Experience with Cybercrime in the Environment of the Police of the Czech Republic – the Police of the Czech Republic and Artificial Intelligence

Martin Bohman,[1] Oldřich Krulík,[2] Marie Mašková[3], Lenka Jirátová[4]

The article firstly describes the challenges, related to the cybercrime in the environment of the Czech Republic, including the feedback, which came from the specialized questionnaire with more than 1,400 respondents (police officers). Second part of the contribution is trying to describe the experience of the Police of the Czech Republic with artificial intelligence (including relevant security research project and other visions).

Keywords: cybercrime, artificial intelligence, research, survey, Czech Republic.

I. Introduction

The article firstly describes the challenges related to the cybercrime in the environment of the Czech Republic, including the feedback that came from the specialized questionnaire with more than 1,400 respondents (police officers). Their suggestions are carefully studied by the police force management and result in organizational and technical changes. The second part of the contribution is trying to describe the experience of the Police of the Czech Republic with artificial intelligence (including relevant security research projects and other visions). Education of police officers and preventive communication with the public is not a side of attention.

II. Method

The key methods used in the text include the annotated use of registered crime statistics in the Czech Republic, as well as the conclusions of research with more than 1,400 respondents, a police officer who took place in July and August 2022. The third source of information is detailed descriptions of research projects, which she entered and whose conclusions are used by the Police of the Czech Republic - in chronological order. The aspect of police education is mentioned separately, not only with regard to the rapidly emerging issue of artificial intelligence. It is thus a kind of primary data that other people interested in the issue can use as a springboard in their possible follow-up research.

[1] col. Martin Bohman, Ph.D., Central Analytical Department, Office of the Criminal Police and Investigation Service, Police of the Czech Republic; Prague, Czech Republic. E-mail: martin.bohman@pcr.cz, orcid.org/0000-0002-5013-5646

[2] doc. Mgr. Oldřich Krulík, Ph.D., academic worker, AMBIS University Prague; Central Analytical Department, Office of the Criminal Police and Investigation Service, Police of the Czech Republic; Prague, Czech Republic; E-mail: oldrich.krulik@pcr.cz; oldrich.krulik@mbis.cz, orcid.org/0000-0003-4048-5965

[3] Mgr. Marie Mašková, analyst, Central Analytical Department, Office of the Criminal Police and Investigation Service, Police of the Czech Republic; Prague, Czech Republic. E-mail: marie.maskova@pcr.cz

[4] Lt.col. Mgr. Lenka Jirátová, Central Analytical Department, Office of the Criminal Police and Investigation Service, Police of the Czech Republic; Prague, Czech Republic. E-mail: lenka.jiratova@pcr.cz

III. Cybercrime in the Environment of the Police of the Czech Republic

The very term "cybercrime" (computer crime etc.) in the environment of the Czech Republic is not always perceived in a completely homogeneous way.

- For the purposes of this study, it is firstly possible to refer to the criminal offenses regulated by Act No. 40/2009 Coll., Criminal Code, as amended, committed in relation to data (stored information): Unauthorized access to a computer system and information medium (Section 230); unauthorized access and damage to the record in the computer system, acquire and holding of the access device and password (Section 231); Damage to the record in the computer system and on the information medium and interference with the computer equipment due to negligence (Section 232).
- Secondly, there are criminal offenses regulated by Act No. 40/2009 Coll., On the Criminal Code, as amended, in which the computer is a means of committing them: Pornography dissemination (Section 191); Production and other handling with the child pornography (Section 192); Establishing illicit contacts with a child (Section 193b); Infringement of copyright, rights related to copyright and rights to the database (Section 270); Defamation of a nation, race, ethnic or other group of persons (Section 355); Incitement to hatred against a group of persons or restriction of their rights and freedoms (Section 356); Dissemination of an alarm message (Section 357); Defamation (Section 184); Blackmail (Section 175), and many more.

In relation to the topic, it is possible to make other observations of a general or current nature:

- It is a part of crime with a considerable latency, where the police probably obtain information only about a small part of the total volume of committed acts.
- This part of criminal activities has risen despite the coronavirus situation.
- The coronavirus period was also typical for the penetration of teleconferencing applications (Teams, Zoom and others) to obtain internal information (to a lesser extent, this was also related to the effort to obtain pornographic material).
- Cyber-attacks on medical facilities and other institutions were also recorded (ransom for unblocking of encrypted data). An example could be the blackmail of the Olomouc municipality /regional capital/ in May 2021, an attempt to raise USD 100,000).

Cybercrime and other crime in cyberspace is in practice divided within the framework of criminal statistics as follows (see Table 1, Table 2 and Figure 1):

Table 1: Cybercrime and other crime in cyberspace in the Czech Republic, general view, years 2017, 2021, 2022 and 2023 (Police of the Czech Republic Statistics).

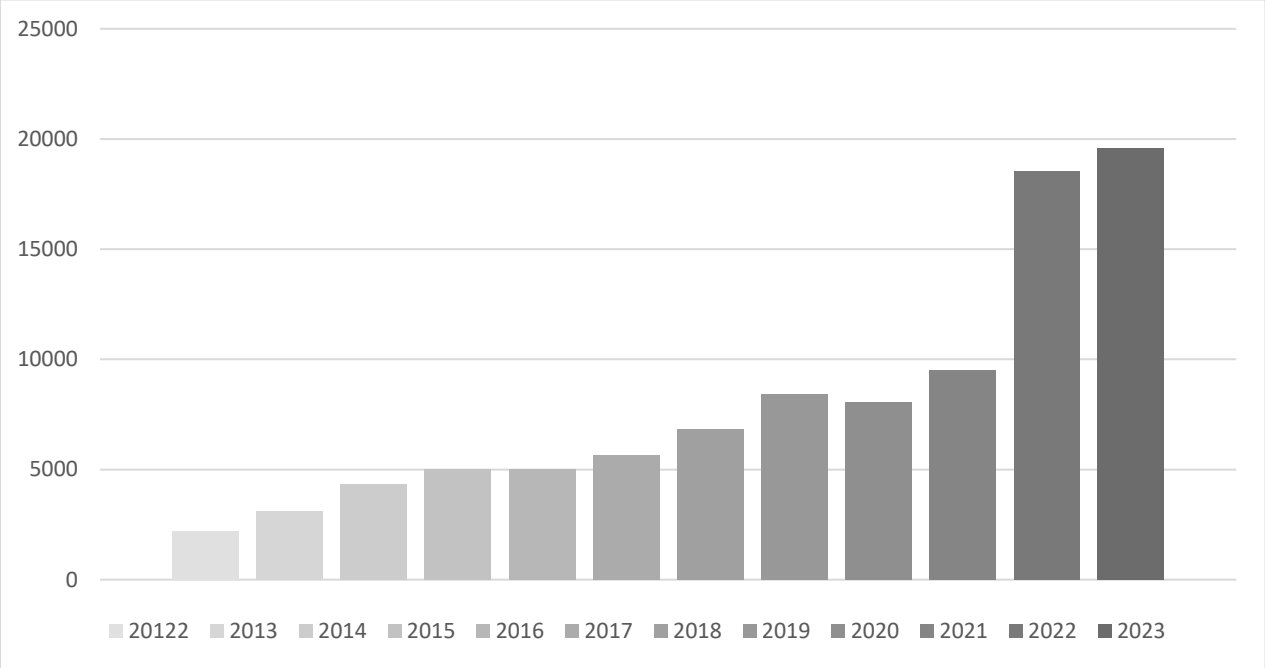
	Year 2017	**Year 2021**	**Year 2022**	**Year 2023**
Part of general crime	2 967	6 010	13 898	15 870
Part of economic crime	2 475	3 278	4 389	3 312
Part of remaining crime	211	226	248	256
Part of war and unconstitutional crime	1	1	7	10
Total cybercrime	5 654	9 518	18 554	19 592
% of total crime	2,79	6,21	10,20	10,80

Table 2: Cybercrime and other crime in cyberspace in the Czech Republic, individual cases, years 2021 and 2022 (Police of the Czech Republic Statistics).

	Cases 2021	Cases 2022	Cases 2023
fraud (of a general nature)	4 087	7 727	8 495
unauthorized acquire, forgery and alteration of means of payment	500	4 283	5 515
unauthorized access and damage to the record in the computer system, acquire and storage of the access device and password	1 682	2 575	1 687
child pornography and child abuse	500	629	546
infringement of copyright, copyright-related rights and database rights	344	564	271
credit fraud	645	527	632
fraud (of an economic nature)	381	407	359
extortion	173	316	406

Table 3 and Figure 1: Cybercrime and other cybercrime: Statistics for the years 2012 to 2023[5]

Year	2012	2013	2014	2015	2016	2017
Total cybercrime	2 195	3 108	4 348	5 023	4 990	5 654
Year	2018	2019	2020	2021	2022	2023
Total cybercrime	6 815	8 417	8 073	9 518	18 554	19 592



[5] Source: Police of the Czech Republic Statistics

Picture 1: Examples of campaign visuals "Scammers Impersonate Your Bank"[6]

IV. Police of the Czech Republic – Cybercrime Survey

With regard to mapping the situation within the Police in the Czech Republic, there is interesting survey that took place in July and August 2022. The issue can be generalized into 12 questions. There were more than 1,400 respondents (police officers).

1) What training courses have you finished or would you recommend to colleagues?

- Courses of the Police Academy of the Czech Republic in Prague.
- Courses at the level of district units, regional police directorates, or part of instructional methodical training dominate – apparently with very diverse form and content.
- Around 7 % of courses are taking place with some international element (CEPOL, Central Europe Police Academy, cooperation with neighbouring countries).
- This aspect would be better solved by a certain intranet discussion thread, where experiences about the quality of training and other educational events would be shared, as well as a notification that a certain course or training is taking place.

2) What other cybercrime training would you welcome in the future?

- "Documenting criminal activity and securing evidence" (53 %).
- "Operational penetration of cyberspace" (24 %).
- "Securing funds – virtual currencies" (9 %).
- The combination of several topics and other issues is also subject of interest.

3) How do you perceive current trends regarding the cybercrime in the Czech Republic?

- The whole agenda will be significantly more serious; the number of reported cases begins to exceed "traditional" (offline) crime (47 %).
- Social engineering (15 %), fraud with use of the cryptocurrencies and other "investments" and so-called "bazaar fraud" are significant.
- It has been repeatedly said that the police force is generally lagging behind the criminals in this fight.

[6] Source: Police of the Czech Republic

4) What specifics of the cybercrime do you perceive with regard to economic crime?

- The prevailing opinion was that law enforcement authorities are lagging behind in all of the aspects of the cybercrime; the Police of the Czech Republic need a **completely different organizational framework in this regard** (17 %).

Regarding specific trends, the respondents said that they perceived the most visible:

- Boom in fraudulent „investments" in cryptocurrencies etc. (11 %).
- The need for closer cooperation with the banking sector. (11 %).
- The international element of the issue and thus its low clearance level (10 %).
- The need for constant public awareness or education (9 %)…
- Fraud is a crucial phenomenon, including so-called bazaar fraud (4 %).
- Traditional challenges are attempts to break into the internet banking (4 %).
- The agenda is highly bureaucratized (4 %).

5) What specifics of the cybercrime do you perceive with regard to vice crime?

- Around 42 % of respondents is not investigating this type of a crime.
- Of the remaining answers, education is perceived as pivotal, in relation to both children and adults (21 %).
- Explicit content is practically impossible to avoid in the current set-up of society (5 %).
- The potential for various forms of extortion is also important (6 %).
- About 2 % of respondents perceive the topic as the domain of less technically proficient criminals, or with less social significance than in the case of „materially-motivated" crime.

6) What specifics of the cybercrime do you perceive with regard to drug crime?

- Around 64 % of respondents is not investigating this type of a crime.
- Regarding the remaining answers, the technical advantage of the perpetrators is perceived as a crucial aspect (59 %).
- This segment of crime is also moving into cyberspace (21 %).
- Abuse of delivery services or the Czech Post for transporting drugs to a customer is not an exception (3 %).

7) What aspects of the cybercrime do you encounter most in your practice?

- Fraud in general is a phenomenon where the perpetrator uses various techniques to achieve his or her objective. The most common sub-variants include bazaar scams, romance scams, bogus banker, "investment" etc. (37 %)
- Efforts to obtain sensitive data by technical means are less frequent (10 %).

8) Which area of the cybercrime do you personally consider to be the current crucial challenge?

- Crimes related to children (child pornography and attempts to establish illicit contacts with children – 47 %).
- Fraud (15 %).
- Other forms of property crime (8 %).
- Hate crime (7 %).
- Various forms of extortion (5 %).

9) What important tools do you possibly lack as police officers?

- Efficient analytical tools (51 %).
- Cover internet connection (21 %).
- Hardware equipment (20 %).
- Fast connection (8 %).

There is also call for de-bureaucratization, including the flexibility of searching in relevant databases or reduction of existing technical restrictions at workplaces.

10) What are the main challenges in detecting and investigating of this type of crime?

- Staffing and organizational changes (21 %).
- Technical equipment (19 %).
- Methodical coverage of the topic (19 %, also through external suppliers, etc.).
- Education and training (16 %).
- Modification of the legal framework (15 %).

11) What topics would you recommend focusing on cybercrime prevention?

- The need for an all-encompassing campaign, based on real cases of today (42 %).
- Cooperation with schools, campaign aimed at children (8 %).
- Activities, cooperation with banks, ideally also co-financed by banks, prevention of misuse of internet banking (7 %).
- Part of the public is "unteachable", resistant to any campaign.

12) Add anything else you think would be helpful in this area.

- Necessity of comprehensive training of police officers (19 %).
- Call for an overall **different organizational approach** regarding the fight against cybercrime within the police force (14 %).
- Necessity of personal strengthening of the agenda (8 %).
- Continuous education towards the public (8 %).

V. Artificial intelligence as a security topic for the European Union and other international organizations[7]

In 2019, the European Commission created a White Paper on Artificial Intelligence,[8] with an emphasis on the ethical implications of the topic. At the same time, debates among the European Union Member States on the possible future direction of this issue were started or renewed. During the same year, the European Union's Directorate-General for Home Affairs, in cooperation with the European Union's member states, organized three workshops[9] that enabled states to identify topics of interest and key challenges in the field of artificial intelligence, such as aspects related to data management and protection of (personal and other potentially sensitive) data.

In February 2020, the White Paper on Artificial Intelligence[10] was adopted as part of the European Union's Digital Strategy.[11] The White Paper highlights the importance of ensuring that security meets the demands of the digital age and is able to strengthen technological independence in the relevant area. In this context, it was found necessary to use the potential that the European Union's

[7] Bohman, Martin and Oldřich Krulík. *Umělá inteligence jako bezpečnostní téma pro Evropskou unii a další mezinárodní organizace*. Mezinárodní bezpečnostní institut, 29 September 2021. https://www.mbi.expert/pracovni-list-umela-inteligence-jako-bezpecnostni-tema-pro-evropskou-unii-a-dalsi-mezinarodni-organizace/

[8] Bílá kniha o umělé inteligenci. *Digi koalice*. https://digikoalice.cz/bila-kniha-o-umele-inteligenci/

[9] Events about Artificial intelligence. *European Commission*. https://wayback.archive-it.org/12090/20210727053425/https://ec.europa.eu/digital-single-market/en/newsroom-agenda/event/artificial-intelligence

[10] Bílá kniha o umělé inteligenci. *Digi koalice*. https://digikoalice.cz/bila-kniha-o-umele-inteligenci/

[11] Evropská strategie pro data. *Evropská komise*. 19 February 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066

Digital Strategy offers in the area of internal affairs. The Union continuously declares the necessity of maximizing the possibilities of financing of the related activities, including through the Digital Europe program.

March 2020 was marked by comments on the draft framework positions for the so-called Digital Package.[12] Specifically, the comments of the Czech Republic were mainly the following:

- Excessive over-regulation, which is perceived as an explicit security threat, must be prevented.
- The related regulatory framework needs to be conceived in general, without excessive technological details.
- A cautious approach to the regulation of artificial intelligence (related technologies) in the area of biometric identification, which is perceived as an area with a direct potential threat to human rights, is necessary.

In April 2020, the European Commission presented an updated Coordinated Plan on Artificial Intelligence and a Communication on Strengthening the European Approach to Artificial Intelligence, published together with the adopted draft Regulation on Artificial Intelligence. A detailed analysis of the issues related to the presented proposal of the Regulation on Artificial Intelligence is available in the related impact assessment report.[13]

In June 2020, Member States were invited to nominate experts to the Expert Group on Artificial Intelligence (the issue of the use of artificial intelligence in the field of law enforcement and police controls; in the field of asylum and border protection).[14] The Czech Republic was in this regard represented by the representative of the Police of the Czech Republic (Department of Informatics and Information Technology Operation).[15] The aforementioned expert group has held a number of expert meetings to date. Among others, the following topics were discussed:

- Reasons for the draft regulation of artificial intelligence; definition of artificial intelligence; typology of artificial intelligence according to its potential riskiness; related objectives of the European Commission in the field of internal affairs; main areas for high-risk applications of artificial intelligence for security forces, rules for the use of biometrics.[16]
- Data Science Framework.[17]

July 2020 is mentioned in connection with the following agenda (documents):

- Document, called Initial Impact Assessment: Artificial Intelligence – Ethical and Legal Requirements.[18]

---

[12] Evropská komise představila digitální balíček, včetně návrhů k umělé inteligenci a datům. *Úřad Vlády České republiky*, 20 February 2020. https://www.vlada.cz/cz/evropske-zalezitosti/aktualne/evropska-komise-predstavila-digitalni-balicek--vcetne-navrhu-k-umele-inteligenci-a-datum-179763/

[13] Posouzení dopadů návrhu Nařízení o umělé inteligenci. *Ministerstvo financí České republiky*, 3 May 2021. https://www.mfcr.cz/cs/soukromy-sektor/inovace-na-financnim-trhu/aktuality/2021/posouzeni-dopadu-navrhu-narizeni-o-umele-41759

[14] Umělá inteligence v oblasti vnitřní bezpečnosti. *Policie České republiky*, PPR-21570-2/ČJ-2021-990770.

[15] Odbor informatiky a provozu informačních technologií. *Policie České republiky*. https://www.policie.cz/clanek/odbor-informatiky-a-provozu-informacnich-technologii.aspx

[16] Babuta, Alexander and Marion Oswald. *Data Analytics and Algorithmic Bias in Policing*. Royal United Services Institute for Defence and Security Studies, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

[17] Data Science and Criminal Justice. *Digi-Crim-Jus*, 6 July 2021. https://www.digicrimjus.com/2021/07/06/data-science-and-criminal-justice/

[18] Umělá inteligence – etické a právní požadavky. *Evropská komise*, 2020. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2020-3896535_cs

- Assessment List for Trustworthy Artificial Intelligence.[19]
- Trusted Artificial Intelligence Industry Recommendations.[20]

An important event in November 2020 was a conference organized by the Council of Europe called Artificial Intelligence for Peace, Justice and Security (in which the Czech Republic participated – through the Department of Informatics and Information Technology Operation of the Police of the Czech Republic).[21]

In May 2021, document No. 8515/21 "High Risk Applications of Artificial Intelligence: Homeland Security Outlook" was released. The text proposes a separate legal framework for artificial intelligence in the field of internal security.[22]

In July 2021, in the context of Slovenia's Presidency, the General Secretariat of the Council of the European Union organized a virtual conference "Artificial Intelligence Regulation – Ethical Aspects and Fundamental Rights Aspects".[23]

The Ministry of the Interior of the Czech Republic announced on March 2021, two public security research competitions. Both concern applications of security technologies such as artificial intelligence, robotics, nanotechnology, laser technology and photonics. The research results are intended to help the components of the Integrated Rescue System of the Czech Republic. Public competitions are announced as part of the IMPAKT and SECTECH programs.[24]

AMBIS University is the main researcher of the Technology Agency of the Czech Republic project "Artificial Intelligence and Human Rights: Risks, Opportunities and Regulation".[25] The aim of the project is to identify and evaluate risks and opportunities in the field of the relationship between artificial intelligence and human rights and to propose solutions for how related technologies could be developed, used and regulated so that they do not threaten human rights and, on the contrary, help its development and protection.

Activities and processes within the International Police Organization, Interpol, related to the issue of artificial intelligence, can be illustrated on the following schedule:[26]

---

[19] Assessment List for Trustworthy Artificial Intelligence for Self-Assessment. *European Commission*, 17th June 2020. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[20] Policy and Investment Recommendations for Trustworthy Artificial Intelligence. *European Commission*, 2020. https://wayback.archive-it.org/12090/20210728103937/https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence

[21] Conference on responsible AI for Peace, Justice and Security. *Council of Europe*, 19 November 2020. https://www.coe.int/en/web/artificial-intelligence/-/conference-on-responsible-ai-for-peace-justice-and-security
Council of Europe and Artificial Intelligence. Council of Europe. https://www.coe.int/en/web/artificial-intelligence/home

[22] High Risk Artifical Intelligence Applications: Internal Security Outlook. *European Commission*, 12th May 2021. https://www.statewatch.org/media/2407/eu-council-ai-internal-security-discussion-paper-8515-21.pdf

[23] Virtual Conference on the Regulation of Artificial Intelligence, Ethics and Fundamental Rights. *Slovenia Presidency of the Council of the European Union*, 20 July 2021. https://slovenian-presidency.consilium.europa.eu/en/news/at-the-virtual-conference-on-the-regulation-of-artificial-intelligence-ethics-and-fundamental-rights/

[24] Ministerstvo vnitra vyhlašuje veřejné soutěže na umělou inteligenci, robotiku a kyberbezpečnost. *Ministerstvo vnitra České republiky*, 2021. https://www.mvcr.cz/clanek/ministerstvo-vnitra-vyhlasuje-verejne-souteze-na-umelou-inteligenci-robotiku-a-kyberbezpecnost.aspx

[25] Umělá inteligence a lidská práva: rizika, příležitosti a regulace. *Vysoká škola AMBIS*. https://www.ambis.cz/umela-inteligence-a-lidska-prava-rizika-prilezitosti-a-regulace

[26] Interpol. *Artifical Intelligence Observatory and Forum.* http://observatory.ilaw.cas.cz/index.php/mezinarodni-aktivity/interpol/

- In November 2020, the 3rd meeting of law enforcement authorities for artificial intelligence took place. It is the embodiment of cooperation between Interpol and the United Nations Interregional Crime and Justice Research Institute. Elements of artificial intelligence in the Czech Republic was presented by the Reliéf project.[27]
- A series of "Artificial Intelligence Virtual Training Rooms", designed to raise awareness of the issue among police officers (how artificial intelligence can impact police models and activities).[28]

VI. Security Research in the Czech Republic, related to the police priorities with use of the artificial intelligence

Following pages are describing the most important variables, related to the security research projects in the Czech Republic, where artificial intelligence aspect were being used. In a very simplified model, it is possible to say, that artificial intelligence is (or will be) used in the analysis of data (big data), sound and image respectively.

A System for Text Analysis for the Needs of the Police of the Czech Republic (2017-2018)[29]

The objective of the project was to implement a system that provides the following functionality for the environment of the Police of the Czech Republic:

- Automatic search for named entities and their relations (persons, companies, addresses, communication means, vehicles, accounts, weapons, drugs, important events etc.) including out-of-vocabulary entities (unknown names, addresses).
- Advanced full-text search with a specific support for Czech and English, capable of aggregating results according to identified named entities.
- Search for similar cases having the same nature or course and differing only in facts (such as date or offender names).

Researchers: Charles University, Faculty of Mathematics and Physics.
Funding: 1 010 000 CZK (42 000 EUR).
Results: Software for text analysis (morphological analysis, named entity analysis and summarization) and document search for needs of Police of the Czech Republic.

B Building and Verification Operation of the Cyber Threat Intelligence System (2017-2021)[30]

The main objective of the project was to strengthen critical information infrastructure protection and reduce damage caused by cybercrime through the establishment of the effective detection, identification and prediction system of cyber threats and evaluation of cybersecurity incidents.

---

[27] Towards Responsible Artificial Intelligence Innovation. *United Nations Interregional Crime and Justice Research Institute*, 2020. http://www.unicri.it/towards-responsible-artificial-intelligence-innovation
UNICRI Centre for Artificial Intelligence and Robotics. *United Nations Interregional Crime and Justice Research Institute*. http://www.unicri.it/in_focus/on/unicri_centre_artificial_robotics
Táborský, Vladimír. Projekt „Reliéf" na 44. evropské regionální konferenci interpolu v Praze. *Bulletin Národní protidrogové centrály*, 2016, No. 3, 43-46. http://future-forces-forum.org/review/236.str.2-.pdf

[28] Interpol Virtual Academy. *Interpol*. https://www.interpol.int/How-we-work/Capacity-building/INTERPOL-Virtual-Academy

[29] System for Text Analysis for the Needs of the Police of the Czech Republic. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20172017023

[30] Building and Verification Operation of the Cyber Threat Intelligence System. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20172021022

Researchers: CZ.NIC; CESNET.
Funding: 25 080 000 CZK (1 040 000 EUR).
Results: Three results, including Cyber Threat Intelligence portal, used for dynamic display of data from the incident database and is based on a client-server architecture with a three-tier architecture. The platform is able to generate events for the creation and subsequent sending of notifications about anomalies to the browser.

C Employment of Artificial Intelligence into an Emergency Call Reception (2019-2022)[31]

The projects investigated the deployment of artificial intelligence for the reception of emergency calls during crisis events with a voice chat-bot.
Researchers: Mining University, Technical University of Ostrava, Faculty of Security Engineering; GoodAI Applied Ltd.; Phonexia Ltd; SpeechTech, Ltd; Brno University of Technology, Faculty of Information Technologies
Funding: 28 938 000 CZK (1 200 000 EUR).
Results: 4 results, see webpage.

D Development and Testing of Algorithms for Predictive Behavioural Analysis of Persons Crossing the External Borders of the European Union (2018-2019)[32]

The objective of the project was to increase the likelihood of timely detection and capture of the interest of the police and other administrative authorities, crossing the external borders of the European Union and the Czech Republic.
Researchers: Czech Technical University in Prague, Faculty of Information Technologies
Funding: 2 808 000 CZK (116 500 EUR).
Results: The summary research report contains a description of the analysis of the available data and their applicability for behavioural analysis of persons, a detailed description of the algorithms examined and an evaluation of their quality and scalability, not only the basic algorithms, but also their combination (ensembles).

E Complex Analysis and Visualization of Large-Scale Heterogeneous Data (2017-2020)[33]

The main objective of the project was to create an integrated distributed system enabling complex analyses of heterogeneous data of large-scale - especially digital artefacts obtained under police investigations. This multidimensional visualization should provide multiple views over analysed data as well as information through interactive combination of annotated graphics (e. g. maps), graphs (statistical and relational), charts, time series, and other specialized visualization techniques.
Researchers: Masaryk University, Institute of Computer Technology
Funding: 13 941 000 CZK (578 000 EUR).
Results: Six results, including the computation subsystem software component used to process and analyse selected data. The visualization software component is an integral part of the system, significantly influencing both its analytical capabilities and user comfort.

---

[31] Employment of Artificial Intelligence into an Emergency Call Reception. *Starfos.* https://starfos.tacr.cz/en/projekty/VI20192022169

[32] Development and Testing of Algorithms for Predictive Behavioral Analysis of Persons Crossing the External Borders of the European Union; VH20182019034. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20182019034

[33] Complex Analysis and Visualization of Large-Scale Heterogeneous Data. *Starfos.* https://starfos.tacr.cz/cs/projekty/VI20172020096

F Lost Persons, Offenders Position Automated Prediction Tool (2018-2021)[34]

The objective of the project was to streamline operational management and speed up the steps necessary to find the missing person as quickly as possible and to reduce the risk of life and health of these or other persons.
Researchers: Eago systems Ltd.
Funding: 33 306 000 CZK (1 380 000 EUR).
Results: Several results, including an automated tool for predicting the location of wanted or missing persons (offenders). The result represents highly automated tool enabling to systematise and accelerate and streamline the operational management aimed on search and find of missed or suspected person (or culprit).

G Integrated Platform for Analysis of Digital Data from Security Incidents (2017-2020)[35]

The project deal with the experimental development of advanced methods and tools of network security analysis based on data mining, machine learning, visual analytics and their implementation as a forensic platform. The project outcome will be demonstrated using practical cases studies, namely, identification of P2P traffic, forensics analysis of mobile devices and investigation of Bitcoin incidents.
Researchers: Brno University of Technology, Faculty of Electrical Engineering and Communication Technologies
Funding: 16 746 000 CZK (694 000 EUR).
Results: About 68 results, including an integrated platform is a set of software and hardware tools for analysing various sources of information to extract artefacts that may indicate the presence of a security incident or are further used to identify such an incident or as evidence in an investigation.

H Tools and Methods for Video and Image Processing to Improve Effectivity of Rescue and Security Services Operations (2017-2020)[36]

The project focused on research in advanced methods for image and video processing. The objective is to create a functional sample of a system that significantly improves effectivity of security and rescue forces intervention.
Researchers: Brno University of Technology, Faculty of Electrical Engineering and Communication Technologies.
Funding: 22 864 000 CZK (948 000 EUR).
Results: Several results, including:

- Software that enables automatic camera calibration using detected key points and their 3D correspondence.
- Sensing device for short firearms. It is a device that is composed of a u-ramp, Microsoft Kinect and two cameras that enable the acquisition of data for 2D and 3D data reconstruction of the scanned object, specifically short firearms.[37]

---

[34] Lost Persons, Offenders Position Automated Prediction Tool. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20182021039
[35] Integrated Platform for Analysis of Digital Data from Security Incidents. *Starfos.* https://starfos.tacr.cz/cs/projekty/VI20172020062
[36] Tools and Methods for Video and Image Processing to Improve Effectivity of Rescue and Security Services Operations. *Starfos.* https://starfos.tacr.cz/cs/projekty/VI20172020068
[37] Snímací zařízení pro krátké střelné zbraně. *Fakulta informačních technologií*; *Vysoké učení technické v Brně*. http://www.fit.vutbr.cz/research/prod/index.php?id=553

VII. Results

Regarding the fight against cybercrime, as well as possible uses of artificial intelligence by the Police of the Czech Republic, the following can be stated: It is necessary to continue in the processes that have already been started, for example regarding the use of sophisticated camera systems (face recognition, even for people who wear veils). It is also necessary to relieve police officers from tedious routine activities, like issuance of official decisions in relation to ever-repeating actions, for example regarding the traffic police. This task can be delegated to artificial intelligence and 90 % of the police officers who have been systemized to it so far can be transferred to some "field activities".

VIII. Conclusion

Cybercrime and other illegal activities in relation to cyberspace, as well as concerns about the massive misuse of artificial intelligence, present a continuous challenge for modern police forces, where there is a fine line between threats and opportunities. Police forces must monitor related developments and actively respond to them, including in the form of commissioning and using the results of security research. The education of police officers and efforts to educate the wider public – which may otherwise be even more exposed to sophisticated fraud than before – also play a role. The Police of the Czech Republic is not an exception with its ambitions and efforts in this regard – insofar as it welcomes the related relevant experience of foreign partners.

IX. References

Assessment List for Trustworthy Artificial Intelligence for Self-Assessment. *European Commission*, 17 June 2020. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Babuta, Alexander and Marion Oswald. Data Analytics and Algorithmic Bias in Policing. *Royal United Services Institute for Defence and Security Studies*, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

Bílá kniha o umělé inteligenci. *Digi koalice*. https://digikoalice.cz/bila-kniha-o-umele-inteligenci/

Bohman, Martin and Oldřich Krulík. *Umělá inteligence jako bezpečnostní téma pro Evropskou unii a další mezinárodní organizace*. Mezinárodní bezpečnostní institut, 29 September 2021. https://www.mbi.expert/pracovni-list-umela-inteligence-jako-bezpecnostni-tema-pro-evropskou-unii-a-dalsi-mezinarodni-organizace/

Building and Verification Operation of the Cyber Threat Intelligence System. *Starfos*. https://starfos.tacr.cz/cs/projekty/VH20172021022

Complex Analysis and Visualization of Large-Scale Heterogeneous Data. *Starfos*. https://starfos.tacr.cz/cs/projekty/VI20172020096

Conference on responsible AI for Peace, Justice and Security. *Council of Europe*, 19 November 2020. https://www.coe.int/en/web/artificial-intelligence/-/conference-on-responsible-ai-for-peace-justice-and-security

Council of Europe and Artificial Intelligence. *Council of Europe*. https://www.coe.int/en/web/artificial-intelligence/home

Data Science and Criminal Justice. *Digi-Crim-Jus*, 6 July 2021. https://www.digicrimjus.com/2021/07/06/data-science-and-criminal-justice/

Development and Testing of Algorithms for Predictive Behavioural Analysis of Persons Crossing the External Borders of the European Union. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20182019034

Employment of Artificial Intelligence into an Emergency Call Reception. *Starfos.* https://starfos.tacr.cz/en/projekty/VI20192022169

Events about Artificial intelligence. *European Commission*. https://wayback.archive-it.org/12090/20210727053425/https://ec.europa.eu/digital-single-market/en/newsroom-agenda/event/artificial-intelligence

Evropská komise představila digitální balíček, včetně návrhů k umělé inteligenci a datům. *Úřad Vlády České republiky*, 20 February 2020. https://www.vlada.cz/cz/evropske-zalezitosti/aktualne/evropska-komise-predstavila-digitalni-balicek--vcetne-navrhu-k-umele-inteligenci-a-datum-179763/

Evropská strategie pro data. *Evropská komise*. 19 February 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066

High Risk Artificial Intelligence Applications: Internal Security Outlook. *European Commission*, 12 May 2021. https://www.statewatch.org/media/2407/eu-council-ai-internal-security-discussion-paper-8515-21.pdf

Integrated Platform for Analysis of Digital Data from Security Incidents. *Starfos.* https://starfos.tacr.cz/cs/projekty/VI20172020062

Interpol Virtual Academy. *Interpol*. https://www.interpol.int/How-we-work/Capacity-building/INTERPOL-Virtual-Academy

Interpol. *Artificial Intelligence Observatory and Forum*. http://observatory.ilaw.cas.cz/index.php/mezinarodni-aktivity/interpol/

Lost Persons, Offenders Position Automated Prediction Tool. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20182021039

Ministerstvo vnitra vyhlašuje veřejné soutěže na umělou inteligenci, robotiku a kyberbezpečnost. *Ministerstvo vnitra České republiky*, 2021. https://www.mvcr.cz/clanek/ministerstvo-vnitra-vyhlasuje-verejne-souteze-na-umelou-inteligenci-robotiku-a-kyberbezpecnost.aspx

Odbor informatiky a provozu informačních technologií. *Policie České republiky*. https://www.policie.cz/clanek/odbor-informatiky-a-provozu-informacnich-technologii.aspx

Policy and Investment Recommendations for Trustworthy Artificial Intelligence. *European Commission*, 2020. https://wayback.archive-it.org/12090/20210728103937/https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence

Posouzení dopadů návrhu Nařízení o umělé inteligenci. *Ministerstvo financí České republiky*, 3 May 2021. https://www.mfcr.cz/cs/soukromy-sektor/inovace-na-financnim-trhu/aktuality/2021/posouzeni-dopadu-navrhu-narizeni-o-umele-41759

Snímací zařízení pro krátké střelné zbraně. *Fakulta informačních technologií*; *Vysoké učení technické v Brně*. http://www.fit.vutbr.cz/research/prod/index.php?id=553

System for Text Analysis for the Needs of the Police of the Czech Republic. *Starfos.* https://starfos.tacr.cz/cs/projekty/VH20172017023

Táborský, Vladimír. Projekt „Reliéf“ na 44. evropské regionální konferenci interpolu v Praze. *Bulletin Národní protidrogové centrály*, 2016, No. 3, 43-46. http://future-forces-forum.org/review/236.str.2-.pdf

Tools and Methods for Video and Image Processing to Improve Effectivity of Rescue and Security Services Operations. *Starfos.* https://starfos.tacr.cz/cs/projekty/VI20172020068

Towards Responsible Artificial Intelligence Innovation. *United Nations Interregional Crime and Justice Research Institute*, 2020. http://www.unicri.it/towards-responsible-artificial-intelligence-innovation

Umělá inteligence – etické a právní požadavky. *Evropská komise*, 2020. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2020-3896535_cs

Umělá inteligence a lidská práva: rizika, příležitosti a regulace. *Vysoká škola AMBIS*. https://www.ambis.cz/umela-inteligence-a-lidska-prava-rizika-prilezitosti-a-regulace

Umělá inteligence v oblasti vnitřní bezpečnosti. *Policie České republiky*, PPR-21570-2/ČJ-2021-990770.

UNICRI Centre for Artificial Intelligence and Robotics. *United Nations Interregional Crime and Justice Research Institute*. http://www.unicri.it/in_focus/on/unicri_centre_artificial robotics

Virtual Conference on the Regulation of Artificial Intelligence, Ethics and Fundamental Rights. *Slovenia Presidency of the Council of the European Union*, 20 July 2021. https://slovenian-presidency.consilium.europa.eu/en/news/at-the-virtual-conference-on-the-regulation-of-artificial-intelligence-ethics-and-fundamental-rights/