DATA EXTRACTION DURING CBRN CRIME SCENE INVESTIGATION

ADATKINYERÉS CBRN KÖRNYEZETBEN

Dr. KAKUJA Izabella[1]

Abstract

Nowadays, it is not a curiosity that a crime scene is contaminated with various hazardous, noxious or CBRN materials. Consequently, the traces, lesions and personal effects left behind by the perpetrator at the scene will also be contaminated. To counter this, the collection of these traces, whether traditional or digital, is necessary. In the event that no CBRN contamination is found at the scene, it is possible to involve persons with specific expertise and to carry out laboratory tests on uncontaminated digital media. However, in the case of digital media contaminated with CBRN material, this is not an option. First the media must be cleaned, but then the problem arises that in the process the traditional traces and residues of the material can be damaged and destroyed. This meant that a method had to be developed whereby both traditional traces and digital data could be retained.

Keywords

CBRN contaminated crime scene, conventional and digital evidences, data extraction, chain of custody.

Absztrakt

Napjainkban nem kuriózum, hogy a bűnügyi helyszín, különböző veszélyes-, káros- vagy CBRN anyaggal szennyezett. Következésképp a helyszínen az elkövető által hátrahagyott nyomok, elváltozások, személyes tárgyak is szennyezettek lesznek/lehetnek. Mindezek ellenére ezen nyomok, legyenek azok hagyományos vagy digitális nyomok begyűjtésére szükség van. Abban az esetben, ha nem jelentkezik CBRN szennyezés a helyszínen, akkor lehetőség van speciális szakértelemmel rendelkező személyek bevonására, illetve a nem szennyezett digitális adathordozók laboratóriumi vizsgálatára. Abban az esetben azonban, mikor a digitális adathordozók CBRN anyaggal szennyezettek ez nem elérhető lehetőség. Először az adathordozókat meg kell tisztítani, azonban ekkor jelentkezik az a probléma, hogy eközben a hagyományos nyomok, anyagmaradványok sérülhetnek, megsemmisülhetnek. Vagyis szükség volt/van egy olyan módszer kialakítására, melynél a hagyományos nyomok és a digitális adatok is egyaránt megtarthatók.

Kulcsszavak

CBRN anyaggal szennyezett helyszín, hagyományos és digitális bizonyíték, adatkinyerés, felügyeleti lánc.

[1] kakujai@nni.police.hu | ORCID: 0000-0003-1324-033X | PhD student, University of Public Service, Military Engineering Doctoral School | PhD hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

INTRODUCTION

First, it is useful to clarify what the popularly known term "crime scene investigation" actually means in reality, far from the world of CSI (crime scene investigation) films. The concept of crime scene investigation itself can be interpreted in two ways: broadly and narrowly. In the narrow sense, it is exclusively a technical and tactical criminal investigation activity, carried out in practice, which serves and/or provides the investigation and evidence in criminal or administrative proceedings by searching for and recording traces and material remains on the spot.[1] While in a broader sense, and in addition to the above activities, it also includes the on-site activities of forensic experts (e.g. forensic, criminalistics), the criminalistics specialisation of canine forensics, and other criminal investigation activities (e.g. forensic traps), and by extension, education.[2]

Accordingly, it is advisable to carry out an on-site inspection where there is something to look for, i.e. where there are traces of evidence and material remains of a crime.[3] It is of particular importance all over the world as it supports both detection and evidence. To achieve its purpose, it requires forensic investigators who are always impartial, who do not look for patterns, but who systematically search the scene. They are aware that a negative trace is a trace.[4] That is, what is not there but should be there, or what is not there but was there. It often says more than the clue that is there.[5] So forensic investigation achieves its maximum objective when we have a highly qualified, impartial team of experts, a well-equipped technical equipment and a well-defined set of procedures defined by legislation and professional codes.

From all this, we can see that the collection of traces and material remains is the task of the crime scene investigation, whether traditional or digital traces. But it is important to give these words substance. Traces, lesions and material remains that are closely related to the so-called classical forensic areas of expertise (trace, weapon, fingerprint, handwriting) can be considered as traditional evidence, since they were created specifically for the purpose of forensic investigation.[6]

Social, scientific and technological changes in recent decades have brought with them the concept of the digital footprint. Social digitalisation as a process has had a significant impact on forensic activities, and it has become necessary to reform previously established procedures and ways of thinking. The use of IT experts for on-site inspections and the provision of equipment for investigating authorities to record and store digital traces have become justified.[7] Electronic evidence, like evidence obtained from digital devices or cyberspace, carries with it its variability and manipulability. For this reason, they are subject to special requirements in order to be admissible in court. I would like to note that the location of the data that can be used as evidence is of particular importance. This data may be stored on a phone, computer, printer or even in a car, smart device (fridge, fridge-freezer, vacuum cleaner, etc.) or the data may be stored only in the cloud.[8] [9] As you can see, digital traces and electronic data are extremely diverse and their storage locations do not always require a physical medium. In my presentation I will focus exclusively on data extraction from physical media.

In this spirit, therefore, "Evidence is only that which is credible and serves to establish the facts to be proved." [10]

The third set of concepts that we need to clarify is the acronym CBRN and their context in the crime scene. Nowadays, the acronyms ABV (Atomic, Biological, Chemical)

and CBRN (Chemical, Biological, Radiological and Nuclear) are used as synonyms for each other. Unlike the military term, CBRN refers to all hazards associated with chemical, biological, radiological and nuclear materials. It is understood that my presentation will only deal with CBRN materials that are out of control, i.e. where a criminal offence is involved. Because only there does the forensic investigation make sense. CBRN hazards pose serious health risks. It is therefore clear that they must be protected against. According to military rules, this is done in 3 steps. This is because ABV [16] protection is a complex system based on three pillars to protect personnel and technical equipment against any ABV attack. The elements of this three pillar system are avoidance, protection and relief.[11]

The concept described above is linked to policing by the nowadays intensified international terrorism and the intertwined CBRN terrorism as a possible instrument of asymmetric warfare. The arsenal and expertise of terrorist organisations is growing. Terrorist organisations and individual terrorists can threaten and achieve their goals by using radiological, toxic and infectious agents. These tools are therefore no longer just weapons of the regular army, but can also be used by extremist groups outside a war situation, even within a country.[12] In other words, the prevention, suppression, detection and proof of such acts, together with the criminal claim of the state, form the basis of police action. As we have already clarified in the concept of the on-site visit, in such cases it is necessary to gather as much evidence as possible, as this can determine the direction of the investigation and can also function as a decision support.

Once these basic concepts have been clarified, it will be clear to everyone that this is not a simple procedure, but a complex task requiring the involvement of a number of different disciplines.

INVESTIGATION, EVIDENCE COLLECTION

The presence of a CBRN element on the site makes the procedural act extremely difficult, since it is not enough to comply with legislation, professional rules and ISO standards, but all this has to be done under time pressure, in heavy protective clothing, with extra security rules and constant communication.

Preparation is also a complex process for this type of site. I will not go into this in my presentation - due to time constraints.

After the preparations, a primary reconnaissance is essential. This activity covers risk assessment, planning of the work and background measurement, followed by a surface contamination investigation (detection of possible spills, contamination), identification, marking and disposal of hot spots (e.g. elevated radiation levels indicating the presence of radiological material, or hot spots).

This is followed by the professional collection of the detected materials using forceps and manipulators. During collection, the safety rules and the ABV protocol must be followed to the maximum extent possible, and care must be taken to avoid contamination (cross-contamination). This is important for two reasons. Firstly, the contamination should not be taken off-site, i.e. no new contaminated area should be created. Secondly, do not contaminate yourself or the crime scene. This can be achieved by always having a "clean" technician on site and having him/her provide the crime bags for the crime scenes and/or by changing gloves between each sample collection. Avoiding cross-contamination is also important for the integration of crime signals. A continuous video and photographic record of

the crime scene shall be made beforehand and during the procedure, including the activities of the forensic technicians, as the procedure itself shall comply with the requirements of the MSZ EN ISO 21043 series of standards, Parts 1 and 2.[17]

All material leaving the scene, including collected crime scene evidence and any equipment used for searching or recording, as well as any instruments or equipment used to detect the material, must be re-measured in the clear zone. They must also be decontaminated (cleaned) there.

After CBRN materials have been collected, repeat measurements should be taken at the site to see if there is any contamination remaining at the site. If not, the site can be handed over to the forensic team and the level of personal protective equipment can be reduced. In the event that contamination remains at the site, the site should be processed under expert guidance. The primary step in this process is to prepare a "TRIAGE" of the crime scene to be collected. The priority here is always to collect first those that can be easily destroyed and that directly point to the perpetrator. Then digital evidence and traditional evidence whose degradation is not immediate. As regards digital evidence, I will only discuss those on physical storage. The treatment of collected digital evidence is identical to the treatment of traditional evidence, as it is subject to the same legislation.

In the case where the digital storage devices are not contaminated with CBRN material, then everything goes its own way, since it is a crime scene from a criminal inspection. Data recovery can begin in the clear zone. If it is not possible or necessary to use other technologies, the data or data storage devices can be removed from the site for further analysis. This means that evidence collection and data extraction and analysis can take place at the same time and in parallel at the site visit. However, in cases where the data storage device is contaminated with CBRN material, the possibilities are limited, as there is no possibility to analyse the data content in a conventional way. We can only start the investigation if we can protect the technical staff, the bystanders, the experts and the site from contamination. In such cases, the data recovery can be carried out by placing the data storage devices issued from the site in glove bags at the same time as the on-site inspection, so that the data recovery officer can work in safe conditions and start the necessary investigations at the same time.(e.g. data recovery can start at the same time as the DNA residue capture - in the case of a telephone device - using UFED technology[18]. However, this procedure implies that the person performing the data collection must also learn at least at a basic level and adhere to the ABV protocol, i.e. wear the specified personal protective equipment in the specified manner and for the required time while performing his or her task. This implies that the data recovery expert should be prepared, if only minimally, for such situations, should be familiar with the protocols, should learn to wear the required personal protective equipment and should be able to perform a high quality job in doing so. He/she must learn the discharge procedures and be able to apply them at a skill level.

The question arises, why is this important?

Well, because traditional crime-signal capture, digital data extraction and CBRN material characterisation are done simultaneously, while still on site, and the immediate secure transmission of the resulting data significantly increases law enforcement competence. There is no doubt that this capability is extremely important in the event of a terrorist incident. If we are able to send video footage of the scene in real time to the command post,

transmit the photographs via a data link as soon as the photograph is taken, then through coordinated action, partner agencies, other experts, law enforcement agencies, even in other countries, can receive a live picture (on an encrypted channel) in real time, thus assisting the team working in the investigation zone or passing the information to the appropriate agency.[13] Also unique to the Hungarian method is the ability of forensic staff to instantly deliver a scaled photograph of traditional crime scenes to forensic institutions, where data processing can begin during the crime scene, so there is no time delay, while the chain of custody of evidence continues.

Figure 1: Safe extraction of radioactively contaminated mobile phone data using a UFED tool, while also capturing DNA residue (Photo: D. Calma UN IAEA)

CONCLUSIONS

The risks posed by CBRN hazards are ever-present in today's world, and therefore the maintenance and development of CBRN detection capabilities remains justified.[14] Education and training of specialist personnel is also important. However, there is a lack of training in this area, as it is not included in the training of forensic technicians. To overcome this, it is proposed to prepare an educational theme specifically for those working in this field, and later to provide theoretical and practical training along this theme.

A crime scene investigation is essential, but CBRN materials complicate the process, as in addition to forensic staff, the presence of people with specific expertise is required who need to know the basics of site inspection. Currently this is also a gap, so the proposal is similar to those mentioned earlier. In other words, the CBRN expert should be familiarised with the basics of the site investigation and the techniques of investigation and

detection, in order to enable the two disciplines to work together as effectively as possible during the procedure.

In addition, if digital evidence is to be extracted, the expert needs to be exposed to both areas, and there is a gap in this area. Proposal follows on from the above. There is a need to ensure interoperability between the knowledge materials of the different disciplines and to ensure knowledge transfer.

In addition to all this, we must not forget to acquire the right equipment and to keep improving it. And the tools must be adapted to the specificities of the field inspection.

At the same time, the coordinated, high quality execution of these activities can result in a powerful unit capable of maximum data collection and analysis in a short time and, when transmitted, can result in a fast, effective law enforcement.

However, one possible direction is to train crime scene technicians to be able to perform such tasks at a basic level. In this case, however, it will still be necessary to involve an expert to analyse the data, i.e. although data analysis and inspection will be carried out in parallel, the on-site data analysis will still require the expert to be familiar with the ABV protocol.

SUMMARY IN NUTSHELL

To summarise the above ideas, in today's digital world, law enforcement agencies cannot afford to ignore electronic data on storage media and in cyberspace. The European Commission's Digital Single Market Strategy for 2015 also argues that the internet and digital technologies are transforming our world.[15] This is precisely why digital data and its carriers cannot be ignored during a site visit, as there is often more data in virtual space than in reality. If all this can be used as evidence in subsequent proceedings, law enforcement agencies can work more effectively.

Data collection may be necessary in all cases, even if the environment is contaminated with CBRN material. So you have to be prepared for this. Partly by education, partly by ensuring knowledge transfer. On the other hand, in the case of a real site, it is necessary to be able to concentrate the technical equipment, the specialised staff with the appropriate knowledge in one place, and to be able to coordinate both the activities and the use of the equipment in the case of several subtasks requiring specialised knowledge. This is the key to efficiency.The sooner and more efficiently coordination can be achieved, the faster and more effective law enforcement will be.

BIBLIOGRAPHY

[1] Csaba Fenyvesi: *The forensic characteristics of the on-site inspection*. PTE ÁJK Pécs, 2009 p. 1.

[2] Gergely Gárdonyi: *CSI Hungary - Facts and Perspectives in Hungarian Crime Scene Investigation* In: Gyula Gaál-Holtán Hautzinger (eds.) Studies from the scientific conference "QUO VADIS police protection? QU QU QU QUO QUO QUALITY QUESTIONS", Pécs, 2010, 104-110 p. [Pécs Border Guard Scientific Publications XI.]

[3] András Benkő - András Huszár - István Szilvásy. In Zoltán Hautzinger (ed.): *Studies on the scientific conference "Border Guard on the Path of Quality*". Hungarian Military

Science Society Border Guard Section Pécs Section, Pécs, 2005, pp. 255-256 [Pécs Border Guard Scientific Publications IV.]
[4] János Dobos: *Negative conditions on the ground*. Internal Affairs Review, 1964/1, pp. 54-59.
[5] Csaba Fenyvesi: *Criminal chess game in the mirror of criminological principles* Internal Affairs Review 2016/11. number, pp. 40-57.
[6] Gabriella Kármán, *The Criminalistics Expert Evidence - The Building Blocks of Credibility* Institute of Criminology, Budapest, 2019, 137 p.
[7] Zoltán Mráz: *The importance of digital evidence tools in the investigation of crimes against property* Internal Affairs Review, Budapest, 2018, 7-8, p.
[8] Zoltán Kovács: *The potential applicability of cloud-based IT systems in law enforcement agencies*- Military Engineer, Volume VI, Issue 4, December 2011, page 177, source: http://hadmernok.hu/2011_4_kovacsz.pdf, downloaded: 2023.09.01.
[9] Gyaraki Eszter Réka: *Problems of computer crime investigation*, PhD thesis, Pécs, 2018, 69. pp.
[10] Vilmos Garamvölgyi - László Viski (eds.): *Kriminalisztika*. Ministry of Interior, Department of Studies and Methodology, Budapest, 1961, p. 688.
[11] Juhász László: *Nuclear, Biological and Chemical (ABV) Reconnaissance, Leadership and Management and Organization*, https://docplayer.hu/24496254-Az-atom-biologiai-es-vegyi-abv-felderites.html downloaded: 10.09.2023.
[12] T. Berek - R. Pellérdi: *Responding to CBRN challenges in the EU* 2011. Bolyai Szemle, Vol. XX, No. 2, http://portal.zmne.hu/download/bjkmk/bsz/bszemle2011/2/Berek_Pellerdi.pdf
[13] Izabella Kakuja: *Unique Hungarian method in radiological crime scene managent*, Budapest, 2022, Military Technology, LVI. year - 2022/5, 58-62
[14] László Juhász: *Nuclear, biological and chemical (ABV) detection* https://docplayer.hu/24496254-Az-atom-biologiai-es-vegyi-abv-felderites.html downloaded: 10.09.2023.
[15] Béla Simon: *Digital challenges facing law enforcement Hungarian Policing* 2017/5. 83-103
[16] The abbreviation ABV is used in MH documents according to the 2009 Uniform Guidance of the MH Standing Working Group on Chemical Defence of the Armed Forces Section
[17] MSZ EN ISO 21043 Forensic science. Part 1: Terminology and definitions Part 2: Searching for, documenting, collecting, transporting and storing evidences (Author)
[18] A UFED (Universal Forensic Extraction Device) is a device for extracting and decrypting information from almost all phones on the market, even those with lock protection. It can be used to retrieve call logs, even for deleted SIM cards, phone numbers, images, videos, audio files, or even graphical geographic labels. (Author)