1. INTRODUCTION

The vast and rapid development in the Internet and Information Communication Technology (ICT) in general has created a new dimension in our world, that is, the cyberworld or cyberspace. In this dimension, almost everything has become possible. Individuals and organizations are extensively using this cyberspace in their daily transaction just like our physical world. This has created a series of competitions in many aspects, such as, e-commerce, e-learning and even e-government portals. The main challenge in the cyberworld is that we deal with virtual world where identities can be hidden or hijacked. Thus, the term cybersecurity has become one of the fundamental pillars in the cyberworld. Cybersecurity has become a common practice and attached to nearly everything connected to the Internet. We usually hear about a friend or a person we know who was hacked, or perhaps, a company that was scammed by an e-mail and lost a considerable amount of money. To many individual, especially those who are specialized in computer and software engineering fields, the concept of hacking, scamming, social engineering, etc., may sound simple and straight forward. However, the shocking fact that in a matter of a few years, major organizations have been hacked and the consequences were major losses and damages\(^1\). In this regard, there is always worst case scenario where some organized cyber attackers may take over the control of some critical facilities, say missile firing control system, Unmanned Combat Aerial Vehicle (UCAV) or a nuclear reactor perhaps. In this case, catastrophic consequences may happen causing, apart from cost effects, major destruction events in the world.

Any violation of criminal law leads to a crime, yet considering the use of computer and Internet, the crime would be described as “cyber-crime or cybercrime”. According to a number of references, specialized in computer criminology\(^2\), there is no real consensus on the definition of cybercrime, however, it can be defined as “an act that covers the entire range of crimes which involves computer, computer network, cell phones, etc., either as its target or as an instrumentality or associate.”\(^3\). These cybercrimes may be represented in the form of licensed programs cracking and piracy, any sort of e-mail offence including: hacking, spoofing, abusing, threatening, and identity theft, scamming, spam and phishing, social engineering; and it may also be performed by more complicated methods such as remote administration tools and carding. Furthermore, there is one of worst cybercrimes against humanity that is online child sexual abuse material. A detailed discussion on cybercrime categorization will be presented in section two. It is important to mention that cybercrimes are also categorized based on the severity according to the judicial system. Thus, this has created a relatively new aspect in criminology concept which is directly related to the cyberspace and laws applied to it. In this regard, variety of recent publications have been produced to study the criminology terms related to cybercrimes and computer crimes, in an explicit attempt to formalize laws, policies, and solutions applicable to and coping with these crimes. For instance, Burden and Palmer\(^4\) published an article explains and summarize some of the key areas of online criminal activities.

They also proposed placing these crimes in the proper judicial context. Relatively similar to the previous idea, Sommer\(^5\) connected policing cybercrimes and issues facing the criminal justice system in the UK. He had attempted to formulate a practical solution to cybercrime from judicial prospective, especially related to digital forensic cases, where he proposed the implementation of software toolkits on computer systems that would assist in apprehending and prosecuting cyber criminals after obtaining enough evidences. Nykodym et al.\(^6\) provided a profiling approach based on some specific characteristics do regularly exist in cybercrimes. According to their article, companies are being much affected by insider offenders and an accurate profile of an inside cybercriminal may help in identifying both prospectively and retrospectively. Nykodym and Taylor\(^7\) proposed in their article that victims of cybercrimes should be able to legally follow the criminals worldwide via an international collaboration for cybercriminals prosecution. Variety of other articles thoroughly discussed related cybercrime issues on national basis\(^8\), \(^9\), \(^10\) and international basis\(^11\), \(^12\).

The judicial terms vary based on the committed crime so are the consequences to be considered. One of these judicial terms is probation, which is defined as “a method of dealing with specially selected offenders and consists of the conditional suspension of punishment while the offender is placed under personal supervision and is given individual guidance or treatment”\(^13\). As the definition suggests, the conditional suspension of punishment is given to selected offenders based on certain criteria vary according to the sanction. In this regard, probation in traditional crimes has been widely investigated on both local and international senses, and there are hundreds of articles based on probationary terms for both probation practitioners and managers, yet this term is considered relatively new in cybercrimes and sanctions related to them. Therefore, in this paper, we will be discussing the probation in cybercrimes according to the followings: section two is presenting the investigation process in both cybercrimes and traditional crimes, section three is covering the cybercrime legislation, and the final remarks and conclusions are presented in section four.

2. INVESTIGATION PROCESS: CYBERCRIMES VS. TRADITIONAL CRIME

In common crime cases, the investigation process starts by confirming the occurrence of crime. Once the authorities determine that a crime has taken a place, they initiate a few formal steps starting by collecting evidences and search and arrest if the court decides to press charges for a reasonable cause. Collecting evidences is generally done to support the prosecution case; these evidences should be lawfully gathered otherwise it may be considered by the judge as inadmissible\(^14\). The reliable and proper evidences can be in the form of forensic evidences, eye witnesses’ statements, photos, video/audio records, and written notes. Once the evidences are gathered, specialized personnel use advanced technologies to identify matching from fingerprints, DNA, etc. which lies under forensic procedures. According to the results of forensic procedures and other relevant evidences analysis, a search warrant shall be issued based on reasonable grounds.

In cybercrime sense, very similar scenario takes place, yet the main difference is that evidence collecting is more
likely to be based on digital forensics. Here, a deep knowledge in computer, networking, cyberspace, and cybercrimes should be considered prior the starting of any investigation step. The general issue is that computer related areas as well as ICT are rapidly evolving and may cause confusion leading to serious obstacles on the way of prosecutors. Unlike traditional crimes, acts, sentences, law statements, and detailed policies related to cybercrimes yet to be established and provided to the judicial system. Furthermore, as the technology evolves, this issue gets more complicated and intensified. Various cases have been studied in literature in an attempt of increasing the awareness of law makers to the aforementioned issue. In an attempt of alleviating this complication, some researchers have proposed a detailed classification of cybercrimes. Table 1 provides a summary of cybercrimes classification based on the work of Alkaabi et al\(^\text{15}\). In this classification approach, the authors proposed categorizing cybercrimes into two main groups based on role of the computer, as a milestone. Even though this classification is useful yet it is not adequate for digital evidence collection.

Table 1: Cybercrimes Classification

<table>
<thead>
<tr>
<th>Classification</th>
<th>Role I</th>
<th>Role II</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion</td>
<td>The computer is being targeted by criminal activities:</td>
<td>The computer is being used as a tool for criminal activities:</td>
</tr>
<tr>
<td></td>
<td>- Unauthorized access offences such as hacking</td>
<td>- Content violation offences such as possession of child pornography, unauthorized possession of military secrets, IP offences</td>
</tr>
<tr>
<td></td>
<td>- Malicious codes offences such as dissemination of viruses and worms</td>
<td>- Unauthorized alteration of data, or software for personal or organizational gain such as online fraud</td>
</tr>
<tr>
<td></td>
<td>- Interruption of services offences such as disrupting or denying computer</td>
<td>- Improper use of telecommunications such as cyber stalking, spamming, and the use of carriage service with the intention or conspiracy to commit harmful or criminal activity.</td>
</tr>
<tr>
<td></td>
<td>- services and applications such as denial of service attacks and Botnets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Theft or misuse of services such as theft or misuse of someone’s Internet account or domain name.</td>
<td></td>
</tr>
</tbody>
</table>

As we mentioned earlier, evidence gathering is usually based on crime scene and its related objects. In this regard, cybercrime may much differ from what traditional crime in a way that tracking evidences occur in the cyberspace. It is often that data retrieval process takes place as a first step in cybercrime investigation where the concern is guided towards whether the data have been moved on the Internet or not. If it is an Internet-based, which is usually the case, then investigators extract the Internet Protocol (IP) to find out who exactly owns and operates the network address, any associated domain or computer name, physical location, any email addresses and Internet Service Provider (ISP) if possible\(^\text{16}\). Accessing the Internet is based on a subscription to companies which ultimately grant or provide the Internet to their users; it is possible to keep track on data movements within ISPs yet time plays an important role here. As the time goes by, retaining data from subscribers may vary. Upon any suspicious activities, investigators usually request ISPs to preserve the data until an official warrant has been issued for the sake of records review. In case there are victims, investigators conduct interviews with them as well to identify any possible leads to the criminal. It is likely for investigators to ask questions related to technology and directly related to computer and Internet sensitive areas, such as, login passwords, network administrator, firewall issues, data backup programs, any relevant recently installed software\(^\text{17}\). This


\(^{17}\) US Department of Justice, Investigative Uses of Technology: Devices, Tools, and Techniques, National Institute of Justice; available online at ([https://www.ncjrs.gov/pdffiles1/nij/213030.pdf](https://www.ncjrs.gov/pdffiles1/nij/213030.pdf))
procedure is useful prior to moving to gathering digital evidences. Digital data are stored in different ways, yet it is very important for investigators to go through any data or data parts during the investigation as they may provide the lead. Formal investigation procedures for digital evidence include: Internet activities in any sort of social media interaction, e-mail correspondence, data movements (download and upload), online shopping, banking transaction, online chatting, etc. All these evidences shall be analyzed during the course of cybercrime investigation where hidden and deleted data should be fully, or at least partially, retrieved for further analysis.

As the technology evolves, digital crime analysis tools should also keep track on up-to-date levels of committed cybercrimes. A careful attention should be given to misleading information an identity theft, not to end up accusing the wrong person. This aspect is more confusing in cybercrimes where identities can be hidden or fraud in worse cases. It is important to mention that in cybercrime evidence collection, evidences from the physical world should be also included, such as phone calls of suspects and victims as well as CCTV records for crime scenes if any. Investigators usually act based on severity of the crime and request collaboration from different departments for the sake of smooth and successful investigation.

3. CYBERCRIME LEGISTLATION

Cybercrimes are crimes committed within the cyberspace. This implies that the impact of cybercrimes may affect any part of the cyberspace which covers, theoretical, the whole globe. Isolating cybercrimes on national basis is not a wise decision, yet the concept of cybercrime legislation should be considered on both national and international communities. Ever since the invention of computer, computer related crimes have been happening. However, connecting computer workstations to the Internet has created sophisticated cybercriminals in the form of individuals and groups. Unlike traditional crimes, the victims of cybercrimes may not be from the same community or even country. Lots of countries are building up mutual collaboration in combating cybercrime and ICT vital information exchange. It is crucial to discuss some of established cybercrime legislations from leading communities on the international level. In Europe, initiatives for private data protection were taken in 1970s\textsuperscript{19}. Data privacy laws were embraced by different countries in Europe, such as, Sweden in 1974, Republic of Germany 1978, Austria, Denmark, France and Norway in 1977. It was also formulated in other countries beyond Europe, such as the United States of America in 1974, Australia and Canada in 1984\textsuperscript{20}. Nevertheless, the concept of probation in cybercrime is relatively a new concept comparing to data protection and privacy. It is not often that we come across an article explains probation in cybercrimes and their legislation within the local and international community. As we mentioned in the first section, the conditional release based on probation or parole has restrictions vary from one crime to another and are decided by law practitioners. According to U.S. Probation & Pretrial Services - Texas Northern\textsuperscript{21}, probation practiced for cybercrime shall be including:

1- **Restricted Computer and Electronic Device Access**

Cybercriminal will be granted limited access to computer and Internet resources. The restriction shall include smartphones, tablets, and other electronic devices.

2- **Monitoring Software Installation Instructions**

This step is being conducted by following a monitored software installation through official website (www.paycomputermonitoring.com) and waiting for the approval from probation officer.

3- **Email Accessing**

All email accessing must be done via approved protocols (POP3/IMAP/SMTP) and approved email clients (i.e. Win-
\textsuperscript{21} http://www.txnp.uscourts.gov/content/cybercrime (Cybercrime; 22.11.2015)
4- Monitoring Software and Payments

All payments must reflect five-digit case number granted to probation practitioner. All online payment must be made via the PCM Store (http://www.paycomputermonitoring.com).

These steps imply that computers and cyberspace activities will be monitored and supervised accordingly. Nevertheless, it can be argued that it is extremely hard to monitor and control all activities in the cyberspace, knowing that some of cybercriminals are very skillful and have advanced level in computer and Internet realm. Meaning that, is it really enough to keep the access and use of computer and electronic devices limited to the previous steps? Most likely a total and tight control in this case is not guaranteed. On the other hand, a complete restricting the access to computers and Internet may create a series of consequences, as our era is totally dependent on the cyberspace.

In the Turkish context, probation system in Turkey was established in 15 August 2005 with Probation Service Code numbered 5402 which entered in force on 20 July 2005 and performs its duties on the grounds of the Regulation of Probation Services which is revised on 05.03.2013. According to the Turkish probation system, there are 12 types or categories of codes in probation have been implemented. These types and the number of those who are affected by them are presented in Table 2 below:

<table>
<thead>
<tr>
<th>Code Type</th>
<th>Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Judicial Control</td>
<td>325,046</td>
</tr>
<tr>
<td>Postponement of the pronouncement of the sentence/Deferral</td>
<td>61,113</td>
</tr>
<tr>
<td>Alternative Sanctions to Short-Term Imprisonment</td>
<td>60,455</td>
</tr>
<tr>
<td>Suspension of Custodial Sentence with Probation</td>
<td>12,615</td>
</tr>
<tr>
<td>Treatment and/or Probation</td>
<td>752,644</td>
</tr>
<tr>
<td>Effective Remorse</td>
<td>2,405</td>
</tr>
<tr>
<td>Prohibition of Enjoying Certain Right and Power</td>
<td>31,045</td>
</tr>
<tr>
<td>Early Release/Execution of Sentences under Probation</td>
<td>324,003</td>
</tr>
<tr>
<td>Community Service Instead of Judicial Fine</td>
<td>206,905</td>
</tr>
<tr>
<td>Conditional Release and Probation for Recidivist after Release</td>
<td>27,186</td>
</tr>
<tr>
<td>Home arrest</td>
<td>1,608</td>
</tr>
<tr>
<td>Probation Sanctions for Juvenile under Supervision</td>
<td>6,333</td>
</tr>
<tr>
<td><strong>Total between 2006-2015</strong></td>
<td><strong>1,811,358</strong></td>
</tr>
</tbody>
</table>

This statistic shows a total number of 1,811,358 individuals who have been affected by probationary terms in Turkey between 2006 and 2015. Although there are 12 categories affected by the probationary terms, yet none of those directly belongs to cybercrimes. As we mentioned above, it would be very confusing to attach a cybercrime to traditional crime, however, incorporating cybercrime to the body and the circumstances of traditional crimes could be the best option.

4. DISCUSSION AND CONCLUSION

In this paper, we have attempted to approach the issue of probation in cybercrimes and elaborated about its details on both local and international aspects. Cybercrimes are generally considered harder to be dealt with, more detailed and based on virtual world or cyberspace. In the cyberspace, the focus shall be always guided towards data other than objects. Things may get complicated if cybercriminals are an organized ICT professional group. Identities could be manipulated, altered or faked and thus tracing back evidence would be a very cumbersome job. Unlike the real world,
evidences related to cybercrimes are mainly based on digital forensics, yet they should be also linked to reality to avoid any misleading during the course of cybercrime investigation. According to our short investigation, there is a very limited research in the literature links cybercrimes to probationary legislation, which opens the door very wide for the investigation of this specific area. As for Turkish probation, the system is considered somehow recent yet those who got affected by its judicial statements are not little. Researchers should take this opportunity to investigate, propose and develop probationary system applicable to cybercrimes in Turkey. There are promising tools, applications software and technologies can be employed for such researches, especially technologies based on the smart devices.

REFERENCES


General Directorate of Prisons and Detention Houses, 2015, Probation in Turkey, Department of Probation, Ankara, p. 2.

General Directorate of Prisons and Detention Houses, 2015, Probation in Turkey, Department of Probation, Ankara, p. 6-7.


US Department of Justice, Investigative Uses of Technology: Devices, Tools, and Techniques, National Institute of Justice; available online at (https://www.ncjrs.gov/pdffiles1/nij/213030.pdf)

stitute of Justice; available online at (https://www.ncjrs.gov/pdffiles1/nij/219941.pdf)
