المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث
يوليو٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد - عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢ ٢٥٤٨١٠٥٠ + ٢٠ محمول: ٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢ ٢٧٩٤٩٢٣٠ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

Infringements of Intellectual Property Rights and Cybercrime

Amgad Gamal Mahmoud Faraht

Infringements of Intellectual Property Rights and Cybercrime

Amgad Gamal Mahmoud Faraht

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities[1].

Intellectual Property (IP) crime is committed when someone uses an intellectual property right without the authorization of its owner. An adequate and globally applicable set of laws to govern the universe that is the internet, for the moment is a pipe dream.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet.

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital

[1] - www.britannica.com/topic/cybercrime#ref235699

information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft.

Cybercrime is possible because computers and networks are not properly secured. Only by understanding how computer security works—and how it sometimes does not—can one predict where and how network attacks and intrusions will occur, track the actions of cybercriminals who break into systems, build evidence based on those break-ins, and help the victims of cybercrime protect themselves from future attacks. The first step in preventing cybercrime is to secure computer systems and networks against attacks. No system can be completely secure, but the goal of security is to present a barrier significant enough to repel most—if not all—attackers. Generally, the elements or issues that must be addressed to create a secure environment are the same for any type of system. But the specifics of how to implement a security policy and how to make individual security changes vary from one operating system to the next, and different technologies such as broadband, mainframe systems, and wireless networks present their own unique challenges. When planning security, one must take into consideration not only the method by which Internet access is brought to a system, but also the software programs used to interact with Internet-based resources. Web browsers are notoriously vulnerable to numerous attacks. However, with a bit of effort to keep the software up-to-date and configure settings for the best security, most common attacks can be avoided[1]

Counterfeiting and piracy are terms used to describe a range of illicit activities related to Intellectual Property rights (IPR)

[1] - Shinder, Michael Cross," Scene of the Cybercrime", 2nd edition) , 2008. P.58

infringement. Most counterfeit goods infringe a trademark, which means that a good is produced without the authorization of its rights holder. Piracy refers to the illegal use of literary and artistic works protected by copyrights.

Organized Crime Groups (OCGs) are increasingly involved in the violation of IPR.

Criminal activity in this area brings potential harm to the consumer health and safety. Health dangers are not only associated with counterfeit food or pharmaceutical products, but also substandard clothing, dangerous electronics or even toys. IP crime also affect the environment. Counterfeit pesticides often contain toxic substances that may contaminate soil, water and food. Last but not least, this crime affects the legitimate economies and results in reduced revenues of the affected businesses, decreased sales volume and job losses[1].

Illicit goods and services are increasingly advertised and sold online. Online marketplaces, both on the surface web and Darknet, are used by criminals to purvey a wide range of illicit commodities, such a drugs, firearms, malware, Child Sexual Exploitation Material (CSEM), counterfeit currency, and goods infringing IPR.

IPR infringing products sold on the Darknet include counterfeit and pirated goods. There is no specific category for such products on criminal markets and they are typically placed, together with genuine goods, within different sub categories, such as Accessories, Clothing, Counterfeit, Digital, Drugs, Electronics, Entertainment, Jewellery, Pharmacy, Software or Others. Categories vary from one Darkent marketplace to another, which

[1] - Europol, Intellectual Property Crime On The Darknet, 2017

makes it a challenge to measure the overall scope of the IPR infringing material on the Darknet.

Counterfeit products alone are estimated to account for between 1.5% and 2.5% of listings on Darkent markets. For instance, on AlphaBay, there were approximately 10000 listings under category Counterfeits. The most commonly listed counterfeit products on the Darkent are those which are obviously illegal-counterfeit banknotes and fake IDs[1].

The majority of counterfeit and pirated products continue to be sold on the surface web, on major, widely available and trusted platforms. The seller present them as , or mix with, genuine products, aiming to reach out to a large number of potential customers.

There is a wide ranges of products infringing IPR available on the Darknet such as clothes, electronics, pirated software, Pharmaceutical products and many others.

Darknet markets are large, diverse and increasingly easy to access and use. They allow criminals anonymity and offer possibilities for poly-criminality (trade in various types of illicit goods and services), at the same time generating substantive profits. Darknet marketplaces are also increasingly attractive to criminals involved in IP crime.

The two forms of IP most frequently involved in cyber crime are copyrighted material and trade secrets. Piracy is a term used to describe IP theft—piracy of software, piracy of music, etc. Theft of IP affects the entire economy. Billions of dollars are lost every

[1] - Europol's Internet Organized Crime Threat Assessment (IOCTA), 2017

year to IP pirates. For example, thieves sell pirated computer software for games or programs to millions of Internet users. The company that actually produced the real product loses these sales and royalties rightfully due to the original creator[1].

Historically, when there were no computers, IP crimes involved a lot of time and labor. Movie or music tapes had to be copied, physically produced, and transported for sale. An individual had to make the sale in person. To steal a trade secret, actual paper plans, files, or blueprints would have to be physically taken from a company's building and likewise sold in person.

In the twenty-first century software, music, and trade secret pirates operate through the Internet. Anything that can be digitized—reduced to a series of zeroes and ones—can be transmitted rapidly from one computer to another. There is no reduction of quality in second, third, or fourth generation copies. Pirated digital copies of copyrighted work transmitted over the Internet are known as "warez." Warez groups are responsible for illegally copying and distributing hundreds of millions of dollars of copyrighted material.

Pirated trade secrets are sold to other companies or illegal groups. Trade secrets no longer have to be physically stolen from a company. Instead, corporate plans and secrets are downloaded by pirates onto a computer disc. The stolen information can be transmitted worldwide in minutes. Trade secret pirates find pathways into a company's computer systems and download the items to be copied. Companies keep almost everything in their computer files. Pirated copies are sold over the Internet to

[1] https:// law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html

customers who provide their credit card numbers then download the copy.

Intellectual property pirates use the computer to steal vast amounts of copyrighted material and cause severe damage to the victimized companies. IP pirates never have to make sales in person or travel, their costs are minimal, and profits are huge. Internet pirates target the online shoppers who look for discounted, but legitimate, products. They do so by emails and Internet advertisements that seem to be the real thing. Not just individuals, but companies, educational institutions, and even government agencies have been tricked by IP pirates into buying stolen goods.

Cybercrime is not just about computers. It is also about people. Understanding cybercrime is the first step in combating it. Understanding the people on the scene of the cybercrime—those who commit it, those who are injured by it, and those who work to stop it—is the first step toward understanding cybercrime[1].

Cybercriminals cannot be easily understood as a group because they engage in a wide range of very different criminal activities for very different reasons. However, we can gain more understanding if we categorize them and analyze each group separately. Understanding the motives, characteristics, and typical behaviors of criminals in each group, along with analyzing the evidence in each particular case, can help us develop a criminal profile that will assist in identifying and capturing offenders.

[1] - Littlejohn Shinder, Michael Cross, op.cit. p.71

Part of the criminal profile involves studying the types of people criminals choose as victims. Victimology also serves other purposes; it allows us to predict where the cybercriminal might strike next and warn potential future victims. Victim profiles can also be used in concocting sting operations that lure the cybercriminal out of the virtual world and into the real one.

Investigators of cybercrime need all the characteristics that are required of any criminal investigator, plus a few extra ones to boot. Not only must cyberspace detectives be smart, logical, objective, patient, curious, and physically fit, but also they must have some knowledge and understanding of computers, networking, technical jargon, the hacker underground, and IT security issues. That's a tall order, and talented, skilled, well-trained cybercrime investigators are in high demand. Law enforcement agencies might have to pay premium salaries to get them—especially considering the discrepancy between compensation in the public sector and the corporate world for IT professionals. However, a professional cyber investigator can be invaluable to law enforcement agencies, which can expect to see the incidence of cybercrime continue to rise at an exponential rate for the foreseeable future.

Understanding the technology of cybercrime is easy compared with understanding the people who carry out the crimes. The human factor is often the most inexplicable component in an investigation.

Criminal vendors involved in IP crime seem to be lone offenders, trading in small amounts, and members of OCGs. They are profit-oriented, aiming to reach out to a large pool if customers and increase the sales volume. In order to do so, vendors tend to

advertise their products on different Darknet markets (often using the same name and selling the products for the same price) but also in the surface web.

It is difficult to determine the overall profits stemming from the trade in IPR infringing material, as the majority of vendors offer a wide scope of products and often on different markets.

The price for counterfeit goods is typically 1/3 lower than for the genuine products. Prices for pharmaceutical products also vary. Pirated software or e-books usually cost, depending on the vendor, about 1/6 of the price charged for the original product.Some criminal vendors on Darknet markets were reported to have sold on average between 500-1500 products since they joined top vendors reaching over 6000 sales.Payment is prevailingly done by bitcoin but other cryptocurrencies are also used[1].

The growing online trade, including IPR infringing products, is closely related o the increasing use of parcel and postal services to import and distribute such goods.

Some vendors include the source of IPR infringing material in the description of a product. For instance, China is allegedly named as a source for counterfeit clothes; India, US, UK, or Canada for counterfeit medicines. Hong Kong often appears as a place of shipment, and is followed by countries from Europe. The majority of products can be delivered worldwide, with some exceptions only available to specific countries.

[1] - Europol, op.cit

IPR infringing material will continue to be increasingly sold on both the surface web and Darknet. Vendors are profit-oriented and will look out for a large clientele online. Darknet markets are becoming more attractive for both criminal vendors and buyers. They allow for anonymity, a poly-criminal environment and high profits. For potential customers, they offer a wide range of commodities and services and are increasingly user-friendly, easier to access and browse through,

In addition, certain measures taken on the surface web against the IP crime, such as frequent monitoring of online marketplaces, may prompt criminals to move the trade into the Darkent. At the same time, the recent law enforcement operation targeting Darkent markets has also shown that those marketplaces are no longer beyond control/impunity. Future trade on the Darknet may increasingly migrate from large marketplaces into new, often smaller ones.

Illicit goods, including counterfeit goods, will be distributed via parcel and postal services; however, the concealment and shipment methods may become more sophisticated to increase anonymity and avoid detections.

Knowledge gaps regarding the Darkent trade in IPR infringing material remain. The involvement of organized crime in such trade and a potential for poly-criminality of vendors need to be further explored. Vendors are only one part of the entire supply chain. Buyers, suppliers and any other actors involved in the illicit trade also require special attention. All need to be better analysed in

order to develop a clear and complete intelligence picture of the mechanisms of Darknet trade[1].

It is very important to regularly monitor and understand emerging threats presented by Darknet, including with regard to IP crime. In addition enforcement response requires a holistic approach and strong cooperation, also with intermediaries such as payment card providers and shipping companies, awareness raising and expertise sharing among investigators responsible for all crime areas represented on the Darkent.

Dareknet markets resemble the markets available on the surface web. They are typically user-friendly, enabling vendors to use various marketing techniques to increase the profits. Products are displayed in different (sub) categories, along with additional information such as the vendor's profile, ratings, customer's feedback, number of placed orders, average volume per order and prices, often available in different currencies.

The absence of territorial limits on the Internet, along with the scope it offers for anonymity, has opened the door to infringements of intellectual property (IP) rights that are new in both nature and scale. Tangible counterfeit or pirated goods of almost every category are traded or exploited online, be it through legitimate business platforms such as online auction-houses, or through websites which trumpet their illicit character. Massive amounts of copyright-protected content in digital form, including software, music, films, electronic games and text, are also distributed online without the copyright owners' consent via dedicated websites or file-sharing networks.

[1] - Europol, op.cit.

The enforcement of IP rights with regard to such activities raises a number of legal questions. From an international perspective, the most comprehensive set of rules relating to the enforcement of IP rights is contained in the 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). While a number of standards set out by this instrument apply equally to the offline and the online dimension of IP enforcement, infringements carried out over the Internet pose some very specific obstacles to effective enforcement which are not addressed in the TRIPS Agreement or in any other global treaty[1].

Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters.

Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law.

[1] -https://www.europol.europa.eu/newsroom/news/setting-scene-for-cybercrime-trends-and-new-challenges

All countries face the same dilemma of how to fight cybercrime and how to effectively promote security to their citizens and organizations.Cybercrime, unlike traditional crime which is committed in one geographic location, is committed online and it is often not clearly linked to any geographic location. Therefore, a coordinated global response to the problem of cybercrime is required. This is largely due to the fact that there are a number of problems, which pose a hindrance to the effective reduction in cybercrime. Some of the main problems arise as a result of the shortcomings of the technology, legislation and cyber criminology[1].

Many criminological perspectives define crime on the social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition of crime has allowed for the characterization of crime, and the subsequent tailoring of crime prevention, mapping and measurement methods to the specific target audience. However, this characterization cannot be carried over to cybercrime, because the environment in which cybercrime is committed cannot be pinpointed to a geographic location, or distinctive social or cultural groups.

Several international treaties have been implemented relating to cybercrime. Overall, existing multilateral and regional legal instruments, and national laws, vary in terms of thematic content and extent of coverage of criminalization, investigative measures and powers, digital evidence, regulation and risk, and jurisdiction and international cooperation. These treaties also vary in geographic scope (i.e., regional or multilateral) and applicability.

[1] - Hamid Jahankhani, "Far, in Cyber Crime and Cyber Terrorism Investigator's Handbook", 2014. P.68

This variation creates obstacles to the effective identification, investigation and prosecution of cybercriminals and the prevention of cybercrime.

Safeguards are needed to ensure that laws that place restrictions on Internet access and content are not abused and are in accordance with the rule of law and human rights. Clarity in law is also needed to ensure that laws are not used to prohibit access to content in a manner that violates human rights law. A danger exists for "mission creep" or "function creep" (i.e., terms used to describe the expansion of law and/or other measures in areas beyond their original scope), where laws and investigatory powers introduced to target one form of cybercrime are then used to target other, less serious forms of cybercrime. What is more, challenges concerning the reach and effect of cybercrime laws arise where "Internet content that is generated and acceptable in one country is made available in a third country" where the content is considered illegal[1].

In Egypt, the Egyptian President Abdel Fattah al-Sisi has issued a new law aimed at cybercrime after its approval by parliament, making it the first legislation that regulates cyberspace which includes content posted on social media and the activities of Internet Service Providers (ISPs).The law enforces a fine on any website or social media account managers who intentionally encourage crimes.

“Anyone responsible for operating a website, private account, email or information system that encourages committing a

[1] - UNODC, 2013, p. 115

cybercrime will face at least one year of imprisonment and a fine between LE 20,000 and LE 200,000," the law reads.

As cybercrime continues to be an increasing and evolving threat, attention must turn toward long-term solutions. Simply blocking these attacks does not provide such long-term solutions, it only allows for cybercriminals to continually improve their attacks, which is relatively easy to do in the current environment. Attribution, leading to criminal justice, is one of the most promising ways to increase the risks associated with performing cybercrime, and therefore providing a way to reduce, in the long term, the prevalence of cybercrime[1].

[1] Robert Layton, " Automating Open Source Intelligence", 2016, p.25

References

1- Encyclopedia Britannica, Cybercrime, ref. 235699

2- Hamid Jankhani, " Far in Cyber Crime and Cyber terrorism Investigator's Handbook", New Delhi, 2014, p.68

3- Robert Layton, " Automating Open Source Intelligence", 2016, p. 25

4- Shinder Michael Cross, " Scene of the Cybercrime, 2nd edition, 2008, p.58

5- Europol's Internet Organized Crime Threat Assessment (IOCTA), 2017
6- Europol, Intellectual Property Crime On The Darknet, 2017
7- UNODC, 2013, p. 115
8- -https://www.europol.europa.eu/newsroom/news/setting-scene-for-cybercrime-trends-and-new-challenges