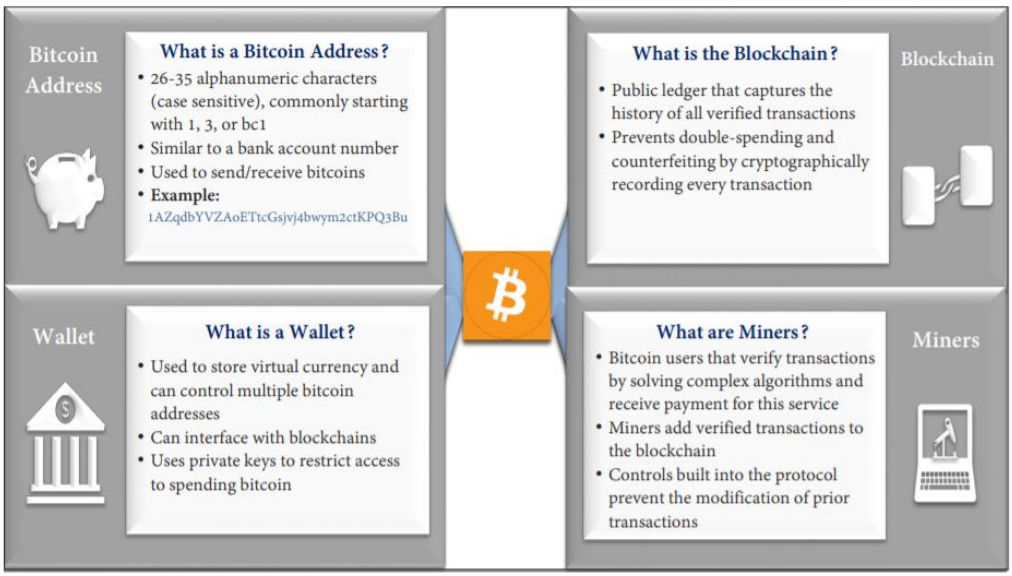
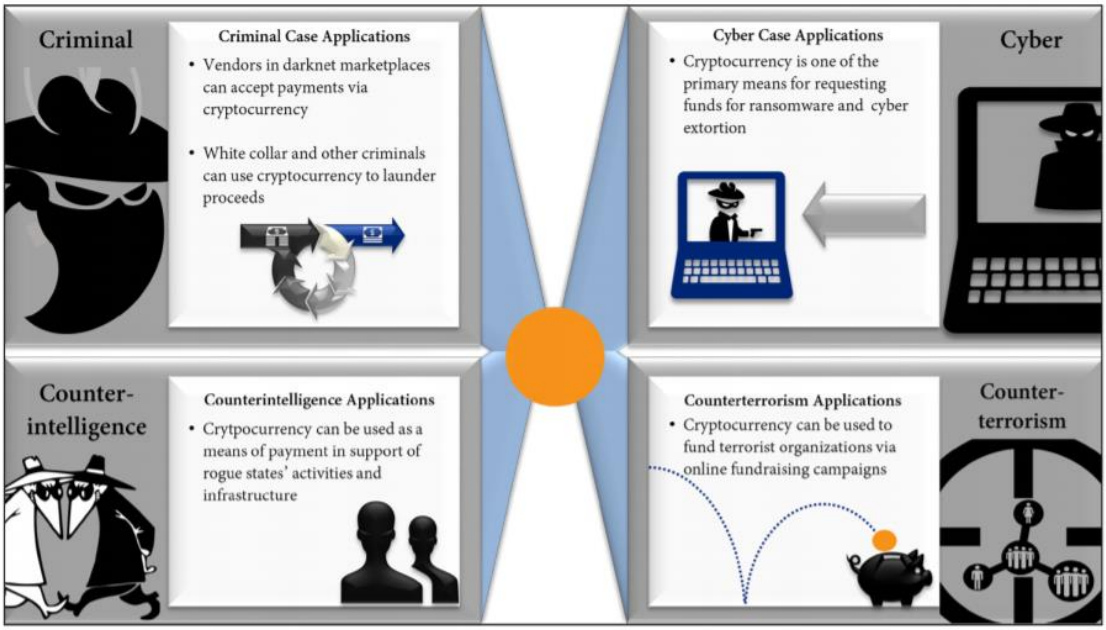



**Figure 3: Bitcoin Basics – Key Terms**



## Figure 4 : Examples of Cryptocurrencies in Investigations



*Number 14*

## UK National Sentenced to Prison for Role in "The Dark Overlord" Hacking Group

Defendant Conspired to Steal Sensitive Personally Identifying Information from Victim Companies and Release those Records on Criminal Marketplaces unless Victims Paid Bitcoin Ransoms

THE UNITED STATES DEPARTMENT of JUSTICE

A United Kingdom national pleaded guilty today to conspiring to commit aggravated identity theft and computer fraud, and was sentenced to five years in federal prison.

U.S. District Judge Ronnie White for the Eastern District of Missouri sentenced Nathan Wyatt, 39, who participated in a computer hacking collective known as "The Dark Overlord," which targeted victims in the St. Louis area beginning in 2016.

Wyatt was extradited from the United Kingdom to the Eastern District of Missouri in December 2019. Judge White also ordered Wyatt to pay $1,467,048 in restitution.

"Nathan Wyatt used his technical skills to prey on Americans' private data and exploited the sensitive nature of their medical and financial records for his own personal gain," said Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division. "Today's guilty plea and sentence demonstrate the department's commitment to ensuring that hackers who seek to profit by illegally invading the privacy of Americans will be found and held accountable, no matter where they may be located."

"The Dark Overlord has victimized innumerable employers in the United States, many of them repeatedly, said U.S Attorney Jeff Jensen of the Eastern District of Missouri. "I am grateful to the victims who came forward despite ransom threats and to the prosecutors and agents who were the first to catch and punish a member of The Dark Overlord in the United States."

"Cyber hackers mistakenly believe they can hide behind a keyboard," said Special Agent in Charge Richard Quinn of the FBI's St. Louis Field Office. "In this case, the FBI demonstrated once again that it will impose consequences on cyber criminals no matter how long it takes or where they are located."

Wyatt admitted that, beginning in 2016, he was a member of The Dark Overlord, a hacking group that was responsible for remotely accessing the

computer networks of multiple U.S. companies without authorization. Victims in the Eastern District of Missouri included healthcare providers, accounting firms, and others.

Wyatt admitted that The Dark Overlord co-conspirators acted by obtaining sensitive data from victim companies, including patient medical records and personal identifying information, and then threatening to release the companies' stolen data unless the companies paid a ransom of between $75,000 and $350,000 in bitcoin.

Wyatt further admitted that he participated in the conspiracy by creating, validating, and maintaining communication, payment, and virtual private network accounts that were used in the course of the scheme to, among other things, send threatening and extortionate messages to victims within the Eastern District of Missouri.

The investigation was conducted by the FBI's St. Louis Field Office. Support was also provided by the FBI's Atlanta Field Office. The Justice Department's Office of International Affairs coordinated the extradition of Wyatt. The department thanks law enforcement authorities in the United Kingdom, including the Metropolitan Police Service, for their substantial assistance in the investigation.

Senior Counsel Laura-Kate Bernstein of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Gwendolyn Carroll prosecuted the case.

*Number 15*

## Russian Hacker Sentenced to Over 7 Years in Prison for Hacking into Three Bay Area Tech Companies

THE UNITED STATES ATTORNEY'S OFFICE
NORTHERN DISTRICT of CALIFORNIA

Yevgeniy Alexandrovich Nikulin was sentenced to 88 months in prison for hacking into LinkedIn, Dropbox, and the now-defunct social networking company formerly known as Formspring, announced United States Attorney David L. Anderson and FBI Special Agent in Charge John L. Bennett. The sentence was handed down by the Honorable William H. Alsup, U.S. District Judge.

The sentence follows a guilty verdict after a 6-day jury trial. A jury found that Nikulin, 32, of Russia, hacked into computers belonging to LinkedIn, Dropbox, and Formspring, damaged computers belonging to LinkedIn and Formspring by installing malware on them, stole and used the login credentials for employees at LinkedIn and Formspring, and sold and conspired with others to sell customer data he stole as a result of his hacks.

Evidence at trial showed that Nikulin was located in Moscow when he hacked into a computer belonging to a Bay Area-based LinkedIn employee and installed malicious software on it, allowing him to control the computer remotely and to use the employee's credentials to access LinkedIn's corporate VPN.

Once he had access to corporate systems, Nikulin stole a database containing LinkedIn users' login information, including encrypted passwords.

In addition, the evidence demonstrated that Nikulin was behind similar intrusions and thefts of data at Dropbox and at Formspring.

The Court also found that Automattic, parent company of Wordpress.com, was the victim of an intrusion by defendant, although there was no evidence that defendant stole any customer credentials.

Nikulin was arrested while traveling in the Czech Republic on October 5, 2016, and extradited to the United States to face trial on March 30, 2018.

When discussing the reasons for imposing the 88-month prison term, Judge Alsup made clear that he hoped the sentence would send a message to deter anyone, including persons living overseas, from engaging in similar conduct.

Nikulin's trial began in March, but proceedings were suspended after just two days in light of the COVID-19 pandemic and ensuing closure of the federal courthouse.

The trial resumed on July 7, 2020, with the defendant, the attorneys, and Judge Alsup wearing masks, and the courtroom configured to allow social distancing by all participants.

Witnesses testified from behind a glass panel to allow testimony to be given while maintaining social distancing.

The trial was broadcast via Zoom to allow the public to view the proceedings without entering the courthouse.

Nikulin was convicted of selling stolen usernames and passwords, in violation of 18 U.S.C. § 1029(a)(2); installing malware on protected computers, in violation of 18 U.S.C. § 1030(a)(5); conspiracy, in violation of 18 U.S.C. § 371; computer intrusion, in violation of 18 U.S.C. § 1030(a)(2)(C); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(1).

Nikulin has been in U.S. custody since his extradition from the Czech Republic and will begin serving his sentence immediately.

Assistant U.S. Attorneys Michelle J. Kane and Katherine Wawrzyniak are prosecuting the case with the assistance of Helen Yee, Jessica Rodriguez Gonzalez, and Kim Richardson.

The prosecution is the result of an investigation by the Federal Bureau of Investigation, with the assistance of authorities in the Czech Republic, the U.S. Secret Service and the U.S. Department of Justice's Criminal Division, Office of International Affairs.

## 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.*