Hindawi
Security and Communication Networks
Volume 2022, Article ID 2806605, 17 pages
https://doi.org/10.1155/2022/2806605

*Research Article*

# Ransomware: An Interdisciplinary Technical and Legal Approach

**M. Robles-Carrillo** [1] **and P. García-Teodoro** [2]

[1]*Network Engineering & Security Group, Faculty of Law, University of Granada, Granada, Spain*
[2]*Network Engineering & Security Group, School of Computer Science and Telecommunication Engineering, University of Granada, Granada, Spain*

Correspondence should be addressed to M. Robles-Carrillo; mrobles@ugr.es

Received 22 February 2022; Accepted 22 June 2022; Published 1 August 2022

Academic Editor: Helena Rifà-Pous



Ransomware constitutes a prevalent global cybersecurity threat since several years ago, but it is almost pandemic at present. To a larger extent, the growth of this criminal practice is due to its high economic efficiency and high degree of impunity. Efficiency in general is mainly a consequence of its high and sophisticated technical development more varieties, more devices to use it on and more functional complexity, while impunity is mostly the result of shortcomings and gaps in legal regulation. However, both of the aspects are closely related, as combating ransomware requires adopting and integrating technical solutions and legal sanctions with an interdisciplinary approach. Regretfully, the analyze of the ransomware's background, theoretical framework and practice shows a vast majority of technical proposals and a lack of either interdisciplinary or legal studies. The technical as well as the legal dimensions of ransomware need to be addressed to properly understand the scope and nature of the problem and its potential solutions. Following this approach, some basic guidelines about defense, mitigation and sanction methods are proposed in order to reach a feasible response to the challenge of defeating ransomware. These include the definition of ransomware as an autonomous offence. After setting out the main results of the doctrine, the conclusion section specifies the solutions drawn from such an interdisciplinary technical-legal approach.

## 1. Introduction

Ransomware is a global security issue at the moment [1]. It consists of "kidnapping" personal data and/or devices until a ransom is paid by the victims. Although paying the ransom is strongly discouraged [2], some studies reveal that around 57 per cent of victims of ransomware paid to recover their data [3], but less than 28% recovered it. Moreover, in some cases, after a ransom is paid, functionality could be restored but in an inconsistent manner [4]. According to the previous reports, around 60% of the organizations consulted were affected by this kind of extortion in the last recent years. Following Kumar et al., "*The first ransomware called AIDS Trojan or PC Cyborg, developed by biologist, Joseph L. Popp from USA in 1989.*" Now, "*cybercrime damages will cost the world annually by 6 trillion dollars in 2021* [5]."

The aim of this work is to analyze the problem of ransomware by following an interdisciplinary methodological approach taking into account both technical and legal issues. To this end, the survey of the ransomware background in Section 2 and the study of the theoretical framework and practical experience developed in Section 3 highlight two main facts: on the one hand, the majority of studies about ransomware are exclusively or mainly technical in nature; and on the other hand, the few proposals made from other areas of knowledge are not adequately addressing the technological dimension of the ransomware issue. In terms of solutions, the technical nature of ransomware is as incontestable as its illegal nature from a legal point of view. Therefore, Section 4 is dedicated to discussing the technical and legal dimensions of ransomware. On this basis, Section 5 provides some basic guidelines about defense, mitigation, prosecution, and sanction methods. Finally, Section 6 concludes with an overview of the solutions proposed by the doctrine as well as the main findings of this methodological interdisciplinary approach.

## 2. Background

Ransomware has become a common and shared concern for states, institutions, agencies, and international organizations. In October 2020, the G7 states included a Ransomware Annex to their final Statement Meeting. They recognized its particularity as a global threat and committed themselves to coordinating action to address and mitigate it (https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf). In June 2021, the G7 Leaders have identified the fight against ransomware among their priorities (https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-3.pdf). In June as well, the European Union and the United States have adopted a Joint Statement in which they stated their common concern on ransomware (https://www.consilium.europa.eu/en/press/press-releases/2021/12/17/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting-washington-d-c-16-december-2021/). In October 2021, more than thirty countries, as well as the European Union, led by the United States, adopted the Joint Statement of the Ministers and Representatives of the Counter Ransomware Initiative. According to it, "*ransomware is an escalating global security threat with serious economic and security consequences*" (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/). In the Carbis Bay Summit Communiqué, the G7 leaders have committed themselves "*to work together to urgently address the escalating shared threat from criminal ransomware networks. We call on all states to urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions*" (https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-3.pdf/). There are also important international bilateral initiatives such as the commitment between the United States and Israel concerning the creation of a U.S.-Israeli Task Force to combat ransomware (https://home.treasury.gov/news/press-releases/jy0479). As an example of public-private cooperation, "No More Ransom" (NMR) is a project launched in 2016 by the Dutch National Police, Europol, Intel Security, and Kaspersky Lab that introduces a different level of cooperation between law enforcement and the private sector to fight ransomware (https://www.eulisa.europa.eu/Newsroom/PressRelease/Documents/PR-NMR.pdf). Although important, many of these initiatives do not have adequate legal support, appear scattered and lack coordination to address a threat that targets an ever growing number of individuals, companies and institutions.

The great spread of ransomware affects not only final users but also enterprises and organizations. In particular, a number of infections in hospitals (e.g., Hollywood Presbyterian Medical Centre in the USA, and Ottawa and Kentucky Methodist Hospitals) and local authorities and facilities (e.g., San Francisco Municipal Transportation Agency and Colorado Department of Transportation at the City of Atlanta, as well as daily US newspapers and a North Carolina water utility) have been reported recent last years [6, 7]. In May 2021, the Irish Government published a statement reporting that there had been a significant ransomware attack on the HSE IT systems (https://www.gov.ie/en/press-release/ab2a6-briefing-on-the-governments-response-to-covid-19-friday-14-may-2021/). Although they emphasised that COVID-19 vaccinations have not been affected, probably the intention of the perpetrators of the attack was probably to take advantage of the health crisis situation to commit the crime with the greatest profitability. Colonial Pipeline paid close to 5 million dollars in ransomware blackmail. According to the reports, although the payment was reportedly made soon after the attack began, it was not enough to stop the disruption (https://www.eff.org/deeplinks/2021/05/faq-darkside-ransomware-group-and-colonial-pipeline).

The FBI estimates that ransomware caused enterprises more than $144 million payments between 2013 and 2019 [8]. In the statement published on 4 June 2021, the FBI considers it a top priority requiring exceptional measures (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware). In February 2022, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, the National Security Agency (NSA), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) have published a joint Cybersecurity Advisory: *2021 Trends Show Increased Globalized Threat of Ransomware* (https://www.cisa.gov/uscert/ncas/alerts/aa22-040). According to it, 14 of the 16 critical infrastructure sectors have experienced ransomware incidents. In addition, it recognized an increased professionalization of ransomware actors. The Federal Trade Commission qualifies ransomware as one of the most serious online threats facing people and businesses [4]. EUROPOL reports that "*the clear majority of law enforcement respondents once again named ransomware as a top priority threat . . . ransomware remains one of the, if not the, most dominant threats* [9]." Following the Joint Statement of the ministers and representatives from the Counter Ransomware Initiative, "*ransomware poses a significant risk to critical infrastructure, essential services, public safety, consumer protection and privacy, and economic prosperity*" (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021).

Actually, ransomware has become an even more lucrative business through so-called *ransomware-as-a-service* (RaaS) [10]. This implies that cybercriminals can acquire their own ransomware, including those with relatively low levels of expertise [11]. For that, well-known exploit kits (EKs) like Rig, Neutrino, and Magnitude are available. As a consequence of the above, ransomware has become one of the main reasons for the increased interest in cyber

insurance policies against attacks on the Internet [12]. Meanwhile, some insurance companies have decided to stop covering ransom payments (https://www.euronews.com/2021/05/07/cybercrime-insurance-giant-axa-to-stop-covering-ransomware-payments-in-france).

In addition to the direct economic negative effects, ransomware usually involves a data breach [13]. Confidentiality, integrity, and availability of data are increasingly at stake as a consequence of this kind of cyberattack [14]. It is not only an issue of human rights or legal concerns. Data are at the core of the digital economy, digital society, and digital government. Although attacks were mainly targeted for some time at individuals or private persons, *Wannacry* marked a turning point in this regard. For some time now, governments, financial or economic entities, and public, educational, or health institutions have become the most common and recurrent targets of ransomware attacks [12, 15–17]. As EUROPOL explains, "The shift in ransomware targeting individual PCs to more high-value targets such as businesses and public sector organizations introduces unique challenges to law enforcement investigations" [9].

There is, indeed, a paradigm change that alerts us about the scope and dangerousness of this type of attack. The RTF (Ransomware Task Force) considers it an "urgent national security risk around the world" [18]. Following media reports, the FBI has even equated this attack with terrorism. Although it has only considered setting up a coordination operation to combat ransomware, the threat has clearly reached proportions that go beyond a purely technical issue. According to Diesch et al., while in the past information security was purely a technical concern, this perspective "fails when it comes to a comprehensive and holistic view and the overall security strategy" [19]. The need for developing a holistic framework for information security governance is thoroughly examined by AlGhamdi et al., including addressing "each aspect of strategy, control, and regulation (. . .) and ensuring continuous evaluation and compliance [20]." As a security issue, a legal response is particularly needed.

However, neither a technical analysis of ransomware nor a strictly legal one is good enough to achieve a holistic understanding of this phenomenon and to design an effective response to it. The analysis must be interdisciplinary, i.e. capable of integrating the technical solution and the legal sanction. Nevertheless, such a response is not so simple.

Generally, technical responses to ransomware may vary depending on the type or scope of the attack. Legal responses might differ according to a variety of criteria, including suspected or alleged perpetrators, intent, target, effects, damage, and victims. This way, an attack that only compromises access is not the same than an attack that affects data. Similarly, an attack that jeopardises network security is not the same as an attack that affects a critical infrastructure. One more, an attack that only causes economic damage is not the same than an attack that might cause damage or loss of lives [18]. Even being technically similar, an attack is more serious and deserves a higher legal sanction than another one if it harms a greater number of legal assets or damages specially protected juridical values.

Moreover, the same or similar modus operandi in the technical response to a ransomware attack does not mean identity or similarity in the legal solution or sanction. The reason is that the legal response depends on different factors and criteria. All of these factors–perpetrators, victims, intention, damage, or, in general, the whole set of rules and rights violated by the attack make it possible to evaluate and legally sanction the attack beyond the strictly technical assessment. When an attack is made on critical infrastructure, for instance, the level of threat and potential risks increase considerably, and so should the safeguards and penalties.

At the end, the problem is that the technical response resolves the incident, but frequently with no consequences for the perpetrator. If there is no legal response, if there is no sanction for the crime, the resulting impunity becomes the main incentive for this offence.

For all the above, it is necessary to address the technical as well as the legal issues. In order to legally assess a given attack, its technical content must be known, and in order to offer a sanction appropriate to the seriousness of the attack, all the rules and rights affected by it must be considered in this context. In addition, the ultimate guarantee for the enforcement of technical measures to prevent and combat ransomware are legal obligations and sanctions. For instance, technical preventive measures are indispensable, but if there is no legal obligation to implement them, there is no effective guarantee of their compliance and no sanction in case of nonapplication. As the RTF points out, "*the international community needs a comprehensive approach that influences the behavior of actors on all sides of the ecosystem* [18]." In the Joint EU-US statement adopted following the EU-US Justice and Home Affairs Ministerial Meeting, on 22 June 2021, both parties agreed on "*the importance of together combating ransomware including through law enforcement action, raising public awareness on how to protect networks as well as the risk of paying the criminals responsible, and to encourage those states that turn a blind eye to this crime to arrest and extradite or effectively prosecute criminals on their territory*" (https://www.consilium.europa.eu/en/press/press-releases/2021/12/17/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting-washington-d-c-16-december-2021/). In addition to technical measures, the legal response is critical. The analysis of the theoretical framework and practice reveals that this is not the normal practice.

## 3. Analysis of the Theoretical Framework and Practice

Ransomware is continuously growing and evolving [21], with new variants appearing and the associated techniques constantly improving [22, 23]. Ransomware is therefore more and more dangerous. For instance, according to Connelly et al., "*Generation III is substantially more of a menace than Generation II because of its greater degree of contagiousness and ability to self-propagate across infected networks* [24]." In addition, as Bander et al. point out,

"*unlike traditional malware, even after removal, ransomware's effect is irreversible and difficult to mitigate without the help of its creator* [21]." If the author of the attack is technically a key factor in returning to the *status quo* prior to the cyberattack, insofar as he/she enables the recovery of files and/or devices, from a legal point of view, he/she might be responsible for both the attack and the failure to assist in resolving it. In any case, the question of attribution of authorship is a paradigmatic example of the need for an interdisciplinary analysis. The perpetrator must be identified and legally sanctioned. The legal sanction ensures compliance with the rules and penalises noncompliance. Law also has an important dissuasive function. Law, however, is missing from most of the studies and proposed solutions to this problem.

*3.1. Ransomware Research.* Technical studies on ransomware are numerous and exhaustive. Many of them deal with the concepts of evolution, families [25, 26], anatomy [5], and characteristics of ransomware behavior [27]. Zimba and Chishimba also explain its evolution, but with the specific aim of making a categorization framework based on the virulence of a given attack [28]. The taxonomy of ransomware, mitigation techniques, and ransom payment guidelines are also analyzed [29], as well as prevention, monitoring, and damage control [30, 31]. Some authors consider a specific typology, such as crypto-ransomware [32], or focus on specific devices or operating systems [33]. By contrast, some of the authors are mainly concerned with the role, position, and reactions of victims [16, 26, 34]. Ali et al. have offered an analysis based on their personal experience as victims of ransomware attacks [35]. Connolly et al. also carried out an empirical study of the experiences of organizations that have fallen victim of this kind of cyberattack [24]. Kurpjuhn addresses how companies should manage this attack [36]. In this regard, Rehman et al. plead for the need of a better technological vision and stronger defenses [13]. Trautman and Ormerod have arrived at the same conclusion after developing a study about *Wannacry* as well as related ransomware cases considered an emerging threat to corporations [15]. With a different approach, Bander et al. have prepared a survey of the existing research into ransomware as a novel ransomware taxonomy [21].

However, as Diesch et al. point out, "*in the past years, there was a shift from the executive technology expert to a management responsibility and a more business-focused view protecting information*." Because of this shift, "*the research focus also changed from studies in a technical context to exploring the management role*" [19]. Shahim develops a similar approach on digital transformation [37]. Cascavilla et al. propose a systematic study based on the intelligence cycle [38]. Also beyond the strictly technical framework, Connelly and Wall have defended that the responses to ransomware are made more complex "*by the nuanced relationship between the technical (malware which encrypts) and the human (social engineering which still instigates most infections) aspects of an attack* [39]." Sherer et al. have provided an overview of the ransomware's development and the general legal landscape [4].

Despite this variety of studies and the interesting proposals put forward in them, the development of independent technical, business or legal responses have evidenced to be not enough to effectively combat ransomware. Both a really interdisciplinary approach and the guarantee of a legal sanction are necessary. Since it is a criminal offence [18], legal action is particularly needed. If legal responses are ignored, do not exist or are insufficient, impunity becomes a major incentive for crime. According to the RTF, "*the majority of ransomware criminals operate with near-impunity*" [18]. For EUROPOL, it is a situation in which "*they can almost act with impunity* [9]." The Commission Ad Hoc maintains that ransomware constitutes "*probablement l'activité criminelle la plus rémunéra-trice et la moins risquée de l'histoire*" [40]. There are several reasons for surrendering to extortion. In some cases, "*ransomware's effects are not just monetary, as the loss of the files themselves (or the cost of ransom) may be eclipsed by the loss of client trust, relationships, and reputation* [4]." Institutions, companies, and professionals are increasingly being targeted by attacks which expose not only their files and data but also those of their clients. As the authors argue, "*the legal implications of Ransomware attacks are still up for debate, and there is no simple answer to the question of how ransomware victims can, or should, deal with an attack* [4]."

Actually, compliance by paying ransoms "*encourages the hacker community and ensures neither the victim's recovery nor their reputation*" [12]. Paying the ransom really means financing an illegal activity. The debate about the legal consequences of paying the ransom is still open. However, depending on the particular legislation, it could be considered collaboration with a criminal organization. As Scherer states, "*an understanding of the relevant legal issues is crucial for practitioners who will encounter ransomware and its effects* [4]."

In fact, it is also crucial to treat the cause of the problem and not just the symptoms [41]. Paying the ransom is not the only problem, nor perhaps the main one. The deepest problem lies in the fact that many of the victims do not use existing legal remedies to report the attack and prosecute the offence. In addition, besides the widespread tendency to manage the problem outside the law, ransomware has even become a business for insurance companies. Contracting an insurance policy to face a possible ransomware is equivalent to providing a legal guarantee of payment for the commission of an unlawful illegal activity. It is, moreover, an additional incentive for the crime because, if the victim cannot pay, the insurance company will. This is, quite simply, the perversion of the law to turn it into a guarantee for the benefit of the criminal.

Ransomware poses a major legal challenge indeed. The main problem is not just the high degree of impunity enjoyed by the perpetrators of this type of attack, but also, and especially, the loss of confidence of the victims in both the legal order and the justice system themselves.

*3.2. A Legal Challenge.* As stated, ransomware is nothing new, but a real explosion has really suffered in the last three years [4, 26, 42]. In 2020, attacks have increased by 148 per

cent worldwide, with an attack happening every 14 seconds [40]. Recent studies show a high rise in ransomware affecting globally, with more impact on advanced countries [29]. Moreover, ransomware has the power to shake not only organizations or individuals but also technological growth. Economic and financial concerns were and still are the primary motive for the majority of attacks [43]. But, as Marinos and Barros note, "*multiple motivations can be identified within a single attack. For example, espionage, political, financial and disruption are often combined motives* [17]." As a result, there is nearly a ransomware's epidemic [44]. Following the RTF, it is a global challenge that "*demands an "all hands on deck" approach, with support from the highest levels of government* [18]."

Additionally, the health crisis caused by COVID-19 has extraordinarily increased this problem (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic//-_Toc37776295) [9, 17]. Two main reasons can explain that: on the one hand, the greater reliance on telematics means due to the widespread situation of quarantine, which has increased dependence on technological devices in all areas of economic and social action; and on the other hand, the growth of threats, risks, and vulnerabilities. This creepy situation is also the consequence of the lack of effective technical and legal measures to respond to the risks arising from massive technological dependence.

Anyway, the exponential growth of ransomware is explained by its economic profitability [45] and the high degree of impunity that characterizes this criminal practice [9, 18]. As Connolly et al. explain, "*since the arrival of ransomware, the volume of academic literature produced on this topic has mushroomed* [24]." Despite that, neither the development of accurate technical remedies nor the implementation of social or business practices have proven to be enough to neutralise or reduce the cases. According to the authors, this kind of effort is of tremendous importance, but there is not sufficient. In their opinion, this is because most of the research on ransomware to date has focused primarily on its technical aspects, with comparatively little attention being given to understanding other aspects such as, in this case, the sociotechnical side. Even "*a more comprehensive, evidence-based picture on the global direct financial impact of ransomware attacks is still missing* [46]." Legally, ransomware involves a variety of complex criminal actions including the hijacking of data and/or devices, the alteration and/or destruction of data and/or devices, extortion, the illegal demand for the payment of a ransom, the laundering of the proceeds of crime, and the possible use of ransom to commit other illegal activities. Ransomware is not only a crime in itself but also a channel for the commission of further crimes.

In this situation, while there is a lack of comprehensive or interdisciplinary studies on ransomware, two general and constant patterns of behavior are confirmed: an almost exclusive reliance on technical measures and a worrying lack of confidence in the legal system as a solution or response to this crime. However, the law is a basic instrument for organizing society by means of principles, norms, and rules whose compliance is obligatory and whose noncompliance can be sanctioned. Not using the legal system to denounce, prosecute, and punish crimes because it seems preferable to accept extortion or because there seems to be no other option, means renouncing justice and encouraging the impunity of the offender. It also implies questioning the efficacy of the law as an instrument for the organization of social coexistence.

Ransomware is possibly, at this time, the greatest exponent, in practical terms, of the loss of trust in law and justice. For whatever reasons, whether it is the fear of losing control over data or of the cyberattack itself or the loss of prestige, the acceptance of or acquiescence to extortion raises not only a technical and/or criminal issue.

It is also a social, political, and legal problem. As a matter of fact, there are two perspectives on this issue: how law may combat ransomware and how ransomware may erode trust in law. Technological advances cannot be used to break the law. Technical solutions to problems are necessary but cannot replace or displace the law because technology and the law have different functions and they must complement each other in order to be effective. In any case, law needs to be necessarily adapted to the technological changes.

Nevertheless, the relationship between technology and law is more complicated than that existing between social, economic, or business aspects. Tatar et al. argue that "*Inconsistency between the way in which the law is structured, and the way in which technologies actually operate is always an interesting and useful topic to explore. When a law conflicts with a business model, the solution will often be changing the business model. However, when the law comes into conflict with the architecture of hardware and software, it is less clear how the problem will be managed* [47]." But the problem arises in both directions. If the regulation is in conflict with the technical component, there is a problem. Likewise, if the technical component conflicts with the norm, there is also a problem. In the latter case, the technical component is illegal. In the first case, the law is ineffective. Whatever the case, there exists a problem. Any solution, in order to be both legal and effective, necessarily involves a careful simultaneous understanding of technical and legal aspects.

Regulatory change is slower than technological change. They can also be more complex. Norms are the result of legally pre-established procedures involving institutions with the necessary power and legitimacy to create, modify, and implement norms. After their adoption, norms become binding. Actions and behaviors are to be adapted to the norm and not the reverse. However, for rules to be effective, they must provide the right response to needs and problems. To do this, the reality to be regulated must be properly understood, even if it is technically complex. As the Commission Ad Hoc notes, "*Le traitement de la cybercriminalité nécessite de connaître les modes opératoires évolutifs des cybercriminels, ce qui suppose de nouer des partenariats solides avec les acteurs essentiels* [40]." In technical and operational terms, ransomware is not the same as other types of malware, nor is it similar to other forms of illicit cyber activity. Despite that, it has not been the subject

of sufficient legal studies nor of the necessary interdisciplinary studies that could explain the technical reality and legal complexity of ransomware and offer a solution to this problem. For this reason, the aim of this work is to analyse ransomware following a holistic approach that includes technical and legal issues.

## 4. Technical and Legal Dimensions of Ransomware

In order to better understand the basics and scope of ransomware and, then, to provide a valid and effective technical and legal solution to this problem, it is necessary to know its objectives, families, variants, and operation.

*4.1. General Approach.* There exist two main types of ransomware [5, 26, 29, 48]:

(i) *Device Lockers.* This type of malware is aimed at locking the device screen and displaying a full-screen image that: (a) blocks access to the device, and (b) demands payment.

(ii) *Crypto-Ransomware.* In this case, user's personal files and documents are ciphered. Again, a ransom is required to the user [27].

Figure 1 shows typical screens for locker- and crypto-ransomware. Both types of ransomware deny access to computer resources until the ransom is paid. However, while locker-typed files can be dismantled through various system restore techniques and tools, encryption-typed files are more destructive in general, as encrypted files cannot be easily deciphered.

This typology of ransomware has been reproduced in legal terms, recognizing two kinds of offences. However, as it will be discussed below, the requirements demanded to prove the existence of the crime in each case do not sufficiently reflect the scope of their differences and, above all, of the possible responses and solutions from a technical point of view. The destructive effect and the reduced chances of recovery in the case of crypto-ransomware have not been sufficiently appreciated.

To begin with, the global and transnational scope of this phenomenon would require a global, international response to this overall challenge. The RTF recommends international cooperation on legal measures as a priority action against ransomware [18]. In October 2021, the adoption of the Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative implies a common understanding on the need for international cooperation. According to it, "*Noting that law enforcement and cybersecurity capacity can be significant limiting factors in a state's ability to address cybercrime, diplomacy in the form of coordinated capacity building has potential to serve as a force multiplier in the fight against ransomware*" (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/). The political commitment made in this joint declaration is quite an important progress, although it is not enough because it does not create obligations for its participants. To be really effective, a legal commitment through an international treaty would have been required.

Although there is no universal legal treaty against ransomware or, more generally, cybercrime, there exists an international convention signed by a majority of states that is, moreover, followed and domestically imitated by many other countries [49]. This international legal framework for the prosecution and punishment of malicious activities in cyberspace is the convention on cybercrime adopted by the Council of Europe in 2001. In this so-called Budapest Convention, Articles 2 to 6 are aimed at protecting the confidentiality, integrity, and availability of computer systems or data. The provisions specifically related to ransomware are:

(i) Article 4, concerning crypto-ransomware, includes "*the damaging, deletion, deterioration, alteration, or suppression of computer data without right*." There are two conditions to the application of this article: (1) the acts are only punishable if committed "*without right*," and (2) the offender must have acted "*intentionally*."

(ii) Article 5, relating to locker-ransomware, refers to "*the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data*." In this case, there are three requirements in order to give rise to criminal sanction: (1) the hindering must be "*serious*," (2) the action must be "*without right*," and (3) the offence must be committed "*intentionally*."

In both cases, the requirement to "intentionally" is reasonable. However, the prevision that "*the hindering must be serious*" makes an important difference between the two types of ransomware from a legal point of view. Crypto-ransomware is considered a serious attack in itself because it is not necessary to demonstrate the seriousness of the attack that is required in the case of locker-ransomware. In this last case, there may be more serious and less serious attacks, and only the former would be punished. However, this requirement about "seriousness" is a relative criterion. Moreover, the simple fact of intentionally hindering the functioning of a system and affecting data without a right or legitimate cause should be considered an unlawful act regardless of the gravity of the effects of the result. The attack may not be serious because it has been neutralised or repelled, or because some technical or nontechnical problem impeded its completion. If it is intentional and without right or cause, the conduct itself should be punishable. The result, more or less serious, should be a criterion for quantifying the penalty, higher or lower, but not a criterion for criminalising the offence.

This legal framework poses two main problems, indeed. The first one is precisely whether there can actually be ransomware attacks that are not serious or graves. Ransomware is an intrusion that would have to be prosecuted


(a) (b)

Figure 1: Example of ransomware screens/messages: (a) locker, (b) crypto-ransomware.

and sanctioned by its simple execution because by itself it affects to the integrity of the devices or data. Requiring a certain level of seriousness of attack would be equivalent to guaranteeing impunity for actions that have not satisfied that condition because of failures in their execution and not because of unwillingness to commit the criminal act. A second question is to ascertain the criteria to be followed in order to assess the seriousness of the attack. It could be qualitative, quantitative or both. The sole certainty is that it has not been determined and this fact leads to legal uncertainty and insecurity.

In any case, furthermore, the question to be asked is if it is sufficient to penalize the result or whether it would be necessary to punish the hijacking action itself regardless of the result. This is an important issue. There are cases in which ransomware is made progressively by hours or by hijacked material or is accompanied by a threat of simultaneous disclosure to pressure for prompt payment. As long as the conduct itself is not penalized and only the result matters, the norm would not perform a preventive or deterrent function and the behavior would not be punished.

The situation is different in the European Union. In similar terms to the Budapest Convention, Directive 2013/40/EU regulates "Illegal access to information systems" (Article 4), "Illegal system interference" (Article 5) and "Illegal data interference" (Article 6). However, article 8 establishes, in addition, the legal regime regarding the cases of incitement, aiding, and abetting, and attempt. According to Article 8.1, Member States "*shall ensure that the incitement, or aiding and abetting, to commit an offence referred to in Articles 3 to 7 is punishable as a criminal offence.*" Along with it, states shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence.

The criminalisation of incitement, complicity, and the attempt to commit an offence is a fundamental difference with respect to the Budapest Convention system. It is an effective approach to the punishment of this offence as well as to limit or reduce the impunity associated with ransomware. It is not only the criminal result that is criminalised, but also the conduct aimed at achieving that result, regardless of whether it is achieved or not. The fact that there are an illegal access or an illegal interference and requirement that the action is committed "intentionally" and "without right" must be sufficient to justify the punishment of such conduct even when the expected result of such an attack is not achieved.

Although in the case of the European Union the regulation seems to be more effective, there is an in-depth problem with the legal approach to ransomware in general. The legal response to ransomware is basically the same as to malware in general [50]. But ransomware differs from many other types of cybercrime on a number of levels [4]. In addition, it is an exception to the traditional data security breach concept [4, 14]. Not only is the data affected, but also privacy, which is another legitimate legal right protected by law. Actually, when the target is a critical infrastructure, the attack implies a contravention of the regulations established to protect it. Regulations on the security of networks and information systems or on the security of electronic communications are also threatened and/or violated by ransomware attacks. Ransomware is a complicated modality of extortion [40, 51]. In addition, "*one of the main reasons ransomware has become prevalent globally is that it uses the Tor system and asks victims to pay in bitcoin or other cryptocurrencies. The Tor system and cryptocurrencies make crime investigation difficult, especially when it comes to tracing the money flow* [11]."

Ransomware is more than simple illegal access to or interference with systems, communications, or data. It cannot be treated merely as such. Ransomware can be a sum of several of these different infractions, or perhaps it should be a specific type of illicit act. Criminalising ransomware as a specific type of offence could be a valid and effective option for a legal response to this particular type of cyberattack.

The uniqueness of ransomware within the overall typology of cyberattacks, due to its nature, characteristics, and performance, may justify its autonomous typification as an independent crime. However, the question arises as to whether the proposal of a single type or a specific offence is viable despite the existence of different types of ransomware and its evolution as well as its operational stages.

*4.2. Ransomware Families.* Based on trojan *Citadel* (which is based on Zeus), *Reveton* appeared in 1989. Also known as *Trojan cop*, it generates a message indicating to the user that some illegal activity has been performed (*e.g.*, pedophile) and that the device is locked until a payment is satisfied.

Since then, a variety of ransomware families, either locker-like or crypto-like are reported at present [17, 26]. In particular, Figure 2 shows newly discovered ransomware families worldwide from 2015 to 2020 [52]. In this context, some of the most relevant ones that have appeared over time are [53–55] (see Figure 3):

(i) *CryptoLocker*. This ransomware managed to infect approximately 250 thousand Windows-based computers around the world, including a police department that paid a ransom to decrypt their documents. This ransomware encrypts with RSA more than 70 types of files (pdf, txt, jpg, ...).

(ii) *CryptoWall*. Developed for Microsoft Windows systems and making use of RSA-2048, this ransomware is highly destructive. The ransom to be paid ranges from $500 to $1,000. Originally named *CryptoDefense*, it was renamed *CryptoWall* after a modification by the creators to avoid file recovery from storing ciphering keys on the target device.

(iii) *CTB-Locker*. Also known as *Citroni*, *CTB (Curve-Tor-Bitcoin)* is a ransomware that uses the TOR network to hide its activities. Different variants give users 72 to 96 hours for the payment; offer an extension of the deadline; and allow the ransom message in different languages.

(iv) *TeslaCrypt*. Initially aimed at encrypting up to 180 file extensions for 40 specific games (*e.g.*, *Call of Duty, World of Warcraft, and Minecraft*), this ransomware was shut down by developers in 2016 and released the master decryption key. After that, ESET released a public tool to decrypt affected computers at no charge (http://download.eset.com/special/ESETTeslaCryptDecryptor.exe).

(v) *MSIL/Samas*. Also known as *SamSam*, this ransomware exploits vulnerable Java-based web servers. *SamSam* is configured to encrypt hundreds of different file types. Once the encryption process is completed, the ransomware deletes itself, leaving a ransom note on the desktop. The note instructs the victim to visit a website and pay a ransom of about 1.5 Bitcoin for each infected computer.

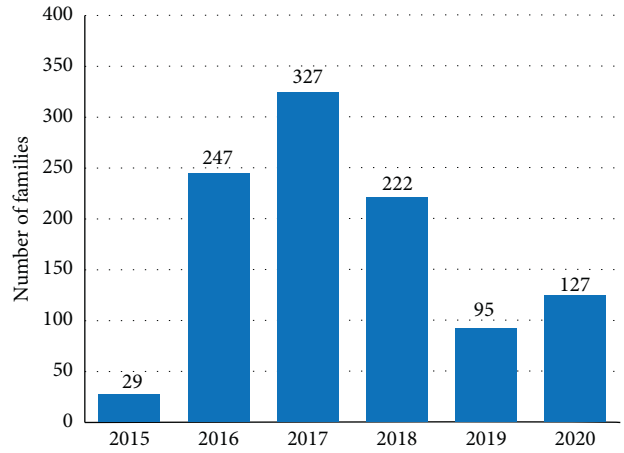


Figure 2: Ransomware families discovered from 2015 to 2020 [52].

(vi) *Locky*. One of the most prolific ransomware variants to date, *Locky* includes malicious Microsoft Office documents or compressed attachments associated with banking trojans such as *Dridex* and *Pony*.

(vii) *Crysis*. Discovered in February 2016, *Crysis* can infect Windows and Mac systems. It encrypts more than 200 file types and deletes the system's shadow/backup copies to avoid the system restoring.

(viii) *Cerber*. Similar to *Locky*, one of *Cerber*'s novel features lets the threat read the ransom note aloud to the victim, using a text-to-speech (TTS) module. In addition, *Cerber* is reportedly capable of adding the infected computer to a botnet which can be used to carry out distributed denial of service (DDoS) attacks.

(ix) *CryptXXX*. Appeared in April 2016, initial variants used weak encryption, allowing cybersecurity researchers to create a decryption tool for compromised computers. However, the attackers responded quickly and newer variants of the malware employ better encryption, making the tool ineffective.

(x) *WannaCry*. Appeared in May 2017, it became famous because of the affection of more than 200,000 computers for a number of relevant international companies. It was propagated through EternalBlue, an exploit developed for Windows systems. While Microsoft had released patches previously to close the exploit, much of *WannaCry's* spread was from organizations that had not applied these.

(xi) *Ryuk*. This variant was derived from the Hermes source code and hit in 2018 and 2019. Its victims were organizations with little tolerance for downtime, including daily US newspapers and a North Carolina water utility struggling with the aftermath of Hurricane Florence.

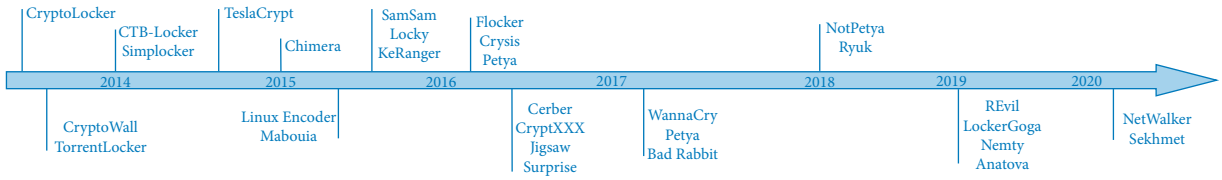


Figure 3: Timeline of some relevant ransomware families and variants.

(xii) *REvil*. Also known as *Sodinokibi*, it first emerged in April of 2019 and, like *Zeppelin*, it appeared to be the descendent of another malware family: *GandCrab*. It also had a code that prevented it from being executed in Russia and several adjacent countries, as well as Syria, indicating that its origin is in that region.

(xiii) *Nemty*. *Nemty* ransomware is one of the top ransomware attacks during 2020-2021, being active from 2019 summer until 2020 summer. It was frequently advertised in the Russian pirated forum websites and acts like a ransomware service. In fact, when a computer infected by *Nemty* paid the ransom, 30% of the payment was transferred to Nemty developers and the rest to the clients.

Ransomware affects mainly Microsoft Windows platforms at present [26]. However, specific ransomware variants also exist for other platforms like Linux, Mac OS, or Android. In the first case, we can mention Linux *Encoder*, a variant of *CBT-Locker* that appeared in late 2015. Around the same date appeared *Mabouia* and *KeRanger* for Mac OS X users. Regarding Android devices, there exist both crypto-ransomware, like *Simplocker* and *DoubleLocker*, and locker-type samples, like *Flocker*, which is capable of locking Android smart TVs.

More recently, it is worth mentioning a 118% increase in ransomware attacks for the first quarter of 2019 [56], where new ransomware families were detected, and threat actors used innovative techniques. This is the case of *LockerGoga* and *Anatova*. *LockerGoga* modifies the user accounts on the infected system by changing passwords. It also tries to log off users logged in to the system. It would then relocate itself into a temp folder and rename itself using the command line (cmd). *Anatova*'s architecture is unusual in that it is modular, which could facilitate future development of ransomware.

Finally, it is necessary to mention that ransomware attacks have doubled in number in the last period. Thus, in the last financial year, ransomware attacks have dramatically increased due to the lack of cybersecurity measures during home-office working that the COVID-19 pandemic has brought along. Furthermore, many ransomware families have improved their skills in stealing sensitive data from various sectors such as banking, financial services, governmental services, insurance, and manufacturing sectors. In this context, we can mention *NetWalker* ransomware, also known as *Mailto*, one of the most destructive malicious software in the ransomware attacks 2020-2021 list. *NetWalker* uses the network of the victim to encrypt all Windows devices by following two different ways to attack: (a) coronavirus phishing mails and (b) executable files that spread through networks. The appearance of the *Sekhmet* ransomware in June 2020 is also noticeable. It encrypts the files and asks for money to decrypt them. Infected files' extensions are randomly changed such as ".HrUSsw, .WNgh, .NdWfEr." After the attack, every single file is left with a ransom note, as "RECOVER-FILES.txt." To encrypt the files, Sekhmet uses a combination of RSA-2048 ve ChaCha encryption algorithms. To decrypt, you need a decryption key. However, this key is kept on a server that belongs to the cybercriminals. In the note within RECOVER-FILES.txt, it is said that the victim's company network has been attacked; sensitive data has been stolen and encrypted. Cybercriminals demand victims contact them within 3 days, otherwise data will be published online.

In addition to the previous families and variants, ransomware is continuously growing, which new techniques and more targets. For example, in addition to encrypting files, *Chimera* threatens to post the victims' files, including personal pictures and videos, on the Internet. Likewise, *Jigsaw* threatens to delete a number of files for every hour the ransom is not paid, while *Surprise* increases the ransom every time the user fails to meet a deadline. A more complex situation is that of *Popcorn Time*, where, with an interface similar to Netflix, the ransomware sample is installed through a movie via BitTorrent. The key point in this case is that, instead of a direct payment to recover the data/device, the user is demanded to infect and force the payment of third parties. Although this ransomware was cancelled in 2014, the project was afterwards forked in other directions. From a legal point of view, this so-called "nasty way" is approaching an illicit association for the commission of a crime or an organized crime if the conditions laid down in that provision are fulfilled. In the Ransomware Annex to their final Statement Meeting, G7 countries warn that "*Ransomware attackers are criminals, many of whom are involved in transnational organized crime groups, and a received ransom payment constitutes criminal proceeds. Those criminals that have employed the use of malware may also be linked to states seeking to evade sanctions. Ransomware proceeds could also be used to finance terrorism once they have been converted into anonymously-held funds by a victim payment into an unidentified virtual asset wallet*" (https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf). According to the United Nations Convention against Transnational Organized Crime, "*Organized criminal group shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences*

*established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*." So, ransomware is also expanding as a form of organized crime.

All these different variants of ransomware paint a considerably more troublesome picture than that of its origins. The analysis provides some conclusions. First, ransomware is a complex attack both from a technical and juridical point of view. Although it constitutes access or unlawful interference, it is technically and legally a more complicated attack that generally damages a larger number of legal assets and rights. Second, while technical responses are being adapted to respond to new variants of attack, there have not been any real changes in the current regulations in spite of the fact that they have proven not to be effective in deterring or punishing this illegal conduct. Third, while statistics on cases, victims, ransoms, and payments are increasing, there are no sufficiently indicative and reliable, comprehensive, or aggregated statistics on reported, investigated, prosecuted, or sentenced ransomware cases. Finally, while ransomware practice has been marginalising the recourse to law and justice, the law has been unable to adapt itself to face the challenges posed by technological progress as well as, particularly, the danger of ransomware.

The analysis of ransomware families indicates that, based on their nature, characteristics, and operation, there are three options for legal response: (1) maintaining the status quo; (2) treating ransomware as a joint or concurrent crime in which several offences can be aggregated by identifying and including, in each case, those that apply; (3) defining ransomware as a specific and autonomous crime. Considering the limited effectiveness demonstrated so far, the first option is becoming increasingly unsustainable. The second one is more complex in technical-legal terms, has less deterrent force, and offers less legal certainty, but it is an immediate or short-term solution. The third is a more dissuasive solution, technically less complicated to implement than the second one, and is justified by the scale and severity of the ransomware problem. The existence of this offence as such would in itself have a dissuasive capacity that is lacking in the current offences that are used to criminalise this type of attack. As seen in the study of the different families, all the forms of ransomware have a common illegal core that allows for autonomous typification. This common core can also be seen through its operation stages.

*4.3. Operation Stages.* Aimed at fighting properly against ransomware, some studies exist where specific samples are collected and analyzed in order to characterize them and extract and learn common behaviors [57, 58]. First of all, it is important to note that ransomware usually goes through several common stages:

(1) Infection/propagation. As any other types of malware, usual infection vectors include spam emails, SMSs, malicious webs (drive-by-download), and the use of infected devices [48]. In this first spreading stage, exploitation of system vulnerabilities is also a principal infection vector. This is the case of vulnerabilities CVE-2016-1001 (for Adobe Flash Player) and CVE-2018-8174 (for Windows), which are recurrently used in EK tools like Neutrino or Rig [43].

(2) Privilege escalation and permission gain. Once the malware is downloaded onto the device, special privileges may be required to access some functionality (*e.g.*, PIN modification to lock screen). This is the case of the tool *Mimikatz*, which is used to steal user credentials from the compromised device.

(3) Ransomware execution. As explained, ransomware is intended to kidnap the user's device, either by ciphering the information or by locking the access. In the first case, some of the most common types of personal files affected are database-related files, web pages, and data and photos. In the case of locker-ransomware, access to system files can be performed to unlock the device (*e.g.*, by changing the entry PIN). Other options go through locking the desktop or disabling some keyboard keys.

Additionally, ransomware can move laterally to discover additional endpoints: personal contacts, GPS location or access keys. The purpose is to provide the attacker with the information in order to blackmail the user, gain access to her/his bank accounts, and so on.

(4) Ransom message. Once the malicious action is carried out, all current families display threatening messages (maybe by e-mail) to monetary extort the user. Otherwise, she/he is advised to lose the data or access to the device.

(5) External communications. As other typology of malware (e.g., botnets), it is usual the communication of the infected device with an external server. The reason for that can be varied: extraction of personal information (leakage), exchange of commands (command and control, or C&C), malware update, etc. In the case of ransomware, such communications can also provide the encryption keys to cipher the user's information.

At this point, it is important to note that all these steps and activities would give way to specific observations able to be used to detect and thus fight against ransomware from a technical perspective.

In short, both the common core identified in the analysis of the different families and that found in the common stages technically justify the legal definition of ransomware as an autonomous offence.

## 5. Guidelines on Defense, Mitigation, and Sanction Methods

According to the Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative, the fight against ransomware "*will include improving network resilience to prevent incidents when possible and respond effectively when incidents do occur; addressing the abuse of*

*financial mechanisms to launder ransom payments or conduct other activities that make ransomware profitable; and disrupting the ransomware ecosystem via law enforcement collaboration to investigate and prosecute ransomware actors, addressing safe havens for ransomware criminals, and continued diplomatic engagement*" (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/).

The RTF proposes a comprehensive general framework for action against ransomware that is organized around four goals: "*deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; disrupt the ransomware business model and reduce criminal profits; help organizations prepare for ransomware attacks; and respond to ransomware attacks more effectively*" [18]. Technical and legal measures can be specified in concrete guidelines for action.

Similarly to generic malware, three are the typical technical defense lines to defeat ransomware: *prevention*, aimed at trying to avoid its occurrence; *detection*, to be aware as soon as possible of its potential appearance; and *recovery*, to mitigate its effects in case of operation and thus to increase the resilience of the target system (Figure 4). A key point regarding this is the need of the existence of a specialized department in the organization in charge of the cybersecurity, the so-called *Security Operations Centre* (SOC). Along with the technical defense lines, nontechnical measures are needed to prevent, deter, investigate, prosecute, and sanction the perpetrators of this cyberattack.

*5.1. Preventing Ransomware.* It is evident that the first defense line must necessarily be that of prevention [5]. Prevention requires the use of technical measures as well as social, educational, and legal instruments and policies. Awareness, education, and training in cybersecurity are essential. Regulation for the prevention, prosecution, and punishment of ransomware is also fundamental, both to fulfil a deterrent function and to avoid the impunity that encourages the commission of these crimes.

The best way to avoid a given pernicious threat is to put into action some mechanisms aimed at preventing the occurrence of the threat. For that, best practices are recommended to minimize risks, which are as follows (Table 1):

(i) Definition and implementation of security policies, which will allow to know in depth the specific context.

(ii) User education and training, for risk awareness and how to deal with them.

(iii) Use and control of legitimate software, thus avoiding potentially malicious applications and services.

(iv) System update and patches installation, to correct exploits and vulnerabilities.

(v) Access control mechanisms, to control the users and the environment.


Figure 4: Security defense lines.

(vi) Users' privilege management, to avoid inadequate permissions and harmful activities.

(vii) Control of service deployment and configuration, including network services to reduce risks.

(viii) Strengthen basic Internet services like e-mail and browser security by installing antispam tools and restricting navigation to malicious sites.

(ix) Periodic data backups, for potential recovery purposes.

(x) Restrictions regarding removable devices such as USBs and DVDs, to avoid infections.

It is important to remark that the previous practices must be necessarily monitored and revised, if necessary, in a dynamic way over time.

From a juridical point of view, at this point, the main challenge is to provide a clear and comprehensive regulation that includes both the prosecution of these crimes and the obligation to establish and regularly adapt all the necessary security and protection measures to combat ransomware. Typification of ransomware as an autonomous offence would provide a clear understanding of the prohibited behavior and its legal consequences.

Moreover, the procurement of insurance policies to respond in case of attack should be prohibited. This practice has been developed faster because it is wrongly recommended as a solution for the possible victims and because it is a business for insurance companies. The insurance contracts actually have an unlawful cause and the *de facto* beneficiary of these policies is the ransomware attacker. In the latter case, it is a guarantee of the success of the attack because in any case the payment is covered by the insurance contract. It is an additional incentive for the commission of the crime. The victims, even if they do not have to pay the ransom, are already paying the insurance. In addition to having an economic cost, this can lead to a relaxation of their own security measures, which, in turn, can result in an increase in the number of attacks.

Along with that, the possibility of prohibiting and penalizing the payment of ransom is being widely debated. In this case, unlike the previous one, the issue is much more complex. On the one hand, it could be a way to combat this crime. But, on the other hand, it would mean accepting a double victimization of the victims as they are first attacked and then punished for responding to the extortion. Legal

Table 1: Defense mechanisms against ransomware.

| Prevention | Detection | Recovery |
|---|---|---|
| (i) Security policies | (i) File system activities | (i) Payment |
| (ii) Training | (ii) API calls | (ii) Cleaning/replacement |
| (iii) Legitimate software | (iii) Registry access | (iii) Backup restore |
| (iv) Updates | (iv) C&C communications | (iv) Law enforcement |
| (v) Privilege management | (v) Encryption procedures | (v) Agencies notification |
| (vi) Service deployment | | |
| (vii) Internet protection | | |
| (viii) Data backup | | |
| (ix) Removable devices | | |

arguments such as force major or state of necessity could be invoked to justify such an action.

Finally, educational and training policies are specially required to avoid the lack of knowledge of the victims, which may facilitate the commission and spread of ransomware.

*5.2. Ransomware Detection.* Despite several prevention mechanisms are adopted, infections are still possible. That is mainly due to human factors (*e.g.*, through social engineering) [4], but also because of the usual existence of vulnerabilities and misconfigurations in software and systems. As a consequence, also detection mechanisms need to be deployed around our environment, aimed at early detecting the potential operation of ransomware to thwart its effects. Actually, "*early detection is not so effective once the victim is infected* [59]."

There are different detection approaches in the literature [60]. Most current detection solutions refer to signature-based tools, like *SurtRight's HitmanPro.Kickstart* or *Avast's Ransomware Removal*. Such approaches rely on the detection of well-known activity patterns. For instance, McAfee reincludes more than 8 million ransomware signatures including *CTB-Locker*, *CryptoWall*, and their variants [61]. Instead, several other current detection solutions rely on analyzing behaviors [62].

A holistic taxonomy of countermeasures for ransomware is introduced in [39], where both technical and education-based, as well as policy and law-related issues are considered. Focusing on a technical perspective, the detection of ransomware action is usually dealt with according to some well-known methodologies [27, 60, 63]:

(i) Static, intended to detect ransomware action before malware runs. This is the case of finding common strings in programs (*e.g.*, "ransom," "bitcoin," "encrypt") or the use of function calls to encrypt files.

(ii) Dynamic, related with the execution of the malware over time. The information accessed in this case can be varied: file system access (overwriting or removing files, file extension modification), network activity (*e.g.*, DNS requests, C&C communications), system registry modification, etc.

Based on the above recurrent aspects, the authors discuss in [64] several proposals developed in the specialized literature to thwart ransomware action. Several of them rely on the use of specific API calls intended, for example, to lock resources or encrypt files. It is also usual that ransomware samples modify system registry values to specify some valuable configuration for the attacker's purposes. In other cases, the usage of system resources (disk, CPU, RAM, network connections) is monitored over time. Beyond the specific parameters considered in detection, some works are mainly focused on evaluating novel analysis methodologies, most of them concerning machine learning approaches.

Although they are numerous and worthwhile, none of the available solutions at present is effective enough against ransomware. Early detection is a main challenge. Although potentially accurate in detection, any valid solution should additionally be as quick as possible. Otherwise, the action regarding the encryption of the system can be completed and, thus, the detection itself will become useless.

In addition to these technical issues, the detection phase is particularly relevant from the juridical point of view. The applicable law and the competent jurisdiction to prosecute this crime, including the complex issue of obtaining and preserving evidence, have to be determined on the basis of the place and time of detection. As it is well known, investigation and criminal prosecution of these offences may fall under different jurisdictions or, because of the negative conflict between them, under no jurisdiction, thus amounting to absolute impunity. Activation of legal measures at the detection stage may be essential to avoid such a situation.

Two main legal issues arise here. First, by nature, ransomware is a transnational crime. Second, there are several different legislation in various countries. The place in which the intrusion is detected may be relevant for the purpose of determining the applicable law. A territorial principle is a legitimate ground for claiming competence and jurisdiction. But it may happen that the place of detection does not coincide with the location of the victims or that there are victims in different places under different jurisdictions. In addition, "*most ransomware criminals are based in nation-states that are unwilling or unable to prosecute this cybercrime*" [18].

Actually, a main challenge is to determine which law is applicable and which jurisdiction is competent in every case when the concurrence of several laws may become an obstacle to the effective implementation of any of them. There are three main rules:

(1) Principle of territoriality: the applicable law and the competent jurisdiction are determined by the location of the intrusion or the location of the target.

(2) Principle of nationality: the nationality of the victims or of the perpetrators may be the determining criterion for the establishment of the applicable law and the competent jurisdiction.

(3) Concurrence of jurisdictions: in the cases in which more than one state could have jurisdiction because of the territorial or national criteria, the affected states should consult each other in order to resolve the conflict of jurisdiction.

In the end, the best mechanisms to tackle the problem are international cooperation and mutual assistance.

Alongside legal action, the provision of effective technical measures for recovery is essential.

*5.3. Recovery from Ransomware.* The disposal of a recovery plan for business continuity is a key aspect of cybersecurity defense (as in any other ICT field). That includes the measures to solve the problem reported (the existence of ransomware in this case) and to restore the system to its previous (noninfected) status. As specified in Figure 4 before, such recovery actions will affect the prevention mechanisms adopted in order to improve overall security. Some mechanisms discussed to recover the system from a ransomware event are as follows:

(i) The first question that arises at this point is whether to pay or not the ransom to recover the data and/or device access. The answer seems to be clear [2, 8]: "*Paying the ransom does not solve the problem because there is not warranty neither to recover the data nor to suffer again the extortion to continue paying!*"

Payment involves contributing to make crime profitable and effective. If payment consists in infecting and forcing others to pay, as in *Popcorn Time*, the victim would become an author or collaborator for directly participating in the commission of the crime.

(ii) Once it is clear that the ransom should not be paid, monetary or otherwise, the next step is to isolate the infected machine to clean it. However, how to be sure about that? Since it is possible that malware persists even after system formatting (take into account that malicious software can be embedded into personal files like pdf), the best option is device replacement instead of simple cleaning.

This option would entail an increase in the amount of the economic damage suffered as a result of ransomware and, consequently, a possible aggravation of the sanction to be imposed through juridical or judicial means.

(iii) In this line, it is recommended to restore the data affected by ransomware from data backups (see *Prevention* above). As an example of this, consider the case of the San Francisco Municipal Transportation Agency, which in 2016 fell victim to a ransomware attack by *Mamba* or *HDDCryptor* that disrupted train ticketing and bus management systems. Attackers demanded a whopping 100 Bitcoin ransom (equivalent to about $73,000 at the time), but thanks to a speedy response and comprehensive backup processes, the SFMTA was able to restore its systems within two days.

Whichever the recovery plan adopted, it is important to urgently report incidents to law enforcement agencies to make it possible to prosecute and punish the illegal action. Otherwise, the intrusion will go unpunished and, probably, reattempted since it has not been sanctioned. A technical response without legal complaint action is a quick short-term solution. But it is not the best option in the medium or long term because the intrusion is more likely to be repeated if there are no legal consequences.

*5.4. Ransomware Attribution, Prosecution, and Sanction.* To a large extent, in the case of ransomware, impunity is due to the fact that "*the extortion takes place in a way that does not compromise the attacker's identity* [21]." Attribution is one of the biggest challenges in the fight against ransomware. As Marinos and Barrios point out, "*Knowing who is responsible or attributing responsibilities to a person or a group for a cybersecurity incident is still a very daunting task and often a worthless exercise* [17]."

The problems of technical traceability and anonymity that characterize cyber actions make it difficult to attribute the actions to a perpetrator or perpetrators. In the case of ransomware, there is an additional problem: the general propensity of the victims to pay the ransom and not to use the existing legal channels to denounce the facts. Due to lack of knowledge, fear of the consequences, fear of losing their reputation, or for any other reason, victims tend to pay the ransom and not to report the facts. As EUROPOL indicates, several law enforcement authorities approach victims to assist them by potentially starting a criminal investigation. But "*this was not generally a priority of the victim organization, as the primary focus was on business continuity and limiting reputational damage*" [9].

The result is that ransomware has really become like an iceberg paradigm. Under-reported crime is a reality. Moreover, the profusion of data on attacks, cases, victims, and payments is in contrast to the absence of data on condemnations and penalties. Paquet-Clouston et al. conclude that "*global and reliable statistics on the impact of cybercrime in general, and ransomware in particular, are missing, causing a large misunderstanding regarding the severity of the threat and the extent to which it fuels a large illicit business. Most of the statistics available on cybercrime and ransomware are produced by private corporations* [46]."

Moreover, even when the facts are reported, the prosecution of the crime is complicated by the difficulty of accessing the evidences needed to incriminate the perpetrators. Ransoms are often paid through cryptocurrency, so they are difficult to trace [18]. With a different opinion, Irwin

and Dawson consider that "*following the money trail is traditionally an effective way of tracking down the perpetrators of crime*." Nevertheless, they recognise that "*although many law enforcement agencies investigate crimes involving cryptocurrencies, such as Bitcoin, there is no standardised, cohesive approach across law enforcements agencies or jurisdictions* [65]." Some authors have been working to design investigation and prosecution processes following the payment trail [43]. Paquet-Clouston et al. have proposed a Bitcoin Traceability Research [46]. For Irwin and Dawson, "*the global regulation of cryptocurrencies and other cybercurrencies can assist in addressing the challenges of attribution when investigating ransomware attacks and other types of cybercrime using these payment methods* [65]," this task of globally regulating of cryptocurrencies, is not simple.

In the end, only a percentage of ransomware attacks are reported, only a percentage of these can be traced and attributed, and only a percentage within of can be prosecuted and ultimately criminally sanctioned. Without sanction, there is no deterrence. Without punishment, there is impunity. With impunity, crime remains profitable and will not stop. Technical measures are able to tackle the ransomware problem in the immediate or short term and on a case-by-case basis. Legal measures and sanctions can and have to provide an effective solution to the global problem. Otherwise, not only the effectiveness but also the very legitimacy of the legal system may be put into question.

## 6. Conclusions

Ransomware has become a serious security issue [29]. As Scherer note, "*Ransomware is not going anywhere and while the meteoric rise and spread of Ransomware has been startling as a singular issue, it also serves as a clear warning of things to come. There is still plenty of room for innovation and tremendous incentives for criminals to pursue these opportunities* [4]." In addition, as Aldaraani and Begum explain, "*It is expected that in the near future, with the increasing number of devices connected to the network, ransomware will soon spread to new categories of devices* [22]."

Among the solutions provided by scientific doctrine, prevention is one of the most important. Aurangzeb et al. conclude that the only way to avoid being affected from this malicious kind of software is to implement precautionary measures [26]. According to Humayun et al. prevention becomes easier than getting a remedy after the ransomware attack. In their opinion, ransomware could only be defeated by promoting a shared responsibility. So, "*User behavior and user training is the key to protect the industries, organizations, and individuals from being infected*" [29]. Prevention techniques alongside with response measures are the main instruments against ransomware for Atapour-Abarghouei et al. [16]. In the same way, education and vigilance to guide strategic responses to ransomware are the proposal defended by Sherer alongside with a proactive approach to it [4].

Also, with a mainly precautionary approach, Taylor and Patel propose an early-warning detection system, *CryptoDrop*, that alerts a user during suspicious file activity. They argue that "*implementing practical defense mechanisms is possible by continuously monitoring the file system activity and registry activity, so if these registry values are put under continuous observation then, detection of ransomware is possible* [30]." Ali et al. defend the use of preventive and detection technical solutions like security backup and antivirus [35].

By their part, Oz et al. recommend the use of technical solutions focused in PCx/workstations and IoT [66]. Following Berrueta et al. the best protection is offered by a combination of detection and backup policies through which the original files can be recovered. But the authors point out that "*the results offered in the literature for the different proposals were difficult, if not impossible, to compare. They did not target the same ransomware families and presented results using different metrics. A unified evaluation and comparison scenario is needed for serious reproducible research* [27]." Bijitha et al. also advocate a revision of the technical solutions [60]. Rehman et al. set up the technical theoretical basis for a high assurance framework [13]. Zimba and Chishimba suggest a most theoretical approach through a ransomware categorization framework based on the virulence of the attack [28]. Finally, Hull et al. propose a predictive model of ransomware stages [34].

From a different perspective, following their empirical study on the experience of organizations, Connelly and Wall set some interesting proposals including the conclusion that "*the strength of ransomware is not in its technical capabilities and rapid evolution; rather, it lies within relentlessness of hackers who are persistently searching for a range of weaknesses within organizations* [24]." Previously, they have defended that "*there is no simple technological* "*silver bullet*" *... Rather, a multilayered approach is needed which consists of sociotechnical measures, zealous front-line managers and active support from senior management* [39]." Trautman and Ormerod propose a governance security model for corporations [15]. However, the references to the current cybersecurity legal framework included in this work are not accurate enough.

Although with different arguments and procedures, Paquet-Clouston et al. Conti et al. and Irwin and Dawson propose following the money trail as an effective way of tracking down the perpetrators of crime. They agree on the fact that "*money laundering and terrorism financing activities are traditionally detected, investigated, and prosecuted through the proper implementation of strict financial transaction reporting* [43, 46, 65]."

Finally, legal studies are focused on certain issues such as the juridical implications of ransomware when it is to be considered a law breach under data privacy laws or data protection laws [14]. In this regard, the main recommendations of the RTF report are: (1) the definition of a comprehensive and resourced strategy through coordinated, international diplomatic and law enforcement authorities' efforts; (2) a sustained, aggressive, whole-of-government, intelligence-driven antiransomware campaign, led by the United States; and (3) an internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks [18]. In addition, this report also

proposes the establishment of cyber response and recovery funds and close regulation of the crypto-currency sector.

In spite of these last references, at the end, the overwhelming majority of the proposed solutions against ransomware are of a technical nature. There are few solutions of any other nature. There are no interdisciplinary proposals despite the fact that the two main reasons for ransomware's success as a criminal activity are *effectiveness* and *impunity*. Effectiveness is mainly a technical issue but impunity is definitely a legal problem. Impunity is the main incentive for this unlawful act.

After the interdisciplinary analysis made in this work, three conclusions can be drawn:

(i) First, concerning the technical and legal fundamentals, the main problem is that the existing regulations at the international and domestic level have not been adapted to the technical nature and evolution of ransomware.

(ii) Second, with regard to the defense guidelines, the legal framework needs to be clarified and strengthened by better adapting it to the technical defense mechanisms.

(iii) Third, at the same point, the technical response should be considered a partial, case-by-case, and short-term solution. The long-term and global solution has to be provided by law.

A legal solution requires some basic changes. The first one is the typification of ransomware as an autonomous and specific crime, taking into account its technical uniqueness. Secondly, the penalisation of incitement, complicity, and the attempt to commit this offence would be an effective approach to limit or reduce impunity. Ransomware is an intrusion that would have to be prosecuted and sanctioned by its simple execution intentionally and without right because it affects the integrity of the devices or data. Thirdly, the prohibition and penalisation of insurance contracts for the payment of ransom is a necessary measure to prevent legal instruments from becoming an additional incentive for criminals in a regrettable perversion of the system. Finally, international cooperation is the main instrument for dealing with the impunity arising from the fact that it is a generally transnational crime. According to the joint statement of the ministers and representatives from the Counter Ransomware Initiative means that there is a common understanding on the need for international cooperation, "*the threat of ransomware is complex and global in nature and requires a shared response. A nation's ability to effectively prevent, detect, mitigate, and respond to threats from ransomware will depend, in part, on the capacity, cooperation, and resilience of global partners, the private sector, civil society, and the general public*" (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021). Although it is a limited agreement due to its political nature, it could be a first step towards a binding international regulation to effectively combat ransomware.

At the end, without a proper legal sanction and without a proper punishment, the crime will be repeated and extended because of the lack of harmful consequences for the aggressor. Technical solutions intended to mitigate the problem are essential, but without adequate legal support, it is difficult to fight effectively against this pandemic.

It is essential to coordinate and merge the technical and legal approaches to provide a feasible response to the problem of ransomware. Trust in the law and justice are also at stake.

## Data Availability

No data or databases have been used in this research. Therefore, they cannot be shared because they do not exist. The research is the result of the analysis of regulations, legislation, documentation, and literature on the subject cited in the references.

## Conflicts of Interest

The authors declare that there are no conflicts of interest.

## Acknowledgments

This work is partly supported by the Spanish Ministry of Economy and Competitiveness and ERDF (European Regional Development Fund) funds through project PID2020-114495RB-I00.

## References

[1] Sophos, "The State of Ransomware 2021," 2021, https://secure2.sophos.com/en-us/medialibrary/pd fs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

[2] FBI, "High-Impact Ransomware Attacks Threaten US Business and Organizations," 2020, https://www.1stsource.com/advice/business/sbr_template.cfm?docnumber=pl34_0025s.htm.

[3] CyberEdge, "Cyberthreat Defense Report," 2021, https://cyber-edge.com/cdr/.

[4] J. A. Sherer, "Ransomware -practical and legal considerations for confronting the new economic engine of the dark web," *Richmond Journal of Law and Technology*, vol. XXIII, pp. 1–49, 2017.

[5] P. R. Kumar and H. R. E. Ramlie, "Anatomy of ransomware: attack stages, patterns and handling techniques," *Advances in Intelligent Systems and Computing*, vol. 12, pp. 205–214, 2021.

[6] CSO, "Recent ransomware attacks define the malware's new age," 2018, https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html.

[7] DigitalGuardian, "A History of Ransomware Attacks," *The Biggest and Worst Ransomware Attacks of All Time*, vol. 12, 2019.

[8] J. DeCapua and S. Francisco, "Feds fighting ransomware: how the FBI investigates and how you can help," *Seminar "Emerging Threats" at RSA Conference*, vol. 1, 2020.

[9] EUROPOL, "European union agency for law enforcement cooperation," 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organise d-crime-threat-assessment-iocta-2020.

[10] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," *Computers & Security*, vol. 92, Article ID 101762, 2020.
[11] R. V. Gundur, M. Levi, and V. Topalli, "Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context," *CrimRxiv*, vol. 3, 2021.
[12] ENISA, "Ransomware threat landscape 2021," 2021, https://www.enisa.europa.eu/publications/enisa-t hreat-landscape-2021.
[13] H. Rehman, E. Yafi, M. Nazir, and K. Mustafa, *Security Assurance Against Cybercrime Ransomware*, vol. 866, 2019.
[14] M. Brewczynska, S. Dunn, and A. Elijahu, "Data privacy laws response to ransomware attacks: a multi- jurisdictional analysis," *Information Technology and Law Series*, vol. 32, 2019.
[15] L. J. Trautman and P. C. Ormerod, "Wannacry, ransomware, and the emerging threat to corporations," *Tennessee Law Review*, vol. 86, no. 503, pp. 505–556, 2019.
[16] A. Atapour-Abarghouei and A. S. McGough, "Volenti non fit injuria: ransomware and its Victims," *IEEE International Conference on Big Data (Big Data)*, vol. 1, pp. 4701–4707, 2019.
[17] L. Marinos and L. Barros, "Main incidents in the EU and worldwide ENISA threat landscape," 2020, https://www.researchgate.net/publication/348154220_Main_incidents_in_the_EU_and_worldwide_ENISA.
[18] RansomwareTaskForce, "Combatting Ransomware. A comprehensive framework for action: key recommendations from the Ransomware Task Force," 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.
[19] R. Diesch, M. PfaffPfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, Article ID 101747, 2020.
[20] S. AlGhamdi, K. T. WinWin, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: systematic review," *Computers & Security*, vol. 99, Article ID 102030, 2020.
[21] A. S. A. Bander, B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions," *Computers & Security*, vol. 74, pp. 144–166, 2018.
[22] N. Aldaraani and Z. Begum, "Understanding the impact of ransomware: a survey on its evolution, mitigation and prevention techniques," *21st Saudi Computer Society National Computer Conference (NCC)*, vol. 12, pp. 1–5, 2018.
[23] A. H. Mohammad, "Ransomware evolution, growth and recommendation for detection," *Modern Applied Science*, vol. 14, no. 3, p. 68, 2020.
[24] L. Y. Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability," *Journal of Cybersecurity*, vol. 6, no. 1, pp. 12–18, 2020.
[25] G. Krunal and P. Viral, "Survey on ransomware: a new era of cyber attack," *International Journal of Computer Application*, vol. 168, no. 3, pp. 38–41, 2017.
[26] S. Aurangzeb, M. Aleem, M. A. Iqbal, and M. A. Islam, "Ransomware: a survey and Trends," *Journal of Information Assurance and Security*, vol. 12, no. 2, pp. 48–58, 2017.
[27] E. Berrueta, D. Morato, E. Magana, and M. Izal, "A survey on detection techniques for cryptographic ransomware," *IEEE Access*, vol. 7, pp. 144925–144944, 2019.
[28] A. Zimba and M. Chishimba, "Understanding the evolution of ransomware: paradigm shifts in attack structures," *International Journal of Computer Network and Information Security*, vol. 11, no. 1, pp. 26–39, 2019.
[29] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 105–117, 2021.
[30] J. P. Tailor and A. D. Patel, "A comprehensive survey: ransomware attacks prevention, monitoring and damage control," *International Journal of Research and Scientific Innovation (IJRSI) IV(VIS)*, pp. 116–121, 2017.
[31] F. Malecki, "Best practices for preventing and recovering from a ransomware attack," *Computer Fraud & Security*, vol. 2019, no. 3, pp. 8–10, 2019.
[32] F. Tang, B. Ma, J. Li, F. Zhang, J. Su, and J. Ma, "RansomSpector: an introspection-based approach to detect crypto ransomware," *Computers & Security*, vol. 97, Article ID 101997, 2020.
[33] M. Scalas, D. Maiorca, F. Mercaldo, C. A. Visaggio, F. Martinelli, and G. Giacinto, "On the effectiveness of system API-related information for Android ransomware detection," *Computers & Security*, vol. 86, pp. 168–182, 2019.
[34] G. Hull, H. John, and B. Rief, "Ransomware deployment methods and analysis: views from a predictive model and human responses," *Crime Science*, vol. 8, no. 1, p. 2, 2019.
[35] A. Ali, R. Murthy, and F. Kohun, "Recovering from the nightmare of ransomware - how savvy users get hit with viruses and malware: a personal case study," *Issues in Information System'*, vol. 17, no. IV, pp. 58–69, 2016.
[36] T. Kurpjuhn, "The Guide to Ransomware: How Business Can Manage the Evolving Threat," *Computer Fraud & Security*, vol. 2019, no. 11, pp. 14–16, 2019.
[37] A. Shahim, "Security of the digital transformation," *Computers & Security*, vol. 108, Article ID 102345, 2021.
[38] G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel, "Cybercrime threat intelligence: a systematic multi-vocal literature review," *Computers & Security*, vol. 105, Article ID 102258, 2021.
[39] L. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures," *Computers & Security*, vol. 87, Article ID 101568, 2019.
[40] ComissionAdHoc, *Le droit penal à l'épreuve des cyberattaques*, Rapport du Club de Juristes, Paris, 2021.
[41] UK Government, "The rise of ransomware," 2020, https://www.ncsc.gov.uk/blog-post/rise-of-ransomwa.
[42] UKGovernment, "Mitigating malware and ransomware attacks," 2021, https://www.ncsc.gov.uk/guidan ce/mitigating-malware-and-ransomware-attacks.
[43] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: a bitcoin transactions perspective," *Computers & Security*, vol. 79, pp. 162–189, 2018.
[44] M. N. Olaimat, M. A. Maarof, and B. A. S. Al-rimy, "Ransomware anti-analysis and evasion techniques: a survey and research directions," in *Proceedings of the 3rd International Cyber Resilience Conference*, pp. 1–6, China, June 2021.
[45] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: a bitcoin transactions perspective," *Computers & Security*, vol. 79, pp. 162–189, 2018.
[46] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," 2018, https://arxiv.org/abs/1804.04080.
[47] U. Tatar and Y. Gokce, "Law versus technology: blockchain, GDPR, and tough tradeoffs," *Computers and Law*, vol. 38, no. 1, Article ID 05454, 2020.

[48] A. Mohanta, M. Hahad, and K. Velmurugan, "Preventing Ransomware: Understand, Prevent, and Remediate Ransomware Attacks," *Packt*, vol. 1, 2018.
[49] D. C. L. Nguyen and D. W. Golman, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'," *Computer Law & Security Report*, vol. 40, Article ID 105521, 2021.
[50] E. Nováčková, *Current Cyberthreats and Relevant Legal Instruments in EU and Canada. Prage Law Working Papers Series*, Charles University Law Faculty, Canada, 2018.
[51] H. U. Salvi and R. V. Kerkar, "Ransomware: a cyber extortion," *Asian Journal of Convergence in Technology*, vol. 2, no. 2, pp. 1–6, 2015.
[52] Statista, "Ransomware families worldwide," 2021, https://www.statista.com/statistics/701029/number-of.
[53] TrendLabs, "1H Security Roundup: The Reign of Ransomware," 2016.
[54] TrendMicro Ransomware, "Past, present, and future," 2016, https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf.
[55] KeepnetLabs, "Top 11 Ransomware Attacks in 2020-2021," 2021, https://www.keepnetlabs.com/top-11.
[56] McAfee, "McAfee Labs Threats Report," 2019, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterl y-threats-aug-2019.pdf.
[57] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: a look under the hood of ransomware attacks," in *Proceedings of the 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, pp. 1–20, Seoul Korea, July 2015.
[58] Cybereason, "Cybereason's Newest Honeypot Shows How Multistage Ransomware Attacks Should Have Critical Infrastructure Providers on High Alert," 2020, https://www.cybereason.com/blog/cybereason-honeypot-multistage-ransomware.
[59] J. A. Gómez-Hernández, L. Álvarez-González, and P. García-Teodoro, "Locker: thwarting ransomware action through a honeyfile-based approach," *Computers & Security*, vol. 73, pp. 389–398, 2018.
[60] C. V. Bijitha, R. Sukumaran, and H. V. Nath, "A survey on ransomware detection techniques," *Communications in Computer and Information Science*, vol. 1186, pp. 55–68, 2020.
[61] McAfee, "How to Protect against Ransomware," 2020, https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-how-to-protect-against-ransomware.pdf.
[62] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting Ransomware Using Process Behavior Analysis," *Procedia Computer Science*, vol. 168, pp. 289–296, 2020.
[63] J. A. Herrera Silva, L. I. Barona López, A. L. Valdivieso Caraguay, and M. Hernández-Álvarez, "A survey on situational awareness of ransomware attacks-detection and prevention parameters," *Remote Sensing*, vol. 11, no. 10, p. 1168, 2019.
[64] H. AlshaikhAlshaikh, N. Ramadan, and H. AhmedAhmed, "Ransomware prevention and mitigation techniques," *International Journal of Computer Application*, vol. 177, no. 40, pp. 31–39, 2020.
[65] A. S. M. Irwin and C. Dawson, "Following the cyber money trail," *Journal of Money Laundering Control*, vol. 22, no. 1, pp. 110–131, 2019.
[66] H. Oz, A. Aris, A. Levi, and A. S. UluagacUluagac, "A survey on ransomware: evolution, taxonomy, and defense solutions," *ACM Computing Surveys*, vol. 1–39, 2022.