(CYBER) SECURITY AND FINANCIAL SECTOR IN THE CZECH REPUBLIC

AUTHORS: Berta Jarošová, Tomáš Koutský & Ondřej Černý

Prague Security Studies Institute

TABLE OF CONTENTS

US embassy

British Embassy Prague

This study was supported by
the Embassy of the United States in Prague and the British Embassy in Prague.

ABOUT THE REPORT

The financial sector is critical to every sovereign State. The vast majority of sectors, if not all, has seen **an unprecedented development and spread of financial technology** created, deployed and used by a wide range of actors in the banking and financial industry, as well as by customers and users. Ranging from online and mobile banking, artificial intelligence, big data, automation and blockchain. Many of these financial services and products have been accompanied by **the emergence of new actors entering the financial infrastructure**, including financial technology (FinTech) and regulatory technology (RegTech) startups. In parallel, traditional sovereign currencies are being altered by **the development of digital currencies** introduced by private companies but also States preparing to launch their national digital currencies. We seem to be witnessing **an unstoppable technology revolution in the financial sector** everyday and world might soon be entering **a new monetary era** with Libra or the Chinese digital currency that might launch soon on the financial market.

Innovation and progress typically go in hand with **new risks and challenges**. New technology based financial products and services, as well as traditional financial actors, including banks, have become **targets of cyber criminals** seeking profit from extortion, theft or fraud. In parallel, **clients' private data have become more vulnerable** to illicit practices worldwide. In the past decade, the financial sector has seen a **growing trend of state-sponsored cyber attacks and cyber espionage** in the financial sector for economic, political and intellectual property motivations. Like any other new phenomenon, the emergence of new financial technologies presents **new opportunities but also new challenges** for everyone: individuals, private companies in the financial sector, government and financial regulators.

The aim of this report is dual. The Czech Republic has not been immune to any of these developments, therefore the basic aim is to **demonstrate the latest legislative and regulatory developments in the field of cyber security and financial sector, underlying the cooperation between private and public sector** . The overall aim is to point out three selected challenges in the financial sector that are closely linked to cyber security or security more broadly. Namely, the report will address challenges in (1) **risks related to implementation of innovations**, including open banking and PSD2, the use of Artificial intelligence (AI) and the Cloud strategy; (2) **risks related to the emergence of FinTech startups**, including cyber risks and the link between startups, data privacy and national security; and lastly (3) **risks related to the development of digital currencies**, including cybercrime, sanction evasion and the future of global digital currency worldwide.

The present report does not seek to address cyber security challenges in the financial sectors in its entirety as it would be simply impossible but rather to **offer an update on the current cyber threat landscape in the financial sector** and t**o identify potential gaps and opportunities for collaboration between private and public sector in order to make the financial infrastructure more resilient** to the current and future threats. The ultimate ambition is to go beyond traditionally widely mentioned need for better cybersecurity hygiene and consider cyber threats predominantly from a national security perspective.

The authors would like to thank Alex Ivančo (Ministry of Finance of the Czech Republic); Petr Dvořák (Wultra); Tereza Gagnon (Wultra); Milan Zrcek (ČSOB); Martin Dlouhý (Raiffeisenbank); Lauri Almann (CybExer), Lucie Kadlecová (ERA-BHC); Dominik Stroukal (CEVRO); Maria Stazskiewicz (Czech FinTech Association) for their valuable guidance, advice and feedback.

INTRODUCTION
COLLABORATION IN CYBER SECURITY AND FINANCIAL SECTOR IN THE CZECH REPUBLIC

1. THE ROLE OF CZECH NATIONAL BANK

The Czech National Bank is the main regulator of banks, traditional financial institutions. Part of the **Czech National Bank's mandate is to supervise the entities operating on the local financial market by creating prudential rules and rules of conduct** towards clients with the aim to protect persons and institutions carrying on business on the financial market.[1]

Public-Private Information Sharing on Cyber Incidents & Events

The Czech National Bank has issued a number of regulations in the field of cybersecurity recently. One of the most important regulations, which contributed to a deeper and systematic cooperation between public and private institutions in cybersecurity, is on **information sharing about cyber incidents and events on the financial sector (2017)**.[2] The regulation concerns (1) the method of exchange of information on cyber incidents and subsequent measures; (2) the scope and format of shared information; and (3) administrative and technical conditions of the access to the database of incidents and events. The aim of the legislation adopted in 2017 was to create **a preventive cybersecurity tool** and enable information sharing between central banking authority and the private sector **to lower the subsequents risks and damages following cyber incidents and events**. According to such legislation, the banks have the obligation to report on occured cybersecurity incidents and have the opportunity to share voluntarily information on the so-called cyber security incidents that might incur information disruption.

Specific Cyber Security Audit Requirements

The Czech National Bank regularly conducts **compliance audits** to verify the compliance of banks with their reporting obligations. Such audits are usually conducted every year and banks can face penalty measures in case of non-compliance. For a long time, these audits have been general: the banks had to deliver a list of risks, stages of implementation of relevant measures, evaluation of the effectiveness of the measures and plan for future improvement in the upcoming year. However, **since September 2019, the Czech National Bank requires banks to report specific cybersecurity focused audits**. The aim of such requirement is to bolster the cyber resilience of banks. Such development only demonstrates the increasing importance of the topic of cyber security in the financial sector.

Permanent Working Group on Cyber Security

Representatives of financial institutions and regulatory bodies, namely the Czech National Bank and the National Cyber and Information Security Agency, admit that systematic coordination and well-established communication with regulators are absolutely crucial in cyber security issues. **A permanent working group on cyber security is regularly con-**

1 https://www.cnb.cz/en/about_cnb/mission/

2 https://www.cnb.cz/cs/financni-trhy/trh-statnich-dluhopisu/Sdeleni-CNB-o-obecnych-pokynech-EBA-k-oznamovani-vyznamnych-incidentu-podle-smernice-EU-2015-2366-o-platebnich-sluzbach-na-vnitrnim-trhu

vened by Czech National Bank to discuss the latest developments and cyber security threat picture. In parallel with a working group, the Czech National Bank regularly organizes cyber security workshops for banking and other professionals to ensure updated knowledge on new trends and threats in the sector and exchange of best practices.

2. THE ROLE OF NATIONAL CYBER AND INFORMATION SECURITY AGENCY

The Act on Cyber Security & NIS Directive: New Obligations for Banks

The Czech Republic was among the first countries to adopt a comprehensive **Act on Cyber Security**[3] in 2014 that defines national critical infrastructure and sets the obligations of the involved institutions, organs and persons. The **adoption of Directive on Security of Network and Information Systems** (NIS Directive), the very first EU comprehensive legislation in cyber security, and its transposition in domestic law in 2017, layed out **new obligations for private institutions** that have been previously left out from the Cyber Security Act, including banks. The NIS directive aims to achieve an even **higher level of security of network and information systems across the EU**, through (1) **improved cyber security capabilities** at the national level; (2) **increased EU-level cooperation**; and (3) **risk management and incident handling obligations** for operators of essential services and digital service providers.[4]

The third goal of NIS Directive is of particular importance to financial sector and banking institutions. Following its transposition to domestic law, The **Act on Cyber Security now defines who is an operator of essential services based on well-defined qualitative or quantitative criteria**, including the amount of clients, the proportion on the market or its relevance to elements of national critical infrastructure. Based on this concrete legislation, **the key criterion in the financial sector is the bank's proportion on the market**.[5] Banks that do qualify as operators of essential services thus need to comply with their obligations set out in the law. The updated Act on Cyber Security and creation of operators of essential services is therefore another example of public regulation that affects banks.

Key responsibilities and obligations of banks that need to be transposed in their internal rules and procedure thus include:

- Obligation to introduce and implement security measures
- Obligation to take into consideration security measures in the supply chain
- Obligation to inform about the operator of Security of Network and Information System
- Obligation to detect and report cyber security incidents
- Obligation to implement measures of the National Cyber and Information Security Agency, including warning; reactive and protective measures

Representatives of banks that do qualify as operators of essential services admit that the transposition of the NIS Directive and new subsequent obligations naturally impacted the **set of the technical, organizational and administrative internal rules and procedures at all levels, including technical, security and risk governance**. At the same time,

3 https://www.govcert.cz/download/kii-vis/preklady/Act_181_2014_EN_v1.0_final.pdf

4 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

5 http://www.psp.cz/sqw/sbirka.sqw?cz=437&r=2017

a general trend can be observed where cyber security is streamlined in private financial institutions as an important topic in regulation across levels, including EU-level, local and internal. The result effect of hereof is that **C-level executives and shareholders in banking sector perceive cyber security as their long term strategic priority** mainly following similar regulatory and legislative developments.

Warning Against Huawei: Effect on Supply Chain in Financial Sector

The National Cyber and Information Security Agency has issued on December 17, 2018 a **warning that 'the use of technical or program tools of Huawei Technologies, Co. and ZTE Corporation, including their subsidiary companies, poses a threat to cyber security.'6** Based on the before-mentioned Act on Cyber Security, banks that do qualify as operators of essential services, have the obligation to **implement measures of the National Cyber and Information Security Agency**, including those following this warning. Banks must also take into consideration such the conclusion of the warning when evaluating risks and planning their risk and threat management.

Some banks have even gone further and explicitly admitted that they have, **following the warning, ruled out both companies (Huawei and ZTE) from their internal and external audits a priori as a precaution measures in order to comply with the warning and maximize the protection of their clients' and company's data.** The warning has been accompanied by Governments' decision to impose the obligation to report new security audits to 160 State and private institutions. Banks that do qualify as operators of essential services under the Cyber Security Act must **conduct an additional security audit.** The National Cyber and Information Security Agency has issued a concrete methodology[7] how institutions shall proceed to analyze and evaluate the risks in their Security of Network and Information Systems, as well as in their current, prospective or closed supply chain contracts.

Although the initial deadline for the delivery of audits delivered to the National Cyber and Information Security Agency was end of May 2019, the audits are, according to the available information, still ongoing. However, the issued warning and the subsequent obligation imposed on critical institutions, including banks, is another example of another **reactive and preventive instrument to minimize the risks associated with certain types of technologies across industries, including the financial sector.** The aim of such measures is to protect the national critical information infrastructure, a priority set out in the current National Cyber Security Strategy (2015–2020).[8]

The Report on the State of Cyber Security in 2019: 'Czech Banking Sector Relatively Well Secured'

In September 2019, the National Cyber and Information Security Agency has released its **annual report on the State of Cyber Security in the Czech Republic in 2018**.[9] Although the financial sector is not the primary focus of the report, **the banking sector is, together with energy, a key sector in which cyber security is of paramount concern.** The report equally notes the **vulnerability of mobile banking applications against cyber attacks, the persistent threat of spear-phishing and warns about the case of modified QRecorder** application that has been later put down by Google from Google Play store. On the other hand, the Agency **welcomes consistent and positive efforts of the Czech National Bank**

6 https://www.govcert.cz/en/info/events/2682-software-and-hardware-of-huawei-and-zte-is-a-security-threat/

7 https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varován%C3%AD_z_17-12-2018_v1.0.pdf

8 https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

9 https://www.nukib.cz/download/publikace/report-czech-cyber-security-2018-en.pdf

in conducting regular cyber security checks in cooperation with banks and positive developments in cyber security becoming a priority for banks amid financial and reputational consequences. Such a positive conclusion demonstrates that banks are aware they cannot ignore cyber security, both for the protection of their clients and business know-how.

'The Czech National Bank conducts regular cyber security checks in the banking sector. The absence of more serious incidents means **we can conclude that the Czech banking sector is relatively well secured**. However, there are still **differences in the maturity of individual financial organizations, in particular in terms of protections against advanced cyber threats and internal intruders** (e.g. in security monitoring and penetration testing). In general, however, banks try not to underestimate cyber security, as the compromise of their information systems could have far reaching financial and reputational consequences.'[10]

The Report however points out to **two majors gaps when it comes to different levels of preparedness of banking sector to face cyber threats**:

— Protections against advanced cyber security threats
— Protections against internal intruders

Such a conclusion is linked to **external and internal cyber resilience of banks**.

In contrast to the Report on Cyber Security in the Czech Republic in 2017 where specific consideration of financial sector was absent, **this year's report analyzes cyber security in the context of financial institutions in several parts, underlying the prevalent trends in the financial sector and the above-mentioned opportunities for improvement**.

3. THE ROLE OF CZECH BANKING ASSOCIATION

Last, but not least, an important role in the institutional structure when it comes to cyber security in the financial sector plays the **Czech Baking Association, uniting more than 39 banks and representing more than 99% of Czech banking sector**. The Association has currently **two publicly available activities in the field of cyber security**: (1) **permanent working group on cyber security issues**; and (2) **annual Cyber Security Index.** The Czech Republic has scored 65 out of 100 points in this year's Cyber Security Index,[11] the best result for the past five years. The index indicates that **the most important challenge remains human factor and insufficient cyber hygiene, as well as growing and often underestimated cyber attacks on mobile banking applications**. Despite positive development, Tomáš Hládek, Advisor of the Czech Banking Association for Payments and Cyber Security, notes that in comparison with other European states, the Czech Republic remains on average.[12]

The Association equally plays **an important role in enabling and facilitating cyber security education, information sharing and fostering public-private cooperation and dialogue.** The latest example of such cooperation resulting in a positive development could be the **recent adoption at the beginning of December 2019 of BankID that will**

10 https://www.nukib.cz/download/publikace/report-czech-cyber-security-2018-en.pdf
11 https://czech-ba.cz/kyberbezpecnost-a-index-bezpecnosti-2019
12 https://czech-ba.cz/kyberbezpecnost-a-index-bezpecnosti-2019

enable the creation and large-scale use of digital banking identity.13 If adopted by the Czech Senate, the innovative legislation will enable the citizens of the Czech Republic to communicate with the public and Government authorities via digital identity leading to an unprecedented digitalization of public and private sector, as comments Filip Hanzlík, Deputy Director of Czech Banking Association. Digital identification has been used in a variety of countries, including in Sweden since 2003. The creation of a unified digital banking identity is of particular importance and relevance with a view to r**ecent regulative development following the European Union's Revised Payment Services Directive (PSD2)** that require banks to provide each other with access to users personal data, including account and transaction information. The effects of PSD2 will be considered in the following part.

13 https://czech-ba.cz/projekt-sonia-snemovna-navrh-schvalila

I. FIRST CHALLENGE: IMPLEMENTING INNOVATIONS IN THE BANKING SECTOR

1. CURRENT IMPLEMENTATION OF PSD2: OPENNESS VS. SECURITY

The **European Union's Revised Payment Services Directive (PSD2)14** was adopted in 2019. PSD2 is one of the most progressive legislations in the banking sector that aims to **facilitate information sharing and collaboration between different private and public financial institutions**. In this way, PSD2 leads to more innovative user friendly open-banking environment. However, there is a concern in the community about finding balance between openness and security in order to ensure clients' data privacy.[15]

The revised Payment Services Directive (PSD2, Directive 2015/2366/EU), proposed by the European Commission in July 2013, became applicable on 13 January 2018. It facilitates innovation and competition in the EU retail payment market. It gives consumers more and better choices and **introduces higher security standards for online payments**. This makes consumers more confident when buying online. It incorporates and repeals Directive 2007/64/EC (Payment Services Directive, or PSD1), which provided the legal basis for the creation of an EU-wide single market for payment services.The revised Directive adapts the rules to cater for emerging and innovative payment services, including internet and mobile payments, while at the same time ensuring a more secure environment for consumers.[16]

The Czech regtech (i.e. regulatory technology) startup Wultra has been recently awarded a public offer by the Czech National Bank to implement PSD2.[17] Such **contract with a private entity to implement a legislation is to a certain extent an unprecedented case and yet another example of vital collaboration between public and private sector in the financial secto**r in the Czech Republic. According to CEO Tomáš Dvořák, Wultra will therefore help the Czech National Bank to implement PSD2 into its internal rules and procedures. However, as he notes, at this stage the **implementation of PSD2 has been postponed because of insufficient preparedness of merchants**. Concerns about the capacity of merchants to operationalize Strong Customer Authentication was previously expressed by the European Banking Authority's opinion in June 2019.[18] However, at this stage, financial sector players are coping with the interpretation and implementation of PSD2. In this respect, **the Czech National Bank has recently organized a workshop to assist all actors involved in the operationalization of PSD2 with current challenges.**[19]

14 https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015L2366

15 https://www.pwc.com/cz/cs/odvetvove-specializace/bankovnictvi-a-financni-sluzby/ps2-v-kostce.html

16 https://ec.europa.eu/info/publications/190913-safer-payment-services_en

17 https://www.lupa.cz/aktuality/cnb-rozjizdi-vlastni-api-odpovidajici-psd2-zakazku-vyhral-cesky-fintech-wultra/

18 https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment

19 https://www.cnb.cz/cs/financni-trhy/trh-statnich-dluhopisu/Sdeleni-CNB-o-obecnych-pokynech-k-bezpecnostnim-opatrenim-podle-PSD2

The European Commission has also stressed that the European Banking Authority **'recognized that migrating the whole EU payments ecosystem to Secure Customer Authentication is challenging'**[20] and noted that in will be particularly vigilant in monitoring that all actors in the financial sector assume their responsibilities.

The issue of implementation of innovative regulation PSD2 generally demonstrates three trends: (1) the financial sector faces an **inherent challenge of multiplicity of actors with different structures and obligations that might pose obstacles to swift implementation of innovations**; (2) there is a **general inequality between the actors in the financial sector in terms of their preparedness**; and (3) however, **innovation can lead to even closer cooperation between public-private sector**, an example of which is the collaboration between the Czech National Bank and Czech startup Wultra.

2. BUSINESS RESPONSIBLE CONDUCT IN ALGORITHMIC AGE

Artificial intelligence (AI) & big data collection have become a standard practice in business, including in the financial sector. On one hand, the institutions **deploy algorithms for analytical purposes, to collect data about behavioral patterns in order to evaluate, customize and personalize their services and products**. On the other hand, institutions **use algorithms for security purposes, to monitor, detect and prevent possible cyber and other threats** both inside and outside their organization with the aim to protect their customers and business. In this respect, artificial intelligence is a particularly **useful tool to detect illicit practices, financial and cyber crime,** as well as to **reduce cyber risk**.[21]

However, **collection, analysis and in particular sharing by financial institutions of private datasets for predictive, evaluative or customer service purposes remains a major challenge**.[22] Artificial intelligence serves today **to evaluate credit eligibility or even to deliver a credit decision**[23] or to power smart chatbots used in private banking and to personalize financial products and services. Generally, customers are unaware of such practices of financial institutions. At the same time, bank representatives have acknowledged that **communication towards clients of the way algorithms and artificial intelligence are being used remains a challenge** for them.[24]

The use of artificial intelligence in financial products and services presents a number of **regulatory and compliance challenges**. Financial institutions, primarily banks, need to ensure that **customers' data are obtained, processed, used and shared appropriately and potential bias is eliminated, making the entire process transparent and explicable to their customers** who are subject to such practices.[25]

The use of artificial intelligence in financial sector is another proof of how technology is changing traditional sectors. The need to

20 https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/190621-eba-opinion-strong-customer-authentication-statement_en.pdf

21 https://www.fintechnews.org/how-ai-and-big-data-will-transform-banking-in-2019/

22 https://www.financierworldwide.com/ai-and-financial-services#.XfeLCy2ZPjA

23 https://www.brookings.edu/research/credit-denial-in-the-age-of-ai/

24 Conclusion based on interviews conducted with three bank representatives in the Czech Republic

25 https://www.financierworldwide.com/ai-and-financial-services#.XfeLCy2ZPjA

apply artificial intelligence in financial sector ethically, securely and responsibly is repeatedly underlined by governments and international organizations, and have become one of the main topics for collaboration between banks and technology companies.

A number of important regulatory developments took place in the framework of **the Organization for Economic Cooperation and Development (OECD).26** In a Blueprint on Responsible Artificial Intelligence for Business, the OECD has closely considered the **link between artificial intelligence, human rights and financial sector,** particularly in connection with the use of artificial intelligence in decision-making; operations and management; service delivery; ownership & research. Interestingly, the OECD also underlines the need to evaluate security risks and encourage responsible investment:

'AI creates entirely new dimensions for responsible investment— opportunities to proactively invest in companies developing AI for a positive social purpose, while **screening for risks that AI is deployed for harm**, such as in autonomous weapons systems or other controversial uses. **Technology is not often considered to be a high-risk sector, but that may need to change.**'[27]

In 2019, the OECD also published a set of **guidelines and artificial intelligence and responsible business conduct**[28] that:

— Lists possible questions to be taken into consideration when **establishing due diligence processes** covering all actors in the AI supply chain;
— Acknowledges the **link between artificial intelligence and human rights**;
— Outlines different **types of harm and risks** associated with artificial intelligence;
— Encourages **cross-sectoral collaboration** on artificial intelligence projects.

Similarly, the OECD published **Council Recommendation on Artificial Intelligence29** this year that calls to all artificial intelligence actors to promote and implement following Principles for responsible stewardship of trustworthy AI: **human centred values and fairness; transparency and explainability; robustness, security and safety; accountability**.

Similar conclusions have been prepared by European Commission.[30] None of the above-mentioned documents is financial sector-specific but despite being general, principles and recommendations set out by the OECD are applicable to the financial industry too.

At the national level, the government has prepared **a complex analysis of the deployment of artificial intelligence in the Czech Republic**.[31] The analysis has, inter alia, specifically considered application of artificial intelligence in financial and banking sector. The study encourages the **promotion of regulatory standboxes for AI development in the financial sector and the increasing use of 'regtech',** an example of which is the above mentioned case of Czech startup Wultra that collaborates with the Czech National Bank in the implementations of PSD2. There is no doubt technology development will foster cross-sectoral collaboration. In the **United Kingdom**, for example, the government has

26 https://www.bsr.org/reports/BSR-Artificial-Intelligence-A-Rights-Based-Blueprint-for-Business-Paper-02.pdf
27 https://www.bsr.org/reports/BSR-Artificial-Intelligence-A-Rights-Based-Blueprint-for-Business-Paper-02.pdf
28 http://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf
29 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
30 https://ec.europa.eu/futurium/en/ai-alliance-consultation
31 https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-Summary-Report.pdf

created the **Centre for Data Ethics and Innovation32** in which private industry, public sector, as well as non-profit organizations and research institutions are involved in order to strengthen the existing regulatory environment and foster ethical use of AI across sectors.

The deployment of artificial intelligence in financial sector is another proof of how **technology is rapidly changing traditionally rather conservative sector**. Such industrial and societal changes will once again **shift governance of AI in financial infrastructure space** and financial institutions will see their obligations increase and progressively lead to **enforcement of the business responsible conduct in the financial industry**. Collaboration between sectors is key and developments are to be expected with implementation of the **Czech Republic's Artificial Intelligence Strategy**.[33]

3. MOVING TO THE CLOUD: SPACE FOR REGULATION

Innovation in the banking sector is also intrinsically linked to **banks gradually moving their products and services to the Cloud**. Generally, financial institutions have a variety of options for different types of Cloud: private Cloud, local Cloud or public Cloud. Another alternative is an international cloud. Some banks have their own internal cloud providers, meanwhile others choose external cloud providers that become their contractors.[34] There is a **variety of Cloud providers who themselves become financial infrastructure players**, ranging from small startups, small-medium sized companies, to transnational technology companies such as Amazon or Microsoft that offer cloud services to financial sector players. The cloud strategy has lately become a big topic for the majority of banks but this domain remains largely unregulated.

However, the new **EU Wide Cyber Security Certification Scheme**[35] that was introduced with the **EU Cyber Security Act**,[36] intends to fill in the gaps and ensure harmonization of certification of changing financial market infrastructure across the EU.

Cloud computing in the financial sector presents a number of technical and operational risks linked to consumers' data management and excessive dependency of financial institutions on cloud providers.37 For this reason, the European Banking Authority has adopted a set of guidelines on outsourcing arrangements[38] that entered into force in September 2019 that sets out **specific provisions for these financial institutions' governance frameworks with regard to their outsourcing arrangements** and the related supervisory expectations and processes. The guidelines also impose stricter obligations on financial institutions subcontracting providers from third countries and considers with a particular focus on **higher regulatory requirements in the context of professional secrecy, access to information and data, protection of personal data.**

32 https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation

33 https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf

34 https://www2.deloitte.com/global/en/pages/financial-services/articles/bank-2030-financial-services-cloud.html

35 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

36 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

37 https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf

38 https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

The **Czech Republic is currently in its second phase of preparations of an eGovernment Cloud**.[39] The preparation involves representatives from Ministry of Finance, Ministry of Interior, National Cyber and Information Security Agency, key national organs and institutions, including intelligence services, and experts. Collaboration and creation of **national regulatory framework will be crucial in ensuring mitigation of cyber security and other risks related to cloud computing**. Further developments can be expected in early 2020.

39 https://www.mvcr.cz/soubor/usneseni-vlady-c-749-2018-sb-o-souhrnne-analyticke-zprave-vystupu-faze-i-projektu-priprava-vybudovani-egovernment-cloudu.aspx

II. SECOND CHALLENGE: FINTECH STARTUPS AND (CYBER) SECURITY CONCERNS

1. COOPERATION BETWEEN BANKS AND FINTECH STARTUPS: CYBER RISKS

The emergence of startups in financial sector has been of unprecedented growth and **banks have been increasingly open for cooperation with FinTech startups** in order to innovate their products and services in an extremely competitive environment. According to KMPG, investment in FinTech in 2018 represented more than $111 billions across the globe.[40] Some banks do even openly run **highly selective FinTech accelerator programs**,[41] other admit to organize **internal startup competitions**.[42] Banks can provide selected startups with initial funding, mentoring program and deeper cooperation in for example market potential analysis based on banks' customers' data sets or cloud support that allows startup to develop their product.[43] If proven successful concepts, selected startups can then be acquired and become an integral part of the bank. Banks also tend to increasingly invest in building their own internal FinTech or subcontract startups for concrete services and products. **FinTech startups became equal business partners of banks and in some cases their competitors.**[44] In the Czech Republic, the cooperation between FinTech ecosystem and traditional financial institutions, as well as public authorities, has been further facilitated and coordinated by **The Czech FinTech Association**.[45]

FinTech startups know-how, products and services are often **based on advanced technology, including machine learning, cloud computing, big data, blockchain or biometric authentication.** FinTech startups therefore become important **aggregators of customers' personal data that increases cyber risks**.[46] These personal data can include transactions listings, consumer behaviour analysis, personal information or biometric data about users. FinTech startups shall therefore follow **cyber due diligence standards47** in order to minimize the above-mentioned cyber risks and lower the possibility of theft or other illicit use of personal data by cyber criminals. Traditional banks shall **consider the cyber risks particularly when cooperating and enabling participation in startup accelerators to companies from third countries**.

FinTech startups are taking over a growing portion of the financial infrastructure, therefore **enforcement of the business responsible conduct and compliance** is more important than ever before to **ensure security, data privacy and intellectual property protection.**[48]

40 https://home.kpmg/xx/en/home/insights/2019/01/pulse-of-fintech-h2-2018.html

41 https://www.e15.cz/byznys/finance-a-bankovnictvi/nejvetsi-ceske-banky-prohlubuji-spolupraci-se-start-upy-1356107

42 Conclusion based on interviews conducted during interviews for the present study.

43 https://fintechcloud.outboxers.com

44 https://bankovnictvionline.cz/aktuality/capgemini-world-fintech-report-2019-bude-open-banking-jiz-v-dohledne-dobe-minulosti

45 http://czechfintech.cz

46 https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf

47 https://www.pwc.com/us/en/services/deals/library/understanding-cyber-due-diligence.html

48 https://www.pwc.in/assets/pdfs/consulting/cyber-security/banking/security-challenges-in-the-evolving-fintech-landscape.pdf

2. FINTECH STARTUPS, INVESTMENT SCREENING AND NATIONAL SECURITY

While the **United States became the land of investment and development of FinTech** startups with over $46 billions invested in FinTech in 2018,[49] **China has become the land of FinTech consumers** and could be, to some extent, be called 'a FinTech society', where mobile payments represent over $17 trillion with WeChat Pay or AliPay at the forefront of Chinese FinTech with more than 1.2 billion users.[50] Only recently, **WeChat Pay and AliPay became accessible to tourist visitors with foreign banking cards** enabling to effectuate instant transactions.[51] Even more importantly, **Chinese FinTech is not only present in China but is progressively expanding to other markets, including the European financial market** and Chinese companies have also expressed **interest in acquiring European entities in the financial sector**. Such investment ambitions did not go unnoticed by European and other Western lawmakers, regulators and politicians, many of who have raised **serious concerns about national security implications of such business plans.**

In January 2018, the Chinese financial conglomerate Ant, mother company of AliPay, has planned to acquire the US company MoneyGram. However, the **investment deal has been blocked by the Committee on Foreign Investment in the United States (CFIUS) over national security concerns**.[52] The **major risk was the safety of data that would allow Chinese entity Ant to identify US citizens and collect sensitive financial information**. In contrast, Ant has been more successful on the European market and took over the UK payments giant WorldFirst in early 2019[53], its biggest overseas expansion since the US ban.

New rules that will be finalized and will enter into force in 2020, will **expand the mandate of the CFIUS** and enlarge the types of transactions under CFIUS jurisdiction, including **assessment of risks connected to transactions in the global financial technology market**. 'CFIUS' jurisdiction will include **non-controlling investments in which a foreign person would gain access to U.S. critical infrastructure or sensitive personal data of U.S. citizens, including financial information**.'[54]

This represents a crucial regulatory step to ensure both national security and data privacy of US citizens are protected. Such decisions and growing scope from the CFIUS jurisdiction over FinTech investments also demonstrates the **growing interest of the Committee in cyber security and concerns over national security in domains that have not been traditionally linked to national security**, including financial sector, at times where technologies are taking a central role in the ongoing trade disputes between the United States and China.

The Czech Republic is currently preparing a **national legislation on foreign investment screening mechanism** that would allow control of investment transactions from third countries. The screening mechanism will **consider national security implication of potential transaction** and will focus pri-

49 https://www.cbinsights.com/research/fintech-startups-us-map/

50 https://kr-asia.com/alipay-serves-1-2-billion-users-after-three-year-global-expansion-push

51 https://www.cnbc.com/2019/11/06/alipay-wechat-pay-allow-tourists-in-china-to-use-foreign-cards.html

52 https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7

53 https://www.bloomberg.com/news/articles/2019-02-14/ant-financial-agrees-to-buy-u-k-payments-firm-worldfirst

54 https://www.rollcall.com/news/congress/proposed-foreign-investment-scrutiny-adds-to-fintech-deal-risk

marily on national critical infrastructure that would allow investors to access sensitive data. According to information available, **cyber security and financial infrastructure will be amongst the top priority screening areas**. The draft law is now being examined by the Parliament's Legislative Committee and is expected to enter into force in the first half of 2020.[55]

3. ALL ROADS TO EUROPEAN FINTECH MARKET LEAD THROUGH LITHUANIA?

Lithuania has become, after the United Kingdom, the second most popular country for FinTech startups. In 2016, the **Lithuanian government and trade agencies have agreed to develop a shared strategic outlook on every level of the FinTech ecosystem**[56] and has ever since been recognized as one of the most progressive regulators of financial sector in the European Union. In 2018, about 170 FinTech startups were based in Lithuania, 47 electronic money institution (EMI) licences issued, 33 payment institutions (PIs) and three specialised banking licences. The streamlining licensing and procedure automation makes the **application for new payment licences and e-money licenses two or three times faster than in any other country in the European European**. The Bank of Lithuania also offers a **regulatory sandbox that allow the newcomer to the market to consult with the regulator and apply for the licence remotely**. In addition, the government also supports the implementation of open banking policies, including the **creation of a financial sector API** (Application Programming Interface) register to give companies greater scope to access customer data. Companies that do obtain a licence in Lithuania are then allowed to operate in the common market of the EU.[57]

Lithuania inevitably offers a friendly environment that prioritizes progress and innovation. However, in the past year, **concerns were raised about prioritizing innovation over security, when Lithuania issued licences to a number of Chinese FinTech companies, allowing them to operate on European Union's financial market**. For example, Lithuania has issued licences to the following Chinese companies (having a mother company established in China or founded by Chinese citizens):

- Paytend Technology Europe
- PayPan Europe
- Goolpay Pay, UAB
- IBS Europe; and other.

No other country in the European Union, according to information available, has issued so many authorizations to Chinese startups enabling them to enter the European market. Such practice is **particularly worrying with regard to European security interests and protection of EU citizens private data**.

Marius Jurgilas, a board member at the Bank of Lithuania, has presented **Lithuania's plans of collaboration in FinTech with China at China Investment Forum in 2018**.[58] This year, Lithuania organized **The China-Central and Eastern European Countries (CEECs) High-level FinTech Forum in October 2019 in Vilnius**, where over 80 representatives from EU countries, including the Czech Republic, met with Chinese delegation to discuss opportunities for **future collaboration in FinTech, including tackling of potential risks and challenges such as cybersecurity,**

55 https://apps.odok.cz/veklep-history-version?pid=KORNBE7J4WXX

56 https://investlithuania.com/wp-content/uploads/2019/01/The-Fintech-Landscape-in-Lithuania-Report-2018.pdf

57 https://www.nsbanking.com/analysis/fintech-lithuania/

58 https://emerging-europe.com/news/lithuania-positions-itself-as-chinas-fintech-gateway-to-europe

data protection and consumer protection.[59] Concerns about such challenges have been notably raised in the context of wider EU security and protection European citizens' data.

In contrast, Lithuania has noted the risks associated with financial industry companies being linked to hostile countries. Its **annual National Threat Assessment Report** has explicitly warned about **risks connected to Russian companies in the financial sector**: 'In 2017, Lithuania passed amendments to its banking legislation and introduced the possibility of establishing specialized banks. These possibilities attracted attention of investment companies from third countries, the companies providing various financial services and financial technology-based systems ("FinTech"). **Some of them did not meet the national security interests due to the origin of their capital funds, their activities and links to the states hostile to Lithuania. Risks to the national security also originated from activities of the companies registered in Lithuania that cooperate with Russian business entities directly linked to the Russian military industrial complex**.'[60] Such findings demonstrate that Lithuania have in place a security screening mechanism.

During the recent Chinese-CEECs High Level FinTech Forum in 2019, Vitas Vasiliauskas, Chairman of the Board of the Bank of Lithuania said 'New FinTech entities with an EU licence can help eliminate existing bottlenecks in the financial sector infrastructure – for instance, by making cross-border retail payments between the EU and China faster, cheaper, and more efficient. **This will make it easier for businesses across Europe to reach the booming Chinese consumer class – and, indeed, for Chinese firms to trade more in Europe**.'[61] Such an approach open to Chinese capital remains questionable in times when the EU is adopting investment screening mechanisms from third countries, carefully considering risks associated with building 5G networks in Europe and intelligence services, including in the Czech Republic, are warning about Chinese influence in Europe.[62] **Therefore, the question is whether close cooperation with China in FinTech proposed by Lithuania is desirable with respect to security risks.**

The Most Popular Neobank Revolut & National Security Concerns

Lithuanian-based revolutionary neobank Revolut is not immune to security concerns. With more than 7 million users across the United Kingdom and Europe, has secured its pan-European banking license in December 2018 issued by the European Central Bank at the proposal of The National Bank of Lithuania. Before that, Revolut had operated in the UK and the European Union under an electronic institution money licence for several years. In April 2019, **Lithuanian MP Stasys Jakeliūnas, chair of the committee on budget and finance, proposed a resolution to review Revolut's operations based on concerns over the prevention of money laundering, and the parentage of co-founder and chief executive Nikolay Storonsky, whose father leads scientific research for a subsidiary of Gazprom, the Russian gas company.** Lithuania's Commission for Coordination of Protection of Objects of Importance to Ensuring National Security is now reviewing and investigating Revolut over the alleged ties.[63] Similarly, Revolut's sanctions-screening systems have been reviewed by the Financial Conduct Authority in the United Kingdom.[64]

59 http://www.xinhuanet.com/english/2019-11/28/c_138589840.htm

60 https://kam.lt›download›eng

61 https://www.lb.lt/en/speeches-interviews-presentations/17-1-high-level-fintech-forum-welcome-speech

62 https://www.bis.cz/vyrocni-zpravy/vyrocni-zprava-bezpecnostni-informacni-sluzby-za-rok-2018-ddd066bb.html

63 https://www.fnlondon.com/articles/revolut-to-face-third-government-review-in-lithuania-20190412

64 https://www.telegraph.co.uk/technology/2019/02/28/revolut-failed-block-suspicious-transactions/

III. THIRD CHALLENGE: DIGITAL CURRENCIES & CYBER SECURITY

1. EMERGENCE OF CRYPTOCURRENCIES: CAPABILITIES VS. RISKS

Over the past decade, the financial sector has also witnessed an **unprecedented development of digital currencies worldwide**. The most popular and widely known is certainly Bitcoin, the cryptocurrency pioneer created in 2009, **based on a distributed ledger technology called blockchain**. Bitcoin acted as a medium of exchange, using cryptography to secure transactions, eliminate government control and exchange rate issues, and create and control a new global currency.[65]

Ever since the emergence of blockchain technology, the advantages of blockchain underlying characteristics have been praised: **immutability, transparency, auditability, data encryption & operational resilience could potentially lead to stronger cyber defense, including in the financial sector**.[66] In contrast, experts have also warned about the risks of this technology widely spread out across the financial sector. From a cyber security risk perspective, challenges associated with cryptocurrencies include:

- **Management risks** (human management can threaten confidentiality, integrity and availability of private keys)
- **Software vulnerabilities** (human error can introduce cyber security risks into blockchain)
- **External data risks** (blockchain inherent interactions with external data sets can introduce risks into blockchain)
- **Identity-based attacks threat** (blockchain is not immune)
- **Long term risks** (the threats landscape, criminal strategies and technology are constantly evolving)[67]

For the above-mentioned reasons, **blockchain-based cryptocurrencies have also been a long-term challenge for regulators worldwide**. The Ministry of Finance of the Czech Republic have convened **consultations with experts on the future of blockchain regulation**.[68] The **Czech National Bank has repeatedly stated that it does not consider blockchain-based currencies as a currency** and there is not a legal definition of blockchain so far.[69] At the recent Crypto-Banking Conference in November 2019 in Prague, the Vice-Governor of the Czech National Bank has noted that 'cryptocurrencies do not fulfill any of good three criteria of sovereign currency, they are nor store of value, nor instrument of cash payment, nor an accounting entity'.[70]

However, **entities trading or exchanging cryptocurrencies need to obtain licenses from the Czech National Bank**, undergo

65 https://greyspark.com/cryptocurrencies-understanding-their-cyber-security-risks/

66 https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html

67 https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity

68 https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613

69 http://www.ghslegal.sk/cz/news/26

70 https://www.seznamzpravy.cz/clanek/viceguverner-cnb-hampl-kryptomeny-nejsou-meny-bitcoinu-by-ale-mel-centralni-banker-rozumet-povinne-61549

a strict application process and comply with anti-money laundering (AML) regulations that serve as a preventive tool against financial crime.[71] **Risks associated with cryptocurrencies and criminal activities were also a subject of the National Cyber Security Report 2018**. The National Cyber and Information Security of the Czech Republic has warned against the **increasing trend of cryptocurrency mining in the Czech Republic,** admitting that such illicit practices remain a minor threat from a cyber security IT infrastructure protection.

'Regarding the means of attack, in 2018, both internationally and in the Czech Republic, extortion attacks (ransomware) became less prevalent and were replaced by cryptocurrency mining through malware. This trend suggests the latter is likely to be a more effective tool to generate financial gain than ransomware attacks. Despite the impact on the computational performance of the infrastructure of the attacked entities, the illegitimate extraction of cryptocurrencies is a minor threat from the perspective of ICT protection. Unlike ransomware attacks, it is not destructive and does not compromise the availability of important data.
Infection by crypto miners is a growing trend noted across most sectors, including in the Czech Republic.'[72]

Of course, blockchain is not all about risks. At the end of November 2018, the Office of the Government of the Czech Republic and the Ministry of Trade and Industry, signed a **memorandum of cooperation73 with Blockchain Republic**;[74] a new initiative aiming to 'create an environment favorable to the development of projects implementing blockchain and decentralized technologies in areas other than cryptocurrencies'[75] in the Czech Republic.

2. THE GOLDEN AGE OF CRYPTO-CLEANSING

Alongside with crypto-mining, another trend that has recently emerged is more closely linked to new technologies and national security: **the phenomenon of crypto-cleansing**. One of the most advantageous characteristics of blockchain technology is the prevalent **anonymity and the consequent near impossibility to link and attribute transactions to individual people or organizations, especially applicable in case of 'privacy coins'**.[76] Security concerns have been raised recently particularly in connection to US Fin-Tech Startup Monero, that allows completely anonymous transactions.[77]

From this perspective, **the downside of blockchain technology is that it has allowed the creation of a new money laundering tool**. In the absence of established standards regulating digital currencies, **the blockchain technology has been used by sanctioned governments, criminal groups and terrorist organizations.** Digital currency is the fastest, easiest and most private way to launder

71 https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf

72 https://www.nukib.cz/download/publikace/report-czech-cyber-security-2018-en.pdf

73 https://www.vlada.cz/assets/media-centrum/aktualne/Memorandum-o-spolupraci.pdf

74 https://www.blockchainrepublic.cz/english

75 https://www.blockchainrepublic.cz/english

76 https://www.bloomberg.com/news/articles/2019-09-19/privacy-coins-face-existential-threat-amid-regulatory-crackdown

77 https://www.cnbc.com/2018/01/10/what-is-monero-north-korea-new-favorite-cryptocurrency.html

money globally and global sanction-screening, anti-money laundering and cyber-risk regulations are still absent.[78] **Security concerns linked to cryptocurrencies have also been raised by G20 finance Ministers at the G20 summit**[79] and **States can use digital currencies to evade international sanction regimes**.[80]

In December 2019, the United States arrested a US citizen who has been allegedly helping and advising North Korea on how to use cryptocurrency and blockchain technology to avoid sanctions.[81] The latest sanctions issued by the United States Department of Treasury targeted, inter alia,a cryptohacker South Korean Lazarus Group, that has been allegedly behind a half a billion dollars theft in cryptocurrency.[82] T**he United Nations Security Council have also expressed concern about cryptocurrencies that are, according to the conclusions, offering North Korea more ways to evade international sanctions**.[83] Evading sanctions by cryptocurrency means is part of North Korea's broader strategy that increasingly relies on complex and sophisticated cybercrime operations techniques[84]. From this perspective, **cryptocurrencies may become the future international security challenge at the global level and Western governments regularly warn against North Korean cybercriminals**.

Criminal organizations can use digital currencies to buy and sell illicit goods and services through the dark web. The dark web has been infamous in creating a nearly perfect environment for illicit and unlawful activities. **According to Europol, the most popular cryptocurrency on dark web remains Bitcoin.** Cryptocurrencies have become a key enabler, as well as the target of cybercrime. On one hand, criminal groups use cryptocurrencies to cover their criminal activity, on the other hand there is **a growing criminal interest in crypto-assets.**[85] **Cryptocurrencies are therefore both means and targets of financial crime.** The paradox is that **criminal groups increasingly use encrypted applications and services to facilitate and also cybercrime**, making it ever harder for law enforcement agencies to detect illicit practices. Applications originally designed to protect oneself from cyber criminals, has now become another helpful tool in their criminal activities.

Terrorist groups can use digital currencies to launder and relocate financial assets around the globe. Cryptocurrencies can be used for fundraising, illegal drug or arms trafficking, transfer of assets or attack and operational funding.[86] Hamas has designed an online campaign where **every visitor is given a unique Bitcoin address that enables him or her to donate and support the funding of the terrorist organization**.[87]

The **proliferation of digital cross-border financial channels** makes it increasingly difficult for governments and financial institutions to monitor and detect illicit transactions. With the development of digital currencies,

78 https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I

79 https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf

80 https://www.hsdl.org/c/resisting-u-s-sanctions-with-cryptocurrency/

81 https://www.ft.com/content/6c9b6be0-12ee-11ea-a7e6-62bf4f9e548a

82 https://www.fpri.org/article/2019/10/pyongyang-coin-and-the-future-of-u-s-sanctions-on-north-korea/

83 https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf

84 https://rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf

85 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

86 https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

87 https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html

now being also considered by States with China possibly at the forefront[88], it seems we are now **entering a new monetary era of 'Digital Currency Wars'** where States and private sector face new economic, diplomatic and security challenges in connection to cryptocurrencies.[89]

3. PRIVATE DIGITAL CURRENCY: SECURITY CONCERN OVER FACEBOOK'S LIBRA

In June 2019, **Facebook presented its plan to launch its own cryptocurrency – Libra**. The cryptocurrency project is administered by a Swiss-based Libra Association and is in line with Facebook's long-term ambition to create its own digital currency. The goal of the project is **to introduce a cryptocurrency built on a secure and stable open-source blockchain, backed by a reserve of real assets, and governed by an independent association**. However, the independence of Libra Association from Facebook, a social media platform with more than 2.4 billion users worldwide, remains questionable. According to the white paper published earlier this year, 'Facebook teams played a key role in the creation of the Libra Association and the Libra Blockchain, working with the other Founding Members. While final decision-making authority rests with the association, Facebook is expected to maintain a leadership role through 2019. **Facebook created Calibra, a regulated subsidiary, to ensure separation between social and financial data and to build and operate services on its behalf on top of the Libra network**.'[90]

Libra's mission is to build a cryptocurrency 'enabling a simple global currency and financial infrastructure that empowers billions of people'.[91] **Regardless how noble such ambition may seem, security risks have to be considered once again against innovation and potential capabilities to do 'global good'**. Governments and experts expressed **concerns about the privacy of users and the potential destabilization of traditional financial system that could happen with the introduction of Libra globally**. The Chair of the House of the Financial Services Committee, together with several congressional leaders have sent a letter to Facebook founder Mark Zuckenberg prompting him to cease the implementation of Libra project before lawmakers can decide on the benefits and risks, as well as possible regulation.

> "Because Facebook is already in the hands of over a quarter of the world's population, **it is imperative that Facebook and its partners immediately cease implementation plans until regulators and Congress have an opportunity to examine these issues and take action**."[92]

US Treasury Secretary Steven Mnuchin said he has serious national security concerns over Facebook's Libra and other cryptocurrencies. Mnuchin explicitly expressed concerns about potential money laundering enabled by cryptocurrency and said the US will hold the providers at the highest standard.[93] The project then became a subject of the Group of Seven (G7) discussions both in July and October 2019 when the G7 work-

88 https://www.ft.com/content/e3f9c3c2-0aaf-11ea-bb52-34c8d9dc6d84

89 https://www.belfercenter.org/dcw

90 https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

91 https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

92 https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=404009

93 https://www.bloomberg.com/news/articles/2019-07-15/mnuchin-plans-briefing-on-cryptocurrency-regulatory-issues

ing group composed of finance ministers, the International Monetary Fund, European Central Bank and World Bank representatives and others concluded that a **global cryptocurrency should not be launched until regulatory issues are resolved because it could threaten international the world's monetary system and financial stability**.[94] The **G7 working group on stablecoins** (including Libra) have, inter alia, **expressly considered cyber security related risks to stablecoins.** According to the report of the group, 'public authorities will require that operational and cyber risks from stablecoins be mitigated through the use of appropriate systems, policies, procedures and controls'.[95] At the same time, the working group note the growing threat of cyber attacks against crypto assets and warned against new risks that might not be yet identified.

Such **security concerns can be seen as understandable, legitimate and justifiable at times where Facebook is in the hands of more than a quarter of the population and following the Cambridge Analytica scandal**.[96] More broadly, they **underline the growing security, diplomatic, economic and regulatory challenges that States now face in relation to the deployment and use of new financial technology worldwide**.

94 https://www.reuters.com/article/us-imf-worldbank-facebook/facebooks-libra-cryptocurrency-faces-new-hurdle-from-g7-nations-idUSKBN1WW33B

95 https://www.bis.org/cpmi/publ/d187.pdf

96 https://www.reuters.com/article/us-usa-privacy-cambridgeanalytica/u-s-ftc-finds-cambridge-analytica-deceived-facebook-users-idUSKBN1YA1YZ

CONCLUSIONS

The financial sector faces fast-paced technology revolution and there is an obvious lack of standards and regulations that would encompass constantly evolving financial technology products, services and financial industry actors despite recent legislative development. **In times of rapidly changing threat landscape in the financial sector, the concept of cyber resilience of all financial industry actors is key.97** The present study highlighted selected number of current and prospective challenges:

— **National security and data privacy** become key considerations in the financial sector superior to business interests.
— **Deployment of artificial intelligence in financial sector** will need to be in line with business responsible conduct guidelines.
— **Security screening mechanisms and cyber due diligence** are put in place to ensure national security interests and private consumers' data.
— **Cryptocurrencies** introduced new types and forms of illicit activities and may become means of conflict in the future.

According to the National Cyber Security Report 2018, **the financial sector in the Czech Republic is 'relatively well secured'.** The present study shows the multiplicity of actors involved in financial sector that cooperate at different levels:

— by **implementing National Cyber and Information Security Agency recommendations** on cyber security in the financial sector;
— by **information sharing between private financial institutions, Czech National Bank, National Cyber and Information Security Agency and other relevant actors** on cyber incidents and events;
— by proposing and **promoting the adoption of new legislation introducing BankID in the framework of Czech Banking Association**;
— by collaborating on **new regulation implementation between Czech National Bank and Czech regtech startup Wultra**.
— By collaborating on **new projects and initiatives in the framework of Czech FinTech Association**.

97 https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

Prague Security Studies Institute
Pohořelec 6, 118 00 Prague 1
Czech Republic
Tel./fax: +420 233 355 735
pssi@pssi.cz
www.pssi.cz