Malaysian Journal of Syariah and Law
مجلة الشريعة والقانون بماليزيا

Vol. 12, No. 2, pp. 334-349 | AUGUST 2024
DOI: https://doi.org/10.33102/mjsl.vol12no2.657

LEGAL PROTECTIONS FOR VICTIMS OF CYBER BLACKMAIL IN THE REPUBLIC OF IRAQ, THE UNITED STATES, AND MALAYSIA

[i]Nazura Abdul Manap & [i,ii,]*Omar Aljuboori

[i]Faculty of Law, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
[ii]Member of the Iraqi Bar Association, 10069 Alkarada, Baghdad, Iraq

*(Corresponding author) e-mail: omar_almulla91@yahoo.com

Article history:
Submission date: 8 Dec 2023
Received in revised form: 8 May 2024
Acceptance date: 28 May 2024
Available online: 31 August 2024

Keywords:
Cyber blackmail, Penal Code, victim, phenomenon, legal

Funding:
The research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Abdul Manap, N., & Aljuboori, O. (2024). Legal protections for victims of cyber blackmail in the Republic of Iraq, the United States, and Malaysia. *Malaysian Journal of Syariah and Law*, *12*(2), 334-349. https://doi.org/10.33102/mjsl.vol12no2.657

ABSTRACT

Cyber blackmail is a crime wherein an individual or corporation threatens to release a victim's private data on social media. As it is a type of crime that expands as technology improves, the rules governing it must be regularly updated and evaluated as and when the crime changes to prevent these rules from becoming obsolete. Multiple amendments must be made to the Republic of Iraq's legislation to enable the country to punish individuals who exploit victims of cyber blackmail. Therefore, this study examines the efficacy of cyber blackmail law by discussing the characteristics of cyber blackmail, the contemporary issues surrounding it, and the relevant national legislation and regulations governing it in Iraq, the United States (U.S.), and Malaysia. Analytical and descriptive approaches were used to define, examine, and analyse the issue from all angles. As a result, Iraqi lawmakers were observed to lack a sincere commitment to passing a potent law targeting cyber blackmail, either through revisions to the Penal Code or by endorsing the draft of the Cybercrime Bill (2011). An analysis of the offense's attributes revealed that its central feature is extortion, coupled with elements of criminal intimidation designed to instill fear in the victim, compelling them to yield to the devious perpetrator's malevolent intentions. The article concludes by offering suggestions to stakeholders on enhancing their approach to addressing this problem.

Introduction

Cyber blackmail is a form of conditional communication used to sway or coerce a targeted recipient and instill the perpetrator with a*"sense of power and control"*. The offense includes, among others, intimate partner violence (IPV), cyber dating abuse (CDA), and violence against women and girls (VAWG). As it is difficult to fully comprehend the scope of the phenomena as well as its significantly adverse effects on individuals, businesses, and society as a whole, it warrants more effective interventions (Vasiu & Vasiu, 2020).

Blackmailers exploit their victims by capitalising on their fears to ensure they comply with specific instructions. There is a complex correlation between the perceived risks and the actual harm that may be borne. For instance, threats may, potentially, psychologically harm a victim. Furthermore, even though a blackmailer may have no intention of ever executing a threat, its impact is similar to a physical attack. Although cyber blackmail and threats are by no means new, it has become increasingly difficult to determine the intentions and capabilities of perpetrators relative to their actions (Ramírez & García-Segura, 2017).

These circumstances are further exacerbated by the ease with which a perpetrator can manipulate their identity, thereby extending their reach and ability to harass more individuals, whether anonymously through the Internet, or offline. This type of offense, characterised by cybercriminals aggressively interfering with the privacy of individuals and entities, presents a societal threat.

In this type of cybercrime, a computer system might be utilised to compromise the integrity, confidentiality, or availability of computer data and methodologies. While these risks can be likened to pilfering from an old storage cabinet, the danger has significantly escalated in the era of advanced technology, where large-scale data theft or manipulation can occur with a mere mouse click. These offenses manifest in three forms: unsanctioned access, malicious software, and distributed denial of service (DoS) attacks (Waheeda, 2015).

A qualitative method was employed to investigate bibliographies and analyse datasets from a legal standpoint, as doctrinal legal research centres on cases, rules, and principles, all of which encompass significant legal information necessary for a deeper understanding of the law. Therefore, this study utilized analytical and descriptive methods to comprehensively define, examine, and assess the issue of cyber blackmail in Iraq, the U.S., and Malaysia. This approach aimed to provide a multifaceted understanding of the issue from a legal perspective, assessing both the efficacy of the law in combating cyber blackmail and its capacity to safeguard victims. This study utilises court cases to examine and analyze cyber blackmail in the Republic of Iraq. A content analysis approach was employed to address the following questions:

i. What are the characteristics of cyber blackmail?

ii. What are the legal frameworks governing the crime of cyber blackmail in Iraq, the United States (U.S.), and Malaysia?

This study is divided into two sections. The first section delves into blackmail and online threats, recognising threats as an essential characteristic of the crime of blackmail. The second section explores the legal frameworks in Iraq, the U.S., and Malaysia relevant to cyber blackmail. Additionally, this study offers suggestions on how stakeholders can more effectively address cyber blackmail.

Characteristics of Cyber Blackmail Crime

The term *"blackmail"* has multiple applications and definitions. It may include threatening to ruin an individual's reputation, disgracing them, divulging secrets that negatively affect them, or forcing them to conduct or refrain from conducting an act against their choice.

The U.S. Sentencing Guidelines (USSG) describes *"blackmail"* as the wrongful use of force, fear of physical injury, or bodily damage to obtain anything of value, such as money, property, a benefit, or sexual relations; from an individual (Vasiu & Vasiu, 2020).

Any threats made with the intention of making a victim believe that their status, wealth, social position, personal or professional security, or self-worth may be at risk is considered blackmail. However, these threats must not solely be used to deprive or evict a victim from a property but must be intended to *"obtain"* or *"acquire"* it. A critical aspect of blackmail is the acquisition of property from an individual *"with his agreement"*, via the illegal use of threats (Sulkowski, 2007).

Cyber blackmail involves the methods and tactics used by the perpetrator to exert pressure on a female victim through various means, such as extensive defamation or the release of sensitive data to the victim's family. This way, the perpetrator subjugates the victim and forces them to comply with their demands, be they sexual, material, or otherwise. The crime also uses emotional, sexual, and physical images (Alisawee, 2019). Most of the time, victims who have succumbed to these threats are likely to receive more demands from the perpetrator, which may develop into a long-term dominance-subordination relationship.

If a threat *"is to be carried out in the future"*, it still qualifies as *"blackmail"* as it is a threat to conduct an illegal act. Threats to harm the property or reputation of a victim by publishing defamatory or hurtful images and videos, as well as false accusations, are common forms of blackmail that perpetrators use. The use of the law, sexual coercion via blackmail, and reputation harm are some of the main types of blackmail (Abdulhameed, 2021).

In many cases, perpetrators have sought to acquire obscene or explicit content on their own. For instance, in *the United States v. Fontana* (2017), the defendant persuaded the victim to remove her blouse by posing as a young child on a chat service. He then secretly videotaped the act and threatened to post the video online unless she engaged in increasingly intrusive sexual acts, which he also filmed and used as extra leverage.

In the *Iraqi Court of Appeal v. Ahmed* (2021), the defendant used malware and other technology to remotely manipulate his victim's cameras, without their consent, to conceal his identity and gather pornographic images and videos. He then threatened to publish these illegally obtained images and videos on their social media accounts if they failed to send more naked images or videos (Hussein et al., 2022).

Legal Frameworks

Iraq, the U.S., and Malaysia have numerous cyber blackmail laws and legislations that protect victims from such offenses. These laws may be implemented depending on the circumstances surrounding each case, as will be discussed below.

The Republic of Iraq

The Iraqi Penal Code No. 111 (1969), does not address blackmail in any of its punitive clauses. However, the Iraqi judiciary, translators, and jurists have distinguished two components of blackmail. The first is the act of breaking in, which relates to the right to privacy (Article 452), while the second addresses engaging in an act that demands an illegal or immoral act or substance. This second element of cyber blackmail deems it a threatening crime as it is similar to the concept of blackmail (Article 431). Therefore, blackmail is the act of threatening someone with a crime that will be (1) committed against them, their money, or another individual, or (2) attributing or exposing matters or materials that are detrimental to their honour in any circumstance other than those specified.

It is difficult to apply traditional legal rules to criminal acts carried out using modern technology. The aforementioned provisions diverge from the standards required to consider an act a cyber blackmail crime, as the Iraqi Penal Code No. 111 was created in 1969, well before cyber blackmail even existed. Therefore, the Iraqi legal system must be reviewed as soon as possible to criminalise cyber blackmail and apply commensurate sanctions. Nevertheless, the present study will examine these resources to determine if they may be used as they are to punish the crime of cyber blackmail.

Articles 430, 433, 437, and 452 of the Iraqi Penal Code No. 111 (1969) have, to some extent, addressed this disparity as they describe the crime of blackmail as any act that threatens, defames, invades the privacy, divulges the secrets, insults, or curses a man, woman, or child. Similarly, sexual blackmail, financial blackmail, or retribution are all possible motives for cyber blackmail, which is also a public violation of an individual's rights and is a severe violation against families and society. Nevertheless, it

is vital to enact specific legislations that specifically address cyber blackmail without solely relying on the provisions of the Iraqi Penal Code.

Iraq has bridged this legislative gap by considering provisions in the Iraqi Penal Code No. 111 (1969) that specifically address threats as an article with which to punish cyber blackmail, as blackmail is also a type of threat that instills fear in women. For instance, Article 430 states:

> Any person who threatens another with the commission of a felony against his person or property or against the person or property of others or with the imputation to him of certain dishonorable matters or with the revelation of such matters and such threat is accompanied by a demand or charge to carry out or refrain from carrying out an act or is intended to be so accompanied is punishable by a term of imprisonment not exceeding 7 years or by detention.

Furthermore, when a threat is made with the intention of damaging a victim or another individual, be it by demanding money or a particular action, the perpetrator's threat as well as the fear that the victim feels may cause the victim to acquiesce to the perpetrator's demands. Article 431 addresses this situation by stating:

> Any person who threatens another with the commission of a felony against his person or property or against the person and property of others or with the imputation to him of certain dishonorable or disrespectful matters or with the revelation of such matters in circumstances other than those mentioned in Article 430 is punishable by detention.

While Article 432 states:

> Any person who threatens another by word or action or in a written or spoken reference or through another person or in circumstances other than those mentioned in Articles 430 and 431 is punishable by a period of detention not exceeding 1 year or by a fine not exceeding 100 dinars.

Meanwhile, the Iraqi Penal Code No. 111 (1969) addresses the intention of a perpetrator to execute a threat:

> The commission of a felony against another person or property, or the commission of a felony against the person or property of others, or the blaming of certain dishonest or disrespectful acts to him, or the revelation of such acts in the circumstances other than those described above, constitutes a felony threat.

Furthermore, according to the Iraqi Court of Cassation:

> Where the threat's objective was just intimidation without the accused intending to commit a particular crime, the act is subject to the conditions of Article 431 the Penal Code, the threat's statements must be grave enough to be enforced.

As previously mentioned, applying these standard texts to contemporary criminal activities conducted using modern technological tools presents a challenge, as the Iraqi Penal Code No. 111 was established in 1969, at a time when cyber blackmail was non-existent. Consequently, the mentioned articles do not align with the norms for cyber blackmail as they are rooted in traditional, non-cyber contexts, and the concept of blackmail lags behind other contemporary offenses. Thus, there is an immediate need to re-evaluate the legal framework to address the criminalisation of cyber blackmail and the enforcement of related penalties. This article will examine the provisions of the Iraqi Penal Code No. 111 (1969) to assess their suitability for tackling cyber blackmail in the present context.

Iraq has drafted a bill on information crimes and the channels with which to publish them. Although it was read by the Council of Ministers in 2011, it was only presented to Parliament in 2020, where it was not voted on due to criticism of exaggerated penalties, fines, and restrictions on the freedom of expression on social media. However, everyone failed to recognise that the primary purpose of this bill was to bridge a gap in cybercrimes in Iraqi legislation, particularly cyber blackmail. The provisions outlining blackmail offenses were introduced in a draft of the Cybercrime Bill (2011). Article 11 of this bill prescribes

penalties involving a maximum imprisonment term of seven years and a fine ranging from a minimum of IQD3000000 to a maximum of IQD5000000 for the following actions:

(1) Threatening another individual using computers and the information network to commit a felony against that individual, their assets, or the lives and assets of others, with the intent to intimidate or coerce them into taking or refraining from a specific action.

(2) Sending or transmitting any message, document, or news containing threatening information using computers or the information network knowingly, with the awareness that it comprises blackmail or threat aimed at intimidating another individual into performing or refraining from a particular act.

The second clause of the draft bill specifies that:

> "Anyone who threatens another with the use of computers or the information network in any circumstance other than those specified in Clause (1) of this Article shall face imprisonment and a fine of not less than 2000000 and not more than 4000000 dinars".

A collection of legal judgments on many cyber blackmail charges is available on Iraq's judiciary's website. Some of them are summarised below (Abdulhameed, 2021):

(1) The Karkh Investigation Court heard the confessions of members of a network that specialised in hacking social networking sites to take pictures, copy cyber conversations, bargain with their owners, and threaten to publish these illegally obtained materials on all platforms with the intention of defaming, threatening, and blackmailing their victims if they did not pay. The perpetrators were prosecuted and sent to the appropriate court under Article 430 of the Iraqi Penal Code No. 111 (1969).

(2) The Karkh Investigative Court heard the admissions of a perpetrator who extorted and threatened women on social media and called himself a *"cyber blackmail warrior"*. The court accepted one of the perpetrator's admissions, that he had blackmailed a minor in return for money. According to the provisions of Article 456 in the Iraqi Penal Code No. 111 (1969), the court began all legal actions against the perpetrator.

(3) The Basra Investigation Court recorded the confessions of a skilled hacker who threatened the privacy of numerous Telegram users by hacking their accounts, obtaining access to personal information, stealing photos, and then demanding sizable sums of money and credit cards. The court reported that many victims had filed several charges against the perpetrator stating the same blackmailing strategy and requesting money in the form of a card (Abdulhameed, 2021).

The penalties for threat-related crimes in the Iraqi Penal Code No. 111 (1969) also apply to those who engage in cyber blackmail. However, it is unclear whether the Iraqi Penal Code No. 111 (1969) sufficiently demonstrates and punishes cyber blackmail in its many forms. Furthermore, it is difficult to apprehend the perpetrators of cyber blackmail as most of them are highly technologically savvy. They are capable of hacking accounts using fake Facebook profiles and obtaining pictures or videos from or of their victims using these materials to blackmail them. As seen in Table 1, cyber blackmail cases in Iraq have increased significantly since 2018. It is noteworthy that Iraq currently ranks second in the Arab world for cyber blackmail and these crimes have proliferated because the current restrictions do not discourage perpetrators.

Table 1. The Number of Cyber Blackmail Cases Reported in Iraq between 2018-2023 in Relation to its Total Population and Percentage of Internet Users

Year	Total Population	Internet Users (%)	Blackmail Cases Reported
2018	40590096	33.9	800
2019	41560107	44.3	1200
2020	42561568	45.8	1800
2021	43530776	48.9	2000
2022	44504550	78.7	2100
2023	45689122	80.1	2500

At present, Iraq's existing laws fail to protect the victims of blackmail. Furthermore, cyber blackmail is only considered a threat crime under the laws of the crime of threat indicated above. This is one of the many critical weaknesses in Iraq's legislative system. Nevertheless, Iraqi politicians have stated that they are making genuine efforts to bridge this legislative gap.

Traditional laws have not kept pace with the advancement of sophisticated electronic criminal technologies. Hence, the Iraqi legislators must establish a distinct, specialised law for all forms of information-related crimes, separate from the penal code. This is in line with the approach adopted by many Arab nations that promptly recognised the gravity of these offenses and enacted specific cybercrime laws to combat and eliminate them. Iraqi lawmakers have been urged to pass such legislation to protect their society from the significant harm inflicted by this type of crime. It should be noted that a country as sizeable as Iraq is fully capable of taking this crucial step.

The United States (U.S.)

Table 2 displays the number of cyber blackmail cases reported in the U.S. between 2018-2023 in relation to its total population and percentage of Internet users.

Table 2. The Number of Cyber Blackmail Cases Reported in the U.S. between 2018-2023 in Relation to its Total Population and Percentage of Internet Users

Year	Total Population	Internet Users (%)	Cyber Blackmail Cases Reported
2018	332140007	87.9	51146
2019	334318671	87.3	43101
2020	336997624	87.3	76714
2021	338289857	90.0	39360
2022	339996563	90.0	39416
2023	341814420	91.3	40300

The similarities between the crimes of extortion and blackmail often confuse the U.S. However, although both involve threats, there are differences in the conduct prohibited for each offense. This will be explained in greater detail below.

Extortion

Extortion involves employing coercion to acquire money, property, or services from a victim. Coercion often involves threats of violence and property destruction, or misuse of governmental authority if the victim does not comply. Some criminal statutes classify threats to hold back testimony in a legal process as a kind of coercion. Most states classify extortion as either a felony or misdemeanour, depending on the value of the property or the amount of money acquired from the victim (Mintzer, 2013).

Before the establishment of criminal laws, extortion was addressed under common law as a crime primarily committed by public officials. In many cases, it revolved around public officials refusing to perform official duties unless they received payment. For instance, a building inspector who withheld approval for a new construction project without financial compensation could be charged with extortion.

Blackmail

Blackmail shares commonalities with extortion in that it typically falls under the category of theft and classifies the making of a threat as prohibited behaviour. In contrast to extortion, blackmail does not involve threats of violence towards an individual or property. Rather, blackmail occurs when a perpetrator threatens to reveal embarrassing or potentially damaging information about the victim's reputation to their family, community, social circles, or professional life unless the victim yields property, money, or services (Islam et al., 2020). It is important to note that the truthfulness or accuracy of the information the perpetrator threatens to disclose is not considered a valid defence against a blackmail charge. The vital aspect in a blackmail case is the threat to disclose the information unless the perpetrator receives something of value.

Blackmail and extortion are similar in that they are regarded as significant violations of criminal laws by judges and prosecutors. Penalties often involve probation, incarceration, fines, and restitution. Due to the severity of the crimes of extortion and blackmail, it would be wise for a defendant to seek the services of a qualified legal representative.

The U.S. viewpoint on racketeering has been the centre of much debate since its inception, as any form of blackmail and threats will result in a federal indictment. Chapter 41 of Title 18 of the United States Code (18 U.S.C.) outlines the types of activities that may lead to federal prosecution rather than state-level prosecution. There are ten distinct statutes within it, each describing a separate offense. These ten statutes define the elements that prosecutors must prove to obtain a conviction and determine the consequences for specific violations (Stern, 1971). Some of the rules are as follows:

i. Section 871 of the 18 U.S.C. prohibits threats against the President and his successors.

ii. Section 873 of the 18 U.S.C. stipulates that anyone who, through the use of fear of reporting or as compensation for not reporting any violation of U.S. law, demands or obtains money or other valuable items, may be subject to a fine under this chapter, imprisonment for up to one year, or both.

iii. Section 874 addresses kickbacks from public works personnel. It states that anyone who compels a person engaged in the prosecution, construction, completion, or overhaul of any public building, public work, or any project partially funded by U.S. loans or grants to relinquish any portion of their contractually entitled compensation, using methods such as intimidation, force, or the threat of dismissal, shall face potential fines or imprisonment for a maximum of one year.

iv. Section 875 of the 18 U.S.C. deals with interstate communications. It outlines that anyone who sends a communication in interstate or foreign commerce containing a request or solicitation for a reward or ransom in exchange for the release of a kidnapped individual may be subject to the provisions of this article or a maximum prison sentence of 20 years, or both.

v. Section 876 of the 18 U.S.C. prohibits the mailing of threatening messages. However, an individual who deposits or causes the delivery of any correspondence that contains kidnapping threats or threats to harm the addressee or any other individual, according to the provisions of this chapter or both, will not be prosecuted or imprisoned for more than 20 years.

vi. Section 877 of the 18 U.S.C., similarly, prohibits the mailing of threatening messages from a foreign country.

vii. Section 878 of the 18 U.S.C. prohibits extorting and threatening the official guests of the U.S. as well as foreign officials and individuals who are internationally protected.

viii. Section 879 of the 18 U.S.C. prohibits threats against previous presidents as well as selected other individuals.

ix. Section 880 of the 18 U.S.C. prohibits receiving the profits of an extortion.

As evident from the information above, both extortion and blackmail involve the unlawful act of seeking financial gain from an individual in return for refraining from reporting certain matters or maintaining secrecy, which could include potentially embarrassing details about that individual. Within the legal framework, Section 873 of the 18 U.S.C. addresses a particular category of this behaviour as a federal offence. For instance, this statute outlines the consequences for individuals who request or accept money or any valuable item by using threats of disclosure or as an incentive to refrain from reporting breaches of federal laws.

When an individual has been charged with blackmail or threat, the exact elements of the crime must be understood as each statute has a detailed definition of a distinct federal felony. For example, Section 873 of the 18 U.S.C. describes blackmail as demanding or obtaining money or other valuable items by threatening to release information or requesting or receiving money or other valuable items in exchange for not disclosing the said information, which is punishable by a fine and imprisonment of up to a year.

This demonstrates that the U.S. legal system is willing to penalise the act of mere request, without even resorting to threats. Iraqi legislation, however, only addresses threats in addition to the perpetrator's acts. In the act of requesting, the value of the item(s) requested does not matter. It simply specifies anything of value without mentioning specific items, which leaves no opportunity for the perpetrator to argue in court that the item(s) requested were worthless.

The federal court framework has implemented several modifications to deal with instances of racketeering offenses. For instance, in the case of *the United States v. Sunmola* (2018), the defendant and his co-conspirators created profiles on dating websites featuring images of U.S. military personnel in uniform. After earning the trust of women whom they had met on the Internet, they requested money and other items. The defendant faced various charges, including interstate blackmail under Section 875(d) of the 18 U.S.C. The defendant sexually exploited the victims by coercing them into engaging in sexually suggestive acts on a webcam. Unbeknownst to the victims, the defendant recorded these acts, uploaded the videos to YouTube, and sent the links to the victims and their relatives, accompanied by a blackmail demand, which included a disturbing warning that the victim *"would want to kill herself by the time he was done with her".*

The court employed several sentencing enhancements in this case, including four levels for leadership, two levels for representing a government agency without authorisation, four levels for causing substantial financial hardship, two sets of vulnerable victims, 16 levels for an intended loss of USD$2054972.66, and two levels for committing the offense outside the U.S. Furthermore, the judge made two upward departures due to the psychological harm inflicted on one victim and the gratuitous injury inflicted on another victim.

As per the pre-sentencing report (PSR), seven victims faced significant financial distress, and a number of them provided victim impact statements. These victims were middle-aged females, not elderly, and many had experienced abandonment, divorce, widowhood, or neglect from the men in their lives. Seeking companionship through online dating left them especially susceptible to falling into the snare of a dangerous man who preyed on vulnerable women.

This case revealed that U.S. federal laws do not allow perpetrators to escape unpunished as it covers the whole spectrum of the crime of blackmail, from threat to request. Furthermore, the perpetrator was also punished for impersonating a military officer and causing financial and psychological harm to his extortion victims.

The criteria for blackmail in U.S. federal laws are not limited to threats but also include extortion. Therefore, Iraqi legislators must act to enact a law that addresses the modern crime of blackmail. Apart from that, the Computer Fraud and Abuse Act (CFAA) of the U.S., under § 1030 in Chapter 47 of the 18 U.S.C., prohibits harmful conduct to computer systems as it is a matter of cyber security law, which protects federal computers, banking computers, and Internet-connected personal computers (PCs). Therefore, this act safeguards protected computers from infiltration, threat, damage, espionage, and corruption by preventing them from being exploited as tools with which to commit fraud. Although the

ruling is incomplete, it fills gaps in the safeguards provided by other federal criminal laws. For instance, subparagraph 7 of this law prohibits computer-based blackmail (Doyle, 2014).

Section 1030(a)(7) of the 18 U.S.C. states:

> "(a) Whoever
>
> (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any
>
> (A) threat to cause damage to a protected computer;
>
> (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
>
> (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;
>
> shall be punished as provided in subsection (c) of this section.
>
> (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section".

In 1996, Congress introduced Section 1030(a)(7)(a) due to concerns regarding the definition of *"property"* within existing statutes, such as the Hobbs Act (1951) on extortion and Section 875(d) of the 18 U.S.C. on interstate communication that threatens to harm another individual's property as these statutes do not explicitly encompass the operation of a computer, the data, or programmes stored within it, its peripheral devices, or encryption keys. Subparagraphs (b) and (c) were subsequently added to § 1030(a)(7) in 2008 on the Department of Justice's recommendation:

> …to cover a situation in which a criminal has already stolen information and threatens to disclose it unless it is repaid" and "in which other criminals first cause harm — such as gaining unauthorized access to a corporate computer and encrypting critical data — and then threaten to withhold correction unless the victim pays (Doyle, 2014).

Section 1030 (a)(7) of the 18 U.S.C. includes computer extortion crimes committed within the U.S. and crimes committed outside the U.S. unless they jeopardise the state's security. It also addresses the threat described in § 1030 (a)(7)(b) and (c), which is distinct from other threats. Subparagraph (b) does not address threats to damage a computer or its data, but threats to compromise the confidentiality of that data while subparagraph (c) does not address threats of future harm but rather the inability to meet excessive demands.

The statute also discusses criminal intent when the level of purpose required to violate Section 1030(a)(7) differs from the level needed to fall short of the fraud requirements of Section 1030. Instead of requiring that the crime be committed *"knowingly and with intent to defraud"*, Section 1030 requires that each felony be committed. Given that such crimes are incomplete until they are committed with the intention to extort, the premise of this paragraph is that the perpetrator intends for their victim to feel intimidated. This enables avoiding some ambiguities associated with threat legislation.

Malaysia

Table 3 displays the number of cyber blackmail cases reported in Malaysia between 2018-2023 in relation to its total population and percentage of Internet users. Act 574 (1936) has always been the main reference point when dealing with the crime of blackmail in Malaysia. Section 383 in Chapter 17 defines the crime of blackmail as:

> Whoever intentionally puts any person in fear of any injury to that person or to any other, and thereby dishonestly induces the person so put in fear to deliver to any person any

property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits *"extortion*.

Table 3. The Number of Cyber Blackmail Cases Reported in Malaysia between 2018-2023 in Relation to its Total Population and Percentage of Internet Users

Year	Total Population	Internet Users (%)	Cyber Blackmail Cases Reported
2018	32400000	87.4	342
2019	32808000	87.5	260
2020	33200000	87.7	596
2021	33940600	90.2	417
2022	34308525	93.3	478
2023	34671895	96.5	646

As previously mentioned, Malaysian legislation places the crime of blackmail under the term extortion. Furthermore, unlike their American counterparts, it also does not distinguish between the two terms.

The definition also does not state that the crime of extortion, which involves elements of fear and harm to a victim or another individual, must result in the delivery of specific items, such as material properties or documents. According to Section 384 of Act 574 (1936), the crime of extortion is punishable by 10 years imprisonment, a fine, and flogging, or any one of these last two penalties.

Act 574 (1936) separates the crime of extortion into several provisions (Section 385 to 389). It also distinguishes the specific crime of extortion in each article, such as coercion leading to work or death. § 385 defines extortion as placing an individual or any other individual in fear of death or great bodily harm, which is punishable by imprisonment for up to 14 years and a fine or flogging.

Meanwhile, Section 387 and 388 define extortion as any individual who causes or attempts to place another individual in fear of death or severe bodily damage, where the individual or other individual will be subject to a prison sentence of not more than 10 years prison as well as a fine or whipping and other punishment.

An individual who extorts another by creating the fear of being accused of, or attempting to commit, an offense punishable by death, imprisonment of up to 20 years, or imprisonment for a term of up to 10 years, or by attempting to induce another individual to commit such an offense will face a penalty of up to 10 years in prison and a fine of up to RM10000.00.

Section 389 prescribes that those engaging in extortion, or attempting to do so, by causing fear of being accused of committing an offense punishable by death, imprisonment up to 20 years, or imprisonment up to 10 years are subject to imprisonment for a period of up to 10 years. Additionally, they may be fined or subjected to whipping, and, upon conviction, they shall receive a sentence. Extortion occurs when an individual deliberately instills fear in another individual and then dishonestly convinces them to surrender any property or valuable security or anything signed and sealed that has the potential to be transformed into a valuable deposit to another individual.

The following are several recorded and convicted cases of extortion in the form of cyber blackmail:

i. In *Public Prosecutor (P.P) v. Muhammad Faez Aiman Toiban* (2017), the defendant was found guilty under Section 385 for sending a threatening WhatsApp message to the victim that he would disseminate her nude photos if she did not pay him RM5000.00 on 7 February 2017.

ii. In *P.P. v. Muhammad Shazarul Ikhmal Rospisham* (2016), the defendant was found guilty under Section 384 for sending 20 nude photos of his former girlfriend to her via WeChat on 10 January 2016 and threatening to post them online if she did not pay him RM200.00 for each of the photos.

iii. In *P.P. v. Muhammad Nor Aliff Basir* (2017), the defendant was found guilty under the provisions of Section 384 of Act 574 (1936) and Section 229 of Act 588 (1998)

for producing and transmitting an explicit video through WhatsApp on 6 April 2017 to the victim, a 24-year-old man that the defendant had been previously befriended on WeChat, with the intention of intimidating and demanding RM1000.00. The defendant threatened to release the explicit video featuring the victim if the victim did not comply with his demands for payment.

iv. In *P.P. v. Mohd Hidayat Abd Ghani @ Mokhtar* (2014), the defendant was found guilty under Section 384 of Act 574 (1936) and Section 229 of Act 588 (1998) for possessing a nude photo of his victim and threatening to post it online unless she gave him her gold bracelet and necklace as well as paid him RM5000.00 between August to September 2013.

It is noteworthy that it is also possible for cyber blackmail to be considered criminal intimidation. For instance, Section 503 states:

> "Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation".

Additionally, Section 507 states:

> "Whoever commits the offence of criminal intimidation by an anonymous communication, or by having taken precautions to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment for a term which may extend to two years, in addition to the punishment provided for the offence by section 506".

The application of the above provisions in acts about cyber blackmail is evidenced in the following cases:

i. In *P.P. v. Wan Azuan W Ismail* (2022), the defendant was found guilty under Section 507 for threatening, during a phone call on 25 January 2022, to distribute explicit photographs of his former girlfriend.

ii. In *P.P. v. Mohamad Fazrul Mohd Fuzi* (2021), the defendant was found guilty under Section 503 for threatening, via WhatsApp on 17 January 2021, to disseminate his former girlfriend's nude photos and videos after she ended their relationship.

iii. In *P.P. v. Teng Chee Sing* (2021), the defendant was found guilty under Section 507 for threatening, via an anonymous phone call, to burn down the house of the father of Kulai MCA Vice Chairman as the latter had been actively fighting against loan shark activities in Kulai, Johor.

iv. In *P.P. v. K. Theepan Raj* (2021), the defendant was found guilty under Section 507 for threatening, via WhatsApp, to burn down the house of a restaurant owner if the latter did not pay a protection racket of RM500.00.

v. In *P.P. v. Kuan Soon Min* (2019), the defendant was found guilty under Section 507 for threatening, via a WhatsApp audio message on 20 March 2019, to set fire to the house and shop owned by the victim's spouse.

vi. In *P.P. v. Mohd Zamri Mohd Yunus* (2019), the defendant was found guilty under Section 507 for threatening, via WhatsApp on 4 February 2019, to murder his ex-wife, Marina Ibrahim.

vii. In *P.P. v. Chang Ye Siong* (2019), the defendant was found guilty under Section 503 of Act 574 (1936) for threatening to disseminate obscene videos, that the defendant had recorded during a video call between him and the victim in September 2017, to her family members. The defendant was also convicted under Section 229 of Act 588

(1998) for possessing obscene videos on two of his mobile phones on 19 December 2018.

viii. In *P.P. v. Abdul Hafiz Rahim* (2018), the defendant was found guilty under Section 507 for threatening, via WhatsApp on 14 November 2017, to murder his employer, Fakhita Halim, and her husband, Muhamad Shafie Zulkarai.

ix. In *P.P. v. Jamilah Othman* (2014), the defendant was found guilty under Section 507 for threatening, via short message service (SMS) on 11 June 2014, her husband, Shahrir Firdaus Nor Ramlai.

x. In *P.P. v. Lum Gah Wai* (2014), the defendant was found guilty under Section 507 for threatening to electronically distribute explicit photographs of his former girlfriend, which were stored in two of his mobile phones, which he did on 23 April 2013, after she refused to assist him in repaying his debt to a loan shark.

xi. In *P.P. v. Muhamad Shukri Kassim* (2011), the defendant was found guilty under Section 503 for threatening, via Facebook message on 15 June 2011, to disseminate the nude photos that the victim had previously sent to the defendant's mobile phone.

Methods of Addressing Cyber Blackmail

This section discusses strategies with which to combat the crime of cyber blackmail. Table 4 below comprehensively categorises the diverse types of crimes as well as describes specific cases, the demands of the perpetrators, and the responses of the victims to the threats. More specifically, the most prevalent cyber blackmail offences as well as the best and most appropriate responses to these threats are explained. In all these cases, the perpetrators were apprehended, and their cases were handled by authorities that specialised in anti-blackmail legislation and measures. The cases outlined below as well as the methods that the victims used to address these threats will enable future victims to address threats of cyber blackmail confidently and without hesitation or fear.

Table 4. The Most Common Types of Cyber Blackmail, Perpetrator Demands, and the Correct Methods of Managing Cyber Blackmail

Case	Perpetrator Demands	Method of Addressing
A male perpetrator recorded all the video calls that he and the female victim engaged in via Telegram during their courtship.	The perpetrator threatened to publish the recordings on Facebook and Instagram if the victim refused to pay him every month.	The victim sought the advice of an anti-extortion officer, who encouraged her to make a police report and provide proof of the threatening conversations between the perpetrator and her as well as the recordings in question. The advice was followed, and action was taken against the perpetrator.
While looking for work, a female victim met a female perpetrator, who posed as a fashion designer living in France and was seeking a model. The female victim sent her curriculum vitae as well as pictures of her body to the female perpetrator.	Upon receiving the victim's curriculum vitae and pictures, the perpetrator sent the victim voice messages threatening to publish the pictures online.	The victim turned to her family, who was understanding. The victim's mother then made a police report and provided proof of the threatening voice messages as well as the pictures in question. Action was taken against the perpetrator and the case was resolved.

A female victim sent her mobile phone to a mobile phone shop to be repaired. However, the perpetrator illegally saved all her private photos.	A few days after sending her phone to the mobile phone shop, the perpetrator sent the victim her pictures and threatened to publish them if she did not pay a specific amount.	The victim was afraid to make a police report or to inform her husband for fear of scandal. As such, she paid the perpetrator the requested amount. However, in the end, the victim contacted a lawyer, who notified the relevant authorities.
A male victim clicked on a link on Facebook and his personal account was hacked, during which all his family pictures and private photos were taken.	The perpetrator contacted the victim and threatened to publish all his private photos.	The victim immediately filed a police report; however, it was discovered that the perpetrator was in a different country, specifically Morocco. The relevant authorities in Morocco were contacted to solve the case and prevent the perpetrator from publishing the victim's private photos.
A female victim was pressured by a perpetrator, a teacher at her university, who then went on to blackmail her.	The perpetrator demanded that the victim engage in inappropriate acts and send the pictures to him.	The victim informed her university's security and the relevant authorities, who established an investigation committee and informed the police. It was discovered that the perpetrator had blackmailed many female students at the university.

Analysis

The following recommendations were made after thoroughly analysing the most common types of cyber blackmail in society, some of which are listed in the table above, as well as the special laws in place for addressing cyber blackmail. It is hoped that the following recommendations will help victims and the relevant authorities identify new methods of combating and addressing cyber blackmail in addition to developing laws with which to combat cyber blackmail and encourage victims to report the crime.

Firstly, the social awareness of vulnerable populations, especially females, must be heightened to safeguard them from cyber blackmail. This can be accomplished by providing additional support to victims, encouraging victims to speak candidly, and encouraging open discussions within families via seminars and conferences that educate families about cyber blackmail. Families should also be cautioned to utilise social media responsibly. For instance, they should be informed not to upload and share intimate images via Facebook, Instagram, and WhatsApp among others due to the possibility of negative repercussions and security concerns. They should also be informed that they should not store bank account information, personal and/or family pictures, as well as confidential information and statements on their computers and/or mobile phones as all these devices are interconnected. As such, they pose a significant threat as they can be easily hacked by blackmailers.

Family ties should also be strengthened. The disintegration of the family unit can be prevented by continuously monitoring and engaging with their children, especially during important stages in their lives. Efforts should also be made to prevent falling behind in terms of globalisation, as it contributes to the destruction of the family unit and the loss of children, particularly girls. Furthermore, the local police must be emboldened to handle cases of cyber blackmail. State institutions, satellite channels, the Ministry of the Interior, the Ministry of Communications, and other appropriate government agencies may also work together to display toll-free numbers for victims to call.

School administrations, representatives from the Ministry of the Interior, and professionals from electronic technology and communications industries may also collaborate to conduct seminars and workshops at schools to increase social awareness of cyber blackmail. These stakeholders may also increase awareness of cyber blackmail using official satellite channels, which would help foster confidence and collaboration between citizens and the relevant authorities.

Legislation pertaining to cybercrime should be adopted and enforced scientifically and legislatively. It should also be based on the type of crime committed and its effects on the victim and their families. This may be accomplished via collaboration between the Ministries of Justice and the Interior. Apart from that, enhancing international cooperation, by signing agreements with nations that prosecute this type of crime, would create a defensive network for the state nationally and internationally.

Lastly, and most importantly, victims of cyber blackmail should notify and seek the advice and help of the relevant authorities.

Recommendations

The provisions of the laws on threats and cyber blackmail in Iraq as well as the approval of Iraq's cybercrime legislation are urgently needed as they have already been delayed for more than a year. This is because formally recognising blackmail as a crime against liberty will amalgamate all blackmail-related texts contained in the draft legislation into a single comprehensive text, regardless of the subject matter or the kind of threats. It is also necessary to develop training programmes that equip employees with the skills to combat communication and information offenses when such threats are sent through these channels.

The government should also enhance public awareness regarding the ethical and legal obligations to maintain the confidentiality of information that should not be publicly disseminated. Apart from that, it should promote awareness of the risks related to the inappropriate use of digital tools and educate individuals about encryption standards and methods. Utilising specialised personnel with expertise in cybercrime and internet matters to monitor best practices in this domain is another approach. Professional development can be attained by engaging in global conferences, seminars, and other pertinent scientific meetings to stay updated on international developments in serious cybercrimes and online extortion. Civil society organisations should also engage with the Ministry of the Interior to combat cyber blackmail by implementing large-scale campaigns that target individuals from multiple socioeconomic backgrounds and ages. Furthermore, victims should be encouraged to come forward and report cyber blackmail in total confidentiality. Overcoming the cultural stigma of shame is another crucial step.

In Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) works with social media sites, such as Facebook, Google, and Twitter, to remove information and accounts that violate community standards, terms of service, and privacy policies. Therefore, the MCMC or the police should act against individuals who disseminate obscene content under Section 233 of Act 588 (1998), which carries a maximum fine of RM50000.00, or a maximum one-year prison sentence, or both.

Although cybercrime is unlawful, recovering what has been lost, particularly data and years of collective intelligence, is often impossible once the damage has been done. In this scenario, prevention is typically preferable to treatment. In practice, several straightforward self-help methods can be applied, such as installing antivirus software or establishing a bring-your-own-device (BYOD) policy. Furthermore, different legal requirements must be adhered to, with some being strict and others serving as guidelines, such as the Personal Data Protection Act (2010). All data users must diligently comply with the Personal Data Protection Act (2010). Specific segments necessitate data users to register; failure to do so may result in a criminal penalty of up to RM500000.00 in fines, a prison term of up to three years, or both.

Conclusion

Growing dependence on computers to use the Internet has exposed several Iraqis to cyber blackmail, and it has become a widespread crime in Iraq. While lawmakers have taken some preliminary steps to deal with this issue, they are grossly inadequate for this kind of cyber extortion. Consequently, Iraqi legislators should also consider revisions instead of depending on prevailing laws and the unenforceable bill. This study demonstrates that the crime of cyber blackmail, particularly in its most extreme forms, can have extremely serious repercussions, such as keeping victims in a continual state of stress and dread, which can cause substantial psychological suffering, general trauma, derail lives, and undermine the public interest.

Cyber blackmail presents complex and multifaceted challenges in terms of criminalisation, prosecution, and sentencing. Therefore, to better address this issue, a more comprehensive understanding of the initiation and escalation of the crimes, the development of threat assessment specialists, and the strengthening of best law enforcement practice guidelines are necessary. A stronger and more comprehensive legal framework is also required, especially in Iraq, instead of relying on the traditional penal code, which does not address extortion crimes in general and only provides for the crime within threats, which are addressed in Articles 430 and 431 of the Iraqi Penal Code No. 111 (1969). In addition, a standard understanding of the legal requirements for the crime of electronic extortion is necessary. Victims' information must also be adequately protected. Public education campaigns that include pertinent topics, such as the dangers of cyber violence, data security, the preservation of digital evidence, effective defences against cyber threats, and incident reporting, can be highly effective in reducing cyber blackmail.

Although the present study solely analysed the prevailing conditions in three different countries, the resulting insights may be universally relevant. These observations can also serve as valuable resources with which to develop educational materials for law enforcement training programmes and law school clinics as well as help students learn the techniques of conducting factual analysis and providing counsel to clients.

References

Abdulhameed, R. S. (2021). Crimes of threats and cyber extortion through social media: A comparative study. *Review of International Geographical Education Online*, *11*(12), 1022-1033.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 383.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 384.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 385.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 386.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 387.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 388.

Act 574. (1936). Malaysian Legislation, Chapter XVII, Section 389.

Act 574. (1936). Malaysian Legislation, Chapter XXII, Section 503.

Act 574. (1936). Malaysian Legislation, Chapter XXII, Section 507.

Act 588. (1998). Malaysian Legislation, Part X, Chapter 1, Section 229.

Act 588. (1998). Malaysian Legislation, Part X, Chapter 2, Section 233.

Alisawee, S. (2019). *The crime of cyber extortion (A comparative study)*. [Unpublished master's thesis]. University of Al-Qadisiyah.

Cybercrime Bill 2011 (Iraq)

Doyle, C. (2014). *"Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws"*. Congressional Research Service. https://digital.library.unt.edu/ark:/67531/metadc461970/m1/1/high_res_d/97-1025_2014Oct15.pdf

Hussein, O. A., Manap, N. A., & Rahman, M. R. A. (2022). Cyber blackmail crime against women - a case study. *Journal of Positive School Psychology*, *6*(3), 6882-6893.

Iraqi Court of Appeal v Ahmed, 1588/C (2021).

Islam, M. Z., Zulhuda, S., Affandi, N. H. M. B., & Shafy, M. A. (2020). Ensuring safe cyberspace for children: An analysis of the legal implications of social media usage in Malaysia and Singapore. *International Islamic University Malaysia (IIUM) Law Journal*, *28*(1), 395-413. https://doi.org/10.31436/iiumlj.v28i(s1).591

Mintzer, R. (2013, December 18). *"Extortion vs. blackmail: What's the difference?"*. Mintzer Law. https://www.mintzerlaw.com/general-law/extortion-vs-blackmail-whats-the-difference

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 2, Section 3, Article 430.

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 2, Section 3, Article 431.

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 2, Section 3, Article 432.

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 2, Section 4, Article 433.

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 2, Section 4, Article 437.

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 3, Section 2, Article 452.

Penal Code No. 111. (1969). Iraqi Legislation, Chapter 3, Section 4, Article 456.
Public Prosecutor v Abdul Hafiz Rahim, 6 MLJU 533 (2018).
Public Prosecutor v Chang Ye Siong, 1 MJL 156 (2019).
Public Prosecutor v Jamilah Othman, 6 MJL 509 (2014).
Public Prosecutor v K. Theepan Raj, 1 MLJU 1178 (2021).
Public Prosecutor v Kuan Soon Min, 1 MLJ 1 (2019).
Public Prosecutor v Lum Gah Wai, 3 MLJ 228 (2014).
Public Prosecutor v Mohamad Fazrul Mohd Fuzi, 4 MLJ 494 (2021).
Public Prosecutor v Mohd Hidayat Abd Ghani @ Mokhtar, 11 MLJ 527 (2014).
Public Prosecutor v Mohd Zamri Mohd Yunus, MLJU 1501 (2019).
Public Prosecutor v Muhamad Shukri Kassim, 7 MLJ 845 (2011).
Public Prosecutor v Muhammad Faez Aiman Toiban, 8 MLJ 777 (2017).
Public Prosecutor v Muhammad Nor Aliff Basir, 6 MLJ 303 (2017).
Public Prosecutor v Muhammad Shazarul Ikhmal Rospisham, 4 MLJ 246 (2016).
Public Prosecutor v Teng Chee Sing, MLJU 865 (2021).
Public Prosecutor v Wan Azuan W Ismail, MLJU 2274 (2022).
Ramírez, J. M., & García-Segura, L. A. (2017). *Cyberspace: Risks and benefits for society, security and development*. Springer.
Stern, H. J. (1971). Prosecutions of local political corruption under the Hobbs Act: The unnecessary distinction between bribery and extortion. *Seton Hall Law Review*, *3*(1), 1-17.
Sulkowski, A. J. (2007). Cyber-extortion: Duties and liabilities related to the elephant in the server room. *Illinois Journal of Law, Technology & Policy*, *1*, 101-144. https://doi.org/10.2139/ssrn.955962
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 871.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 873.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 874.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 875.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 876.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 877.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 878.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 879.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 41, Section 880.
United States Code. (1948). American Legislation, Title 18, Part 1, Chapter 47, Section 1030.
United States of America v Antonio Fontana, 869 F.3d 464 (2017).
United States of America v Olayinka Ilumsa Sunmola, 887 F.3d 830 (2018).
Vasiu, I., & Vasiu, L. (2020). Cyber extortion and threats: Analysis of the United States case law. *Masaryk University Journal of Law and Technology*, *14*(1), 3-28. https://doi.org/10.5817/mujlt2020-1-1
Waheeda, F. (2015). Legislating for cybercrimes in the Maldives: Challenges and prospects. *International Islamic University Malaysia (IIUM) Law Journal*, *23*(3), 415-438. https://doi.org/10.31436/iiumlj.v23i3.183