FIGHTING THE CLASSICAL CRIME-SCENE ASSUMPTIONS. CRITICAL ASPECTS IN ESTABLISHING THE CRIME-SCENE PERIMETER IN COMPUTER-BASED EVIDENCE CASES

Cristian DRIGĂ[*]
Svetlana PURICI[**]

Abstract

Physical-world forensic investigation has the luxury of being tied to the sciences governing the investigated space, hence some assumptions can be made with some degree of certainty when investigating a crime. Cyberspace on the other hand, has a dual nature comprising both a physical layer susceptible of scientific analysis, and a virtual layer governed entirely by the conventions established between the various actors involved at a certain moment in time, defining the actual digital landscape and being the layer where the actual facts relevant from the legal point of view occur. This distinct nature renders unusable many of the assumptions which the legal professionals and the courts of law are used to operate with. The article intends to identify the most important features of cyberspace having immediate legal consequences, with the purpose to establish new and safe assumptions from the legal professional's perspective when cross-examining facts that occurred in cyberspace.

Keywords: *cybercrime, criminal law, digital evidence, cyberspace, forensic investigation.*

1. Introduction

Bringing criminal cases involving computer generated or stored evidence, as well as crimes committed entirely through information systems to justice is a major challenge for the legal system in general and for all the actors involved, ranging from the investigators, to prosecutors, judges and defense attorneys. The judicial system relies heavily on assumptions developed during a long time in processing physical-world crime cases. The rapidly-evolving digital age crimes, being partly or totally committed inside a new medium with different properties than the physical world, requires major changes in the way in which the legal professionals regard the criminal cases. While the laws slowly adapt, a more rapid adaptation can be achieved through understanding cyberspace and its governing "laws" as well as through putting aside the classical crime-scene assumptions and developing new ones. This article intends to identify such assumptions that cannot be used anymore in the digital crime cases and attempts to identify new assumptions that are safe to operate with in the pursuit of justice in the digital society.

2. Generic assumptions in regular crime cases

If a common crime takes place in a closed room, chances are that at the crime scene, evidence on how it was committed could still be found intact. On the other hand, for crimes committed in the street and public places, chances to find the same evidence intact are almost zero, given the multitude of elements that could destroy it. Similarly, while in closed space crime cases the possible suspects could be narrowed down to those having access or entering that particular room, in public-space crime cases, anyone passing by leaves a trace, thus being a potential suspect. These are typical assumptions that can be made with some degree of certainty when starting a forensic investigation in the physical world.

The key role of such assumptions is to help streamlining the first step in the forensic investigation[1], namely establishing the perimeter from where relevant evidence could be collected, the possible sources of information, the methods and tools that should be used and the type of evidence that could be obtained, and, in the court of law, to help analyzing the results of the investigation.

3. Assumptions in cyberspace crime cases

In criminal cases involving computer generated or stored evidence, as well as in crimes committed entirely through information systems, a new dimension is added to the traditional three dimensional space of the perimeter to be established as a first step in investigation: the cyberspace[2].

Be it the personal digital space or the greater public Internet, its unique properties like the ability

[*] Attorney at law Cybercrime Research Centre Assoc., Iasi, Romania (e-mail: **contact@cybercrime.org.ro**).
[**] Ph.D. student Svetlana Purici, Moldova State University, Faculty of Law, Chisinau, Moldova (e-mail: **purici.svetlana@gmail.com**).

[1] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Crime Scene Investigation: A Guide for Law Enforcement (2000)*, 19.

[2] http://thelawdictionary.org/cyberspace/

to cross the limits of rooms and buildings, national borders or even continents, as well as the multitude of devices and electronic services which may be part of it, raise a whole set of issues both for investigators as well as for the legal professionals. In such cases neglecting one possible source of evidence or failing to correctly establish the digital perimeter of the investigation[3], could easily lead to either failing to prove the offender guilty beyond any reasonable doubt, or worse, to grave judicial errors.

Even if it contains the notion of "space", the cyberspace does not possess the same properties the physical world has, rendering unusable many of the assumptions the legal professionals are used to operate with in the real life crime cases. Even if the forensic investigation ultimately examines physical devices seized from a specific physical location and the information stored inside them, prosecuting, judging or defending a suspect in a computer related crime case requires a good understanding of the nature of cyberspace and its properties as well as putting aside some of the real-world crime case assumptions.

Possibilities such as remote access and control of computer systems, automation of computer crime through malware programs, on-line identity theft, anonymization techniques as well as hijacking network identity, are but a few of the extremely common situations in cyberspace with significant legal consequences that need to be tackled since the early stages of the forensic investigation and thoroughly examined during the trial phase in the courtroom. The difference between guilty and not guilty can ultimately go down to the difference between 0 and 1 in a bit of information discovered inside an information system which was either neglected or correctly understood.

For instance, the closed room assumptions are not applicable to computers connected to the Internet no matter if the room containing the computer was even locked from inside. Also, if the computer through which the crime was committed belongs to a certain person does not make that person the author of a particular crime. On the contrary, given the statistical occurrence of computers being part of automated bot networks committing crimes[4], or the frequency of the computer malware infections providing remote access to perpetrators, transforms the personal virtual space into a public place, making it more likely in some cases to reverse the initial assumptions or to establish new ones, in order to safely operate when investigating cyberspace in the pursuit of justice.

As a different medium with its own unique properties and interactions, the cyberspace can provide relevant evidence which correctly understood as nature and properly collected, preserved, analyzed and interpreted, could make the difference between sound cases from the legal point of view and terrible prosecution failures. In courtroom, understanding the nature of electronic evidence, the interactions that could take place and the unique properties of the cyberspace, could level up the degree of certainty when sentencing the offender.

4. The nature of cyberspace

Traditional dimensions VS. dimensions established through conventions

The physical-space forensic investigation has the luxury of being tied to the laws of the science governing the investigated space or the nature of the objects in question (physics, chemistry etc). Cyberspace on the other hand, has a dual nature which brings in new variables into the forensic equation which are of critical importance from the legal point of view in establishing the truth in criminal cases:

The physical layer or the infrastructure - governed by the laws of physics (namely electricity, mathematics, etc) and comprising of the actual physical information systems, devices and networks subject to containing the evidence in form of digital information;

The virtual layer - built entirely from the data stored in or circulating the systems and networks, it comprises the software programs and services available at a certain moment in time, together with their automatic or user generated information, the usage rules and possible actions and interactions between systems, programs or services, the intended behavior or the actual behavior at given time of certain devices, software programs, services or computer systems. It basically defines the landscape in the digital space, the actions that could be taken by an individual and the data either automatically or user generated. As a distinct medium, the virtual layer is governed entirely by the conventions established between the various actors involved at a certain moment in time.

Both layers are of great importance when analyzing the virtual crime scene. While the former provides the actual information bits, the latter, correctly identified and analyzed allows the re-construction of the facts as they happened in a particular case.

The physical layer, being the closest to the physical world, thus susceptible of scientific analysis, defines certain characteristics of the information it could contain, leading to mandatory actions and precautions to be taken in the forensic

[3] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition (2008), 19.

[4] Romanian Computer Emergency Response Team, *REPORT on Cyber Security Alerts processed by CERT-RO in 2014,* (2015).

investigation in order to produce results admissible in court as evidence. The virtual layer instead, being the sum of both formal and informal conventions between software developers, hardware manufacturers and/or service providers to which we add the user actions and the user generated information, is subject to continuous evolution, its properties continuously changing, hence the impossibility to establish the same principles and assumptions from the classical criminal cases. However, being the layer where facts occur, it is of the utmost importance in assessing the events in a manner that could be relevant for the court.

5. Legal issues in virtual-space crime cases

Lawful usage, Terms of usage, Liberty of usage.

Regulating the Internet and the cyberspace in general is a hot legal topic under continuous development at international level[5]. Laws and treaties are developed to establish standards to which the various actors should adhere, in order to bring in some predictability in cyberspace that would allow more in depth enforcing of the real world established laws into the virtual society, shaping at least part of the virtual space through legal means.

As a trend in regulating cyberspace we see tremendous efforts in imposing new laws to the service providers which offer the infrastructure for the information society. However, beyond the physical infrastructure, few laws manage to properly regulate the actual virtual cyber-landscape in a manner that would increase the number of assumptions which can be made in investigations, therefore, efforts should be made in each case and trial stage for assessing the degree in which the perimeter of the crime, through its actors, was compliant with the applicable legal provisions.

Laws attempting to regulate the actual virtual space are usually implemented by the service providers through technical means enforcing a certain behavior or usage scenario, as well as through terms of usage of services, placing the legal responsibility to the end-users. Both aspects may become relevant in some of the cases in court in an attempt to determine the actual circumstances of a case.

Trust-related issues in cyberspace investigations.

Being established through conventions between multiple entities, as opposed to the physical space in which laws of physics, chemistry and other sciences are always applicable, cyberspace as a forensic investigation perimeter requires assessing the medium-specific properties, the boundaries and the applicable "laws" at the moment when the crime was committed. Being spread across multiple systems, networks, regions and participating entities, the investigated perimeter is highly dependent on the trust that can be attributed to each and every actor involved.

One important step, easy to neglect when starting an investigation, is to establish a thorough list of the participating entities from which, further on, the entities that can be trusted should be established both as source of evidence and for crossing them out from the list of suspects. The Internet being a public place, the open-street scenario and assumptions are the safest to apply even for computers with apparently a single user in a room locked from the inside.

In courtroom, the *presumtion of innocence* and the *benefit of the doubt* as two of the founding blocks in criminal justice, are most likely to throw out cases in which the aspect of throughly identifying the participating entities and properly addressing the issue of trust for each of them was neglected.

Discovering the perpetrator earlier, without assessing the "circle of trust" and delimiting it from the "circle of possible suspects" can be considered at most a lucky occurrence. Indeed such event reduces the costs and the investigators can move to the next case. From a technical point of view the findings may even prove right, but without the admission of committing the crime or without other non-digital evidence to corroborate the facts in the absence of admission, chances are that either the defense will appeal to the benefit of the doubt or, in case all parties ignore the issue, judicial errors might occur.

Time-related issues.

Being a continuously changing landscape, the cyberspace, even if it comprises of a single device, puts pressure on the investigators to capture a snapshot of the virtual perimeter at the moment when the crime occurred, either by reconstructing it from the recovered digital evidence seized from storage mediums belonging to the suspect, or by literally freezing parts of the information circulating through trusted provider's networks and servers using the proper procedural legal means.

The time issue, from the legal point of view is directly dependent on the trust issue and failing to assess if the time was correctly set and recorded in the investigated systems and in the network or service provider's systems, can lead to errors in identifying the perpetrator, especially in cases where identification relies on this correlation as the only means to connect the crime to the suspect's computer.

Network infrastructure assessment and legal compliance.

One such aspect relevant in court of justice, in cases where the device investigated is connected to

[5] Organization for Economic Co-operation and Development, *The role of internet intermediaries in advancing public policy objectives*, (2011).

the Internet, is the degree in which the service providers (Internet service providers ISPs, On-line service providers, etc.) comply with the applicable laws (for instance by implementing all the technical means required by the law) thus offering some degree of certainty regarding the evidence they provide and the facts that occurred in a certain criminal case.

Aside from the problem of jurisdiction under which a certain piece of the personal virtual space of the suspect or some of the digital evidence resides, assessing the real status of the Internet service provider offering connectivity to the suspect is more likely to be cross-examined by the defense in search for vulnerable spots of the investigation.

The *presumtion of innocence* in case of computer networks requires eliminating all other scenarios in which the perpetrator is somebody else than the suspect. For instance, if by any chance the ISP is not a legally established service provider but instead an individual providing Internet in a private network spanning several flats or buildings, the circle of suspects is mandatory to be enlarged to all the systems in the network and to their owners. Same situation applies when the connection to the outside word is made through a network switch instead of a router, or without having implemented proper technical means to detect or eliminate the impersonation of the suspect's computer by someone else in the network. Failing this assessment and to correctly identify the limits of the physical network at the time of the domiciliary raid can either lead to judicial errors or to providing ammunition for the benefit of the doubt defense strategy in court.

At procedural level, of a special importance are the legal instruments chosen to complete the steps of seizing and collecting the digital evidence from the service providers. Non-repudiation, juridical responsibility for the contents and integrity of the data, are but two of the most important legal aspects subject to scrutiny in the court of law.

The Entry Points legal issue.

The virtual space being collectively built and designed for interaction and spanning numerous devices, networks, software programs and services, presents as many entry points for someone to commit a crime as the multitude of elements comprising it.

This specific nature of the virtual space makes it impossible for digital investigations to address all the entry points in a manner that would eliminate entirely the possible alternative scenarios of committing a crime. The reason for this assumption is mathematical and is based on the myriad of combinations that can be achieved by inter-connecting the physical elements sustaining the virtual space, to which we add the possible combinations between the software programs, services and human elements interacting and defining the investigated virtual space.

To tackle the multiple entry points problem, the best-practice manuals always recommend performing classical police investigations in addition to the digital investigation prior to submitting the case to court. Classical evidence would short-circuit some of the most common defenses which appeal to the benefit of the doubt derived from the possibility that the crime was committed by someone else.

From the legal point of view, failing to address the physical open points in which the perpetrator could've commit the crime by hijacking for instance the network identity of the suspect through IP spoofing or ARP spoofing techniques, will always be exploited by the defense.

Other commonly met defense scenarios in the court of law exploit the software related entry points, such as the possibility of remote controlling a computer system as well as the automation of such control through computer viruses and similar means, the Trojan Horse defense[6] being such an example scenario, in which the defendant denies responsibility for committing the crime given the presence of viruses inside his computer systems which could either provide remote control capabilities to the actual criminal located somewhere else or could automatically commit the crime, in both cases without the knowledge of the defendant.

Staying current with the latest developments in the cyber-security field, given the raise of numerous new methods of penetrating a network or someone's computer, and especially with the statistics regarding the occurrence of certain types of attacks and exploitation of IT infrastructure can also indicate some of the alternative perpetrator scenarios that should be addressed and eliminated when building the court case.

6. Final remarks

Given the volatile and always changing nature of cyberspace, classical crime-scene assumptions are but a source of errors for the legal professionals in re-constructing the facts that occurred in committing a computer related crime. The legal system is used to rely on technical experts to gather the relevant data and to “translate” it into the concepts with which the legal professionals are used to operate.

Given the distinct nature of cyberspace, no matter how good the “translation” is, the findings and the information that can be obtained from the technical experts, processed using the physical-space crime-scene assumptions, could lead to miss-interpreting the evidence. Without understanding the properties and the possible actions in the investigated medium, the cross-examination in

[6] Susan W. Brenner, Brian Carrier, and Jef Henninger, *The Trojan Horse Defense in Cybercrime Cases*, 21 Santa Clara High Tech. L.J. 1 (2004).

courtroom is more likely to fail in discovering the truth and the parties involved in the trial are often put in the impossibility to grasp the relevant aspects and nuances of the facts, in order to further ask the experts the right questions.

The forensic examination of the physical electronic devices is subject to standardization. Adherence to standards is key to securing the evidence and collecting it in a forensically sound manner.

But the physical devices are but a small part of the cyberspace. The rest of the investigated perimeter, where the facts actually occur, being so volatile and differing from case to case, can only be subject to best-practice manuals in an effort of establish common would-be standards. To cope with this problem, understanding the cyberspace nature and a thorough examination of the virtual landscape in all stages of the trial as well as staying informed with the latest relevant evolutions in the field become mandatory even for legal professionals.

In the pursuit of justice, in cases involving digital evidence and cybercrime, the common assumption that being related to computer systems makes it solely the job of computer experts to understand the nature of cyberspace, becomes the most important assumption to put aside.

Resources:

- U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Crime Scene Investigation: A Guide for Law Enforcement.* (2000). Available at: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/twgcsi.pdf
- U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition (2008). Available at: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- Romanian Computer Emergency Response Team, *REPORT on Cyber Security Alerts processed by CERT-RO in 2014* (2015). Available at: http://www.botfree.ro/articles/pages/en/2015-05-15-article-cyber-security-alerts-2014.html
- Organization for Economic Co-operation and Development, *The role of internet intermediaries in advancing public policy objectives* (2011). Available at: http://www.oecd.org/internet/ieconomy/ 48685066.pdf
- Susan W. Brenner, Brian Carrier, and Jef Henninger, *The Trojan Horse Defense in Cybercrime Cases*, 21 Santa Clara High Tech. L.J. 1 (2004). Available at: http://digitalcommons.law.scu.edu/ chtlj/vol21/iss1/1