ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

Publisher
http://jssidoi.org/esc/home

THE SOCIAL AND LEGISLATIVE PRINCIPLES OF COUNTERACTING RANSOMWARE CRIME

Mafura Uandykova [1], Anton Lisin [2]*, Diana Stepanova [3], Laura Baitenova [4], Lyailya Mutaliyeva [5], Serhat Yuksel [6], Hasan Dincer [7]

[1,4]Narxoz Uniiversity, St. Zhandosova, 55, 050035, Almaty, Republic of Kazakhstan
[2]Financial University under the Government of the Russian Federation, 125167, Leningradsky Ave, 49, Moscow, Russian Federation
[3]Plekhanov Russian University of Economics, Stremyanny Lane 36, 117997, Moscow, Russian Federation
[5]L. N. Gumilyov Eurasian National University, Satpayev str. 2, 010008, Nur-Sultan, Republic of Kazakhstan
[6,7]Istanbul Medipol University, 34083, Istanbul, Turkey

*[*1]E-mail: mrfoxv@list.ru (corresponding author)*

Received 15 March 2020; accepted 24 September 2020; published 30 December 2020

Abstract. This article aims to analyze the relationship between the threat of ransomware and new effective counteraction principles for law enforcement agencies to utilize. Moreover, it contemplates on how specific behavior of persons can help reduce the threat of being infected with this malicious software. It establishes that certain changes made in society's mentality towards their computer and network systems can significantly reduce the consequent damages of ransomware attacks. The manuscript uses a qualitative research approach and the analysis of variance (ANOVA), including an F-test, which defines major challenges in ransomware. This is the first empirical research piece which uses this type of data and approach for the analysis of current threats in global ransomware security. The article suggests that the main challenge is the systematic growth of ransomware connected to illegal businesses and the inattentive actions of casual users. The research paper proposes the implementation of global ransomware counteraction principles on the base of challenges that are present now and the prospects of rising threats in the future. In addition, the manuscript analyzes the trends of the last 2-years of attacks to find and determine new ways of successfully counteracting it for optimal innovative regional development.

Keywords: organizational performance; cybercrimes; innovation; regional development; information; security awareness; ransomware; law

Reference to this paper should be made as follows: Uandykova, M., Lisin, A., Stepanova, D., Baitenova, L., Mutaliyeva, L., Yuksel, S., Dincer, H. 2020. The social and legislative principles of counteracting ransomware crime. *Entrepreneurship and Sustainability Issues* 8(2), 777-798. http://doi.org/10.9770/jesi.2020.8.2(47)

JEL Classifications: K24, R58, R59, K16, M15

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

1. Introduction

The post-industrial era makes global digital technologies accessible and easy-to-use. Today's society is reliant on the internet, although the effects of this dependence is a common topic of debate. Information Technologies (IT) provide many services that contribute to making our everyday lives simpler and more organized.

However, availability of global digital technologies opens opportunities for individuals who are looking to take advantage of their vulnerabilities. Security breakdowns can lead to economic losses of innocent citizens, companies and even governments. Worse still, perpetrators can use computers and network systems to raise alarms, create panic in anticipation of violent ransomware attacks–and to coordinate and carry out terrorist acts. To great despair, counteraction of cybercrime has faced many problems, which have yet to be resolved (Zimba et al., 2018; Plėta et al., 2020).

One of the most effective ways of bypassing security protocols of computer systems and consequently infecting them is through ransomware. Ransomware is one of many categories of malicious software and affects masses of computers: ranging from family desktop PCs to corporate systems. Ransomware is described as a "kind of malware which demands a payment in exchange for a stolen functionality". Unfortunately, these ransomware attacks are prominent to this day and pose a significant threat.

Researchers have attributed the lack of an acute response to these crybercrimes to many factors. Among them is IT professionals' lack of understanding and interest in the phenomenon of cybercrime. Moreover, law enforcement officials lack the tools necessary to address the problem: old laws cannot conform with committed crimes. At the same time, new laws have very few judicial precedents that can be guided (Mercaldo et al., 2016).

As will be further discussed in the study, virtually everyone has the potential to counter cybercrime, especially ransomware. And if everyone is well-informed, attentive and careful, society in its entirety will have a better understanding of the principles of preventing these ransomware attacks. Of course, lots of changes will have to be made to achieve this (Kurpjuhn, 2019). But two groups specifically can increase their efforts to handle this problem and pave the way for countering this phenomenon (Chung, 2019; Al-rimy et al., 2018).

Another problem that should be emphasized is that everyone is talking about cybercrime despite not having an official definition of it (O'Kane et al., 2018).

2. Literature review

As cyberspace becomes more prominent in the modern world, it is evident that law enforcement agencies are not always able to keep up with its rates of growth. The scale at which IT has consumed the world has made systematicly and successfully committing cybercrimes possible. Because of this, networks of cyberfraud begin to nest in virtual space and harm individuals, governments, businesses. Responses to these actions should be strategical, tactical, and cooperative (Fagioli, 2019).

Cybercrime counteraction faces many problems. The general confusion surrounding the definition of cybercrime is an issue that needs to be addressed and resolved. A lack of professionals correctly determining the unique nature and threats of cybercrime could result in an array of complications which make counteracting it even harder.

There are many reasons justifying the development of a model definition of cybercrime specifically. A standardized perception of cybercrime across IT personnel, computer users, victims, police officers, detectives, prosecutors and judges will lead to the aforementioned unification of different social institutions, which, above all

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

else, is arguably the most important aspect of dealing with this lawlessness. Furthermore, the problem of insufficient and unreliable statistics could begin to be resolved if different participating branches use a single classification of cybercrime (Furnell and Emm, 2017; Genc et al., 2018).

Cybercrime definition should be unified not only among agencies, but among countries as well, due to the possibilities that cyberspace, the virtual space in which cybercrimes are committed, grants. This virtual world allows crimes to happen wherever. Thus, a mutual understanding of cybercrime across the globe is necessary to counteract this aspect of the problem (Kolodenker et al., 2017; Alwaelya et al., 2020; Yumashev and Mikhaylov, 2020; Yumashev et al., 2020).

Cybercrime definition would aid not only cooperation between agencies but also all parties individually. For example, IT professionals need a good definition of cybercrime to know when (and what) to report to authorities. At the same time, law enforcement needs a legislative definition of this type of crime to prosecute offenders, as laws must be defined in order to be enforceable (Pope, 2016).

Attempts to define cybercrime illustrate that it is a very generalized term. Practically speaking, these definitions are useless in almost any discussion, especially that which attempts to fully analyze cybercrime. This research paper now presents some noteworthy interpretations of cybercrime (Paquet-Clouston et al., 2019).

Many state-level and international organizations have attempted to give a working definition. The Council of Europe's Cybercrime Treaty's definition of cybercrime is broad, including such offences as criminal activity aimed at collecting or manipulating data and even copyright infringement. The United Nations Manual on the Prevention and Control of Computer Related Crime on the other hand, includes more misdemeanors, such as forgery, unauthorized access to computer systems and fraud. Symantec Corporation, which is a company specializing in computer security, gives the following definition of cybercrime: "any crime that is committed using a computer or network, or hardware device". At this point in the 21st century though, almost any action of any person in a First-world country utilizes the listed elements, so, perhaps, the line between a regular crime and cybercrime becomes too blurry.

Other studies and research papers are categorizing cybercrimes in order to come to a more cohesive conclusion. Gordon and Ford (2006) brought the idea of distinguishing Type I and Type II cybercrime based on the offences' characteristics, including whether or not the act was limited to computer systems exclusively (Covic and Voß, 2019; Mikhaylov and Tarakanov, 2020, Mikhaylov and Sokolinskaya, 2019).

Conversations and discussions on cybercrime in general can be extensive. However, this study focuses on one of the most common offences in cyberspace: ransomware. Ransomware, as has been already stated, is a type of malicicious software (Malware) which infects many Personal Computers. The infection, generally, can be in two forms. The first one completely locks out the user from accessing their system unless a ransom is paid. The other form restricts access to sensitive documents and information under the threat of deleting them unless the same condition is met. The size of the ransom can vary depending on the victim and situation, and criminals often demand the fee be payed in Bitcoin due to the privacy and lack of transparency that comes with cryptocurrency payements and transfers. Regardless, the general consensus is to not pay the ransom, as in doing so, the victim is proving the hackers' scheme to be profitable and they will continue to harm other systems. Moreover, no victim can be sure that the criminals will "hold up their end of the bargain" and actually unlock the system and/or files (Gonzales and Hayaineh, 2017; Zhang et al., 2019; Meynkhard, 2019; Lopatin, 2019; Lopatin, 2020; Denisova et al., 2019; Mikhaylov, 2018a; Mikhaylov, 2018b).

Although CryptoWall, which had become the leading version of ransomware in 2015, had great reputation for decrypting files after paying the fee, far from many other criminals and systems were as honest, which, of course,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

is unsurprising. Because of this and many other reasons, involving the threat of more frequent ransomware attacks in the long term, the demanded sum of money had never been paid in over 3% of known cases (Richardson and North, 2017; Szlosarek et al., 2019; Covic and Voss, 2019; Dorantes-Argandar et al., 2019; Iliopoulou et al., 2019; Huang et al., 2019; Hadiuzzaman et al., 2019; Jasti et al., 2019).

Ransomware has been terrorizing persons' computer systems for over a decade now. The volume of these infections when the first ransomware ransomware attacks were made was initially low. Nevertheless, the rate at which ransomware spread increased over 500% in the year 2013 when compared to previous years. One of the many reasons that the number of ransomware attacks had increased exponentially was due to the fact that ransomware has shifted from infecting business network systems and computers to personal computers in households. It is noteworthy that these ransomware attacks are also more frightening, which is explained by the nature of household users to neglect backing up their files and using an effective antivirus that may prevent such happening in the first place (Connolly and Wall, 2019; Meynkhard, 2020b; Nyangarika et al., 2018; Nyangarika et al., 2019a, Meynkhard, 2020a; Nyangarika et al., 2019b).

Malware itself is accompanied by other viruses and worms, which harm computer systems and are a breach of security and privacy. One of the key issues relating to this subject is that programs meant to decrease victimization risk are not very effective. As of 2020, it is estimated that 33.28% of unprotected computer systems are infected with malware. Compare this to the 25% of PCs that are infected despite having anti-virus programs installed, and it would seem, as indicated by the relatively small spread between the figures, that these applications alone cannot prevent infections from happening. Moreover, criminology and IT are not capable of single-handedly counteracting this problem. It is an individual's responsibility to be familiar with the consequences of browsing suspicious and unsafe websites and change their behavior accordingly (An and Dorofeev, 2019; Brewer, 2016; Varyash et al., 2020; Moiseev et al., 2020; Nie et al., 2020).

Taking these facts into consideration, self-control is an important factor when analyzing victimization rates. It is a user's responsibility to be wary of visited websites and downloaded files. Low levels of self-control contribute to certain types of security breaches, data manipulation, and on-line harassment. Not only that, but these individual characteristics can be associated with minor cyberdeviance. These discoveries illustrate that individual characteristics and decisions are vital for safety in cyberspace but are not able to sufficiently provide a full line of security (Everett, 2016; Mohurle and Patil, 2017; Mikhaylov, 2019; Dayong et al., 2020; Denisova et al., 2019; Dooyum et al., 2020).

Among many cyberspace attacks, ransomware in particular is dependant and reliant on the behavior of the infected user – the victim. Ransomware attacks can be coordinated, targeting a specific system, e.g. a company's network of computers. However, these offences often happen due to a lack of attention from potential users – they "accidentally" get infected whilst visiting suspicious websites and downloading unsafe files. The behaviour of a user is presented not only by whether or not he has been infected, but also by his decision to pay the ransom or not. This is a key component in understanding and preventing ransomware attacks, because the decision to comply with hackers can give them incentive to keep their criminal spree going (Bhardwaj et al., 2016; Aurangzeb et al., 2017). This problem for IT-infrastucture of transport sector is researched (Chiabaut and Barcet, 2019; Nguyen et al., 2019; Bešinović and Goverde, 2019; Enayatollahi et al., 2019; Mohri and Akbarzadeh, 2019; Sun and Apland, 2019; Jevinger and Persson, 2019; Czioska et al., 2019; Heyken Soares et al., 2019; Habib and Hasnine, 2019; Malucelli and Tresoldi, 2019; Downward et al., 2019; Candelieri et al., 2019).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

3. Materials and methods

A qualitative research approach is used in this study to reach its goals. Qualitative inquiries can be used for deep studying of ransomware crime like researchers before (Connolly and Wall, 2019). A focus group was created in order to be examined and analyzed. Our sample is made by persons who had rich experience with crypto-ransomware ransomware attacks.

Several measures were taken to verify the study's results and ensure reliability of the findings. Secondary data served as an important validator of discoveries. Moreover, the employment of a purposeful sampling technique prevented sampling distortion. The sample size itself was determined by the principle of theoretical saturation, equating to 30 interviewees.

Another key technique used in the study was asking respondents to provide feedback on interview transcripts and study findings and subsequently rationalizing them. The results of the survey were shared with an experienced researcher from TrendMicro, who provided important expert comments. All findings are supported by interviewees' quotes, providing additional verification. Finally, study informants showcased a high degree of unanimity about the necessary organizational measures needed to respond to the crypto-ransomware threat suggests that the results are reliable and will not change significantly if additional organizations were to be interviewed.

It is our belief that these precautions have eliminated most inaccuracies and misunderstandings from the data collection. Although we do not claim that the list of proposed measures is exhaustive, the utilization of the aforementioned principles ensures reliable results. As for the validity of findings, the situation is generally more complex. Interviews inevitably allow participants to answer questions in ways that distort facts. However, in this study, the situation appears to be unique. Participants had various incentives to provide factual answers. Although we do not claim that the study participants were entirely honest or forthcoming, several factors allow us to conclude that interviewees provided trust- worthy replies (Mikhaylov, 2020a; Mikhaylov, 2020b; Mikhaylov et al., 2020).

This conclusion can be made based on several reasonings. The majority of victims suffered greatly from crypto-ransomware attacks, including personal emotional distress as well as physical damage to IT infrastructure. The key incentive for participation in this study was to share their experiences with the aim to prevent future ransomware attacks on other organizations. Interviewees appeared to be genuinely concerned with the threat that these attacks present, including its recent proliferation and the consequences it may entail. Several respondents strongly disapproved the fact that many organizations are hiding active cyber-ransomware attacks. Moreover, several interviewees were appalled by the fact that criminals held them hostages and wanted to 'share their story' and warn others (Mikhaylov et al., 2019; Mikhaylov et al., 2018).

Almost all victims actively participated in validation exercises and expressed a keen interest in receiving final results and conclusions. As for Police Officers from the CCUs, the very nature of their job is to reduce cybercrime. Hence, they have a genuine interest in providing objective data. Our observation was that law enforcement representatives readily shared data on ransomware ransomware attacks, carefully concealing victims' identities. Other tactics that may have ensured honesty in informants included clearly communicated anonymity procedures, an option to change or delete parts of text in the transcripts (Sunchalin et al, 2019; Gura et al., 2020; Mikhaylov et al., 2020; Prosekov et al., 2020).

With respect to the respondents' confidentiality, aliases are used for the informants and ransom amounts are concealed, as the latter could otherwise be used to identify some of the interviewees (Table 1).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

Table 1. Ransomware types and targets.

Organisation alias	Industry	Target
LawEnfJ	Law enforcement; small; public	Person
GovSecJN	Military; large; public	Person
GovSecJ	Military; large; public	Multiple ransomware attacks
EducInstF	Education; large; public	Computer
EducInstFB	Education; large; public	Computer
LawEnfM	Law enforcement; small	Multiple ransomware attacks
GovSecA	Military; large; public	Computer
LawEnfJU	Law enforcement; medium; public	Person
HealthSerJU	Health service; large; public	Multiple ransomware attacks
LawEnfF	Law enforcement; medium; public	Person
ITOrgA	IT; small; private	Computer
ConstrSupA	Construction; small; private	Computer
EducOrgA	Education; small; public	Computer
SecOrgM	IT; small; private	Person
ITOrgJL	IT; small; private	Computer
CloudProvJL	IT; small; private	Computer
InfOrgJL	Infrastructure; medium; private	Computer
ConstrSupJ	Construction; small; private	Computer
RelOrgJ	Religion; medium; private	Person
SportClubJ	Sport; large; private	Computer
UtilOrgD	Utilities; large; private	Computer

Source: authors

The data was used between January and December 2018. The interview questions are as follows:

Can you please describe the experience of the ransomware incident?
What made you understand that a ransomware ransomware attack took place?
What was the source of the ransomware?
In your opinion, why was the ransomware effective in infecting the network?
Does your organization have ransomware policies and provide specific training?
Does your organization backup its files and electronic documents?
Does your organization utilize antivirus software?
Does your organization have cybersecurity insurance that overs ransomware?
What did you learn from this experience?
What changes have been made in the organization following the ransomware attack?

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

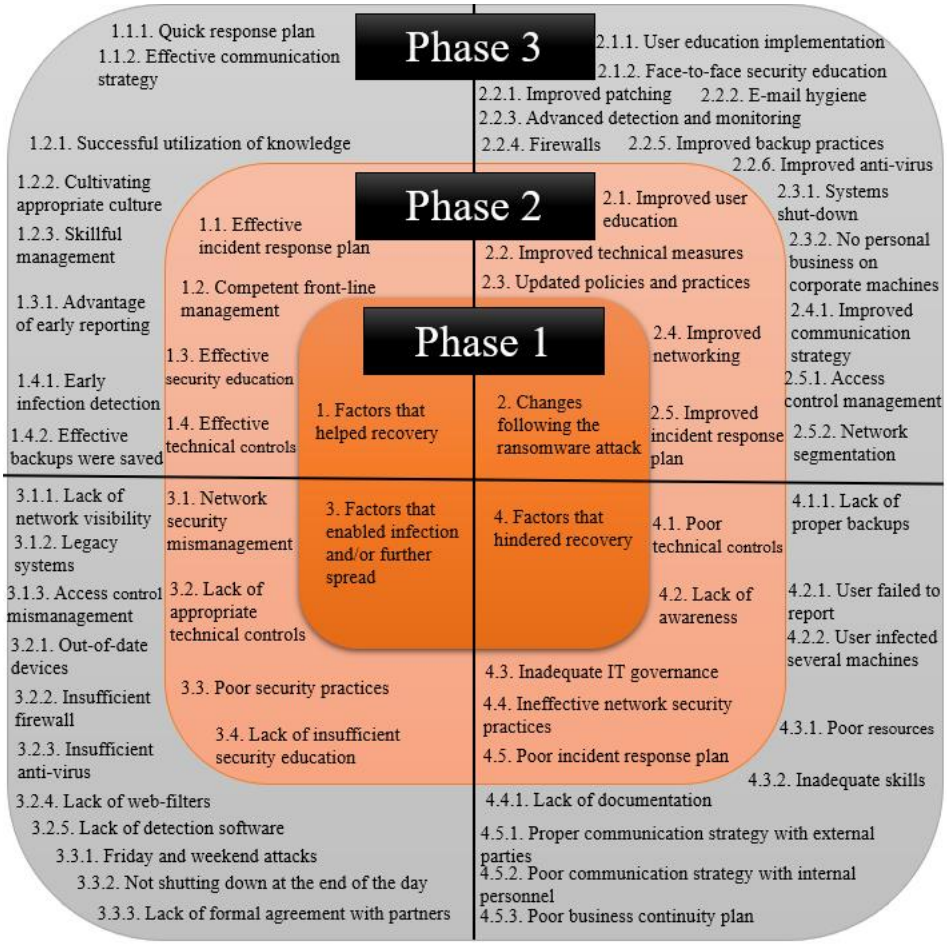

Fig. 1. The phases of analysis
Source: authors

The research targeted the speacilists' reaction during the cybercrime incidents and has 3 phases of analysis (Fig. 1). The paper classifies answers and obtained results of the ransomware attacks. The ransomware attack time horizon is from the years of 2014 until 2018. These ransomware attacks were structured by the types of crypto-ransomware. The aim is to find a balance between using specific humans or machine systems as initial targets. (Ivanyuk and Soloviev, 2019; Ivanyuk, 2018; Radosteva et al., 2018; Elizarov et al., 2017).

Furthermore, statistics on e-mail spam and phishing rates (Appendix) are used to confirm the thesis that they are both correlated in infecting computer systems with ransomware. It is noteworthy that the analysis of variance (ANOVA) in particular is used in order to find possible discrepencies and differences between the cases. The tables are used as samples and the discovery of variance. Whilst related methods, such as the *t-test are* similar, and can also be used, the decision to use the ANOVA specifically was made due to familiarity of the authors with it (An et al., 2019a; An et al., 2019b; An et al., 2019c; An et al., 2020a; An et al., 2020b; An et al., 2020c).

4. Results

As we have already reviewed, the behavior of people is incredibly important in situations regarding the prevention of infections in cyberspace and the successful reolvement of problems which may arise. The interview that was conducted is meant to understand what methods organizations utilize to keep their data and systems safe.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

The collected data shows that over half of victims are able to retrieve lost data using backups. This method, as described by the interviewees themselves, allowed them to avoid some damage caused by the attack, whilst simultaneously not succumbing to the criminals' demands. This has proven to be incredibly effective.

An aspect that had been vital to understanding the scale and consequences of ransomware infections is insurance. Figure 1 presents data on countries with cybersecurity insurance and contrasting insurance which covers ransomware attacks in 2019. This data directly parallels with the study's first stage of analysis titled "Factors that helped recovery" and the subsequent stages.

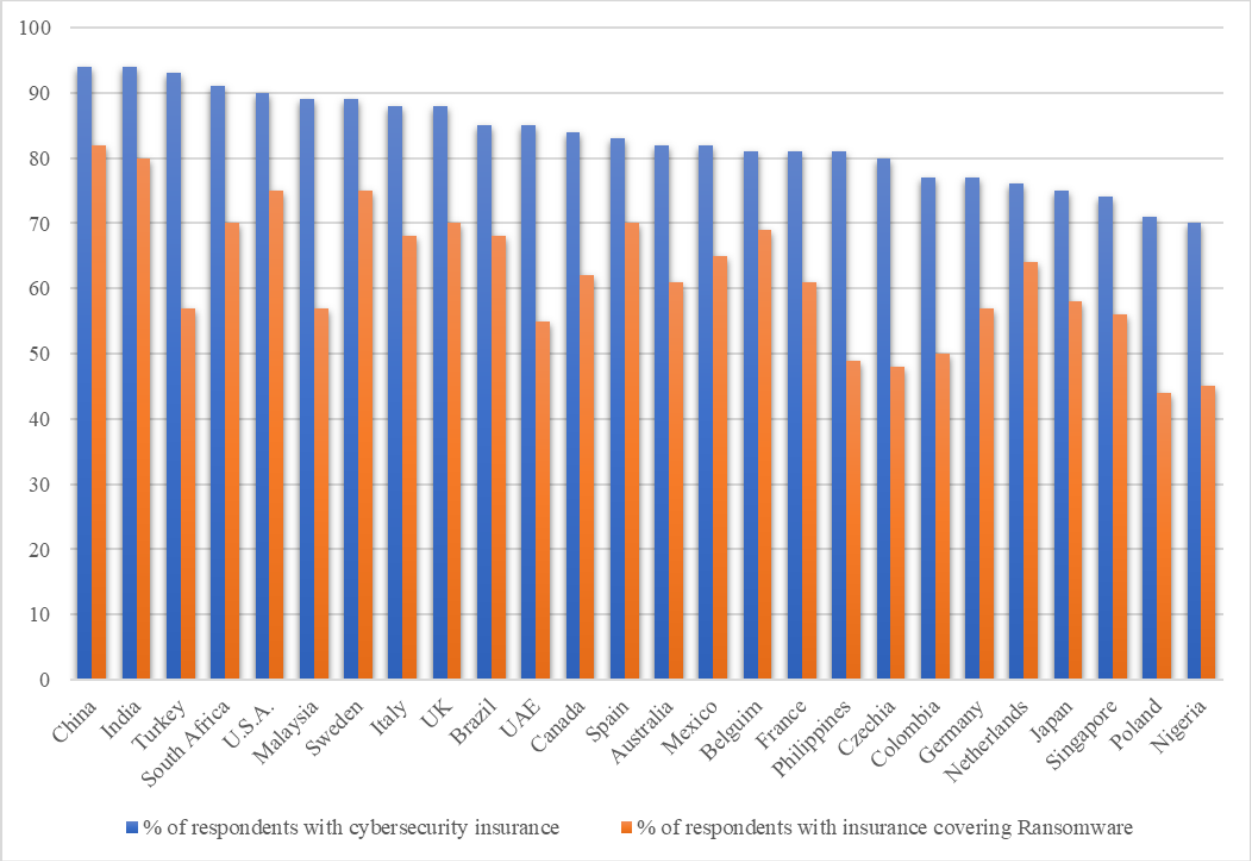

Fig. 2. Cybersecurity insurance by country in 2019.
Source: Sophos

As evident by the Figure, the choice of obtaining insurance that covers ransomware is inconsistent among the examined countries. Some countries decide to "go the extra mile" and also protect themselves from Ransomware. In order to understand the reason behind some countries' organizations valuing ransomware insurance more than others, the study observes the states in which ransomware attacks are more frequent (Figure 3).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

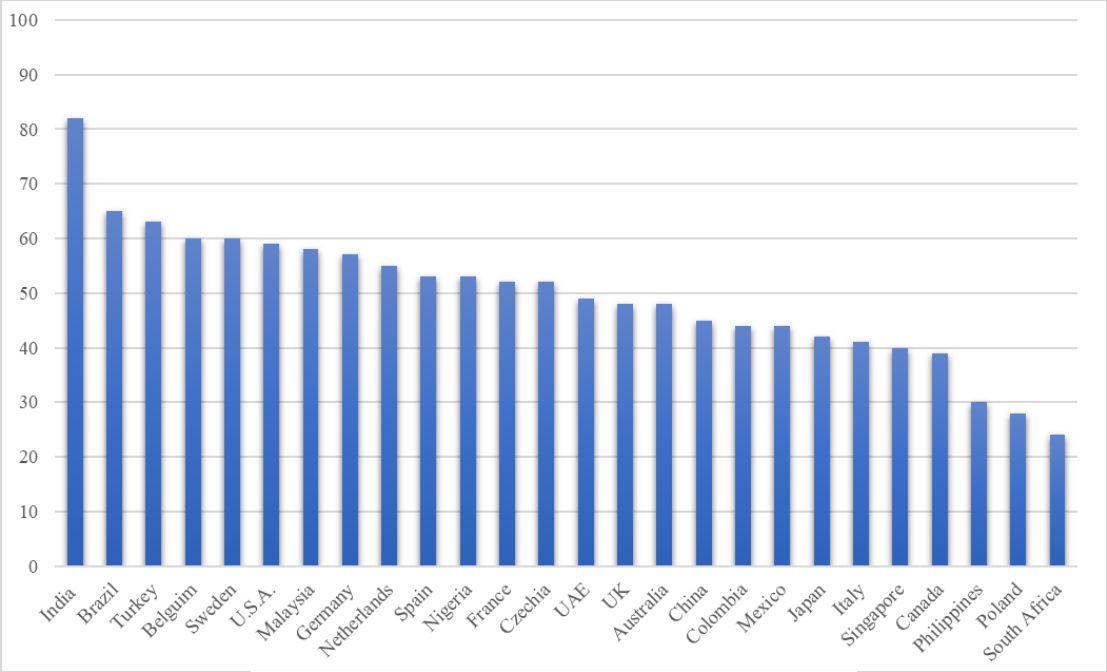

Fig. 3. Percentage of organizations hit by ransomware in 2019.
Source: Sophos

As you can see, India has been targetted most often, which explains the neccessity to buy not only cybersecurity insurance, but also that which protects from ransomware. Of curse, this may lead to subsequent problems, which is based on the ransom being paid (Figure 4).

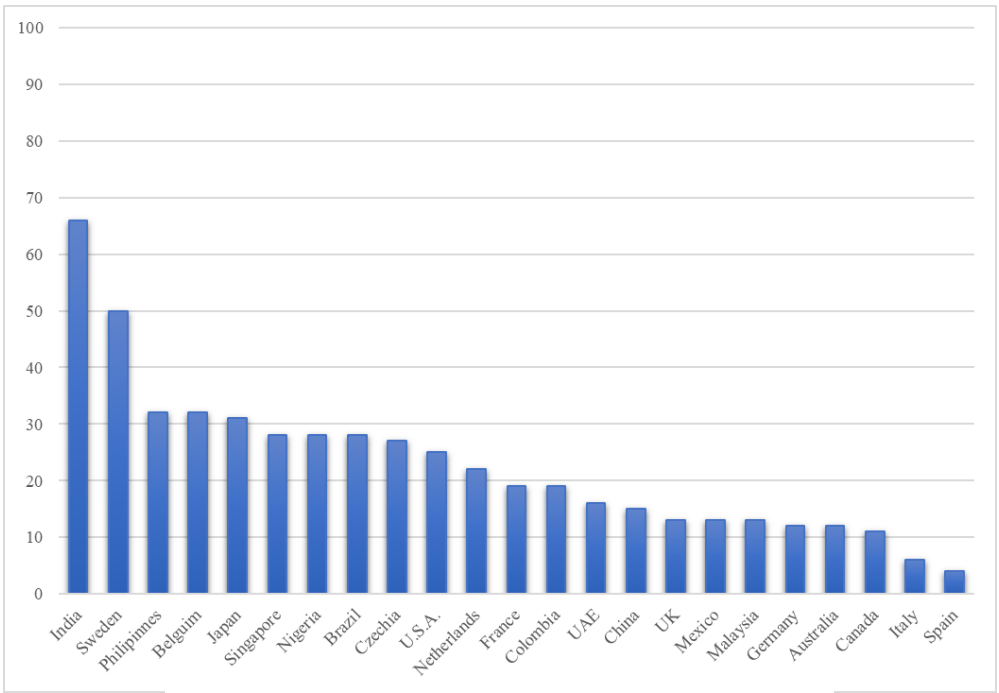

Fig. 4. Percentage of organizations that paid the ransomware in 2019.
Source: Sophos

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

It is not surprising that the country with the most intense insurance-policy pays the ransom far more often than many other states. This method of dealing with ransomware, as stated by our interviewees, proves to be effective, as almost every organization that was attacked by ransomware and paid the fee had the ransom paid by insurance. Subsequently, this often resulted in data and systems being unlocked.

The sums of money paid should also be put in perspective. The figure 5 below shows the average fee among ransomware infections contrasted with one of the most expensive types of ransomware – Ryuk. The key takeaway from this graph is that this volume of money ends up in the hands of criminals, that may use these new resources to continue harming other computer systems.

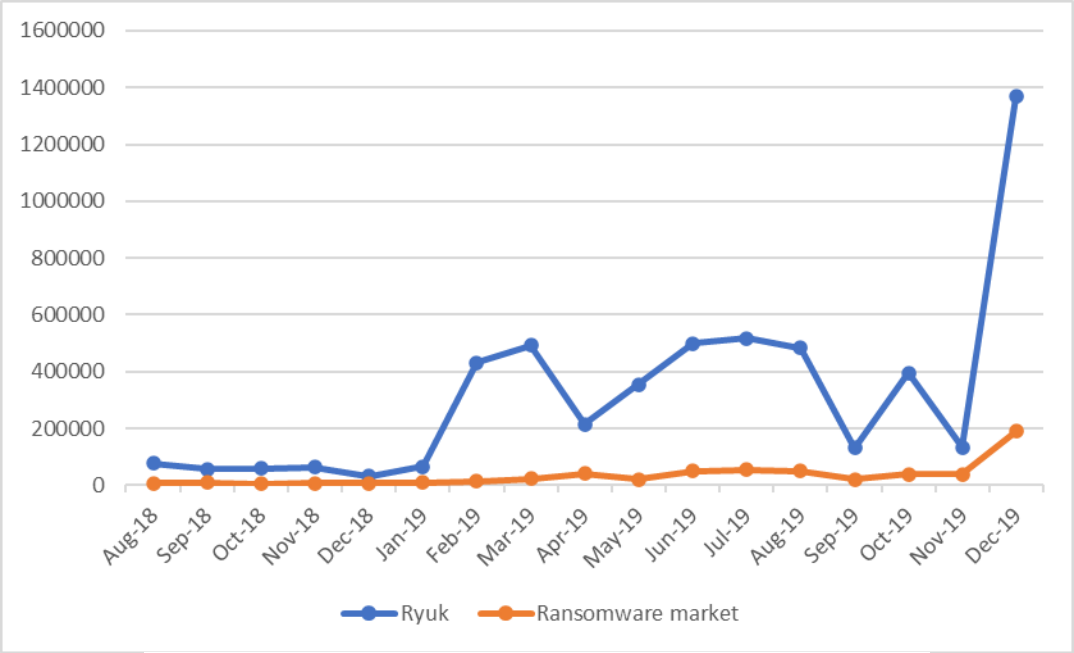

Fig. 5. Ransomware fee. Ryuk average fee and Ransomware average fee (USD$).
Source: Sophos

Regarding the ANOVA test, a strong correlation (F=10019) was found between email spam rate and email phishing rate (Table 2). These methods are both common, and thus users should be informed about the possible dangers of both methods in which hackers can take advantage of vulnerebilities in their systems. These results also parallel with the results of our interview, where most infections were said to happen through e-mail messengers.

Table 2. ANOVA summary

Data Summary			
	Samples		
	1	2	Total
N	45	45	90
ΣX	2455.3	2.5451	2457.8451

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

-Mean	54.5622	0.0566	27.3094
- ΣX^2	134553.45	0.3952	134553.8452
Variance	13.3369	0.0057	757.6584
Std.Dev.	3.652	0.0756	27.5256
Std.Err.	0.5444	0.0113	2.9015

standard weighted-means analysis

ANOVA Summary Independent Samples k=2

Source	SS	Df	MS	F	P
Treatment [between groups]	66844.518	1	66844.518	10019.67	<.0001
Error	587.077	88	6.6713		

Source: authors

5. Discussion

Commercial companies have given employees short seminars about these problems. There are programs for theoretical studies and practical experiences of law enforcement in big cities (Malecki, 2019; Yaqoob et al., 2017).

In rural areas and provinces, only a few law enforcements officers have specialized training in computer crime investigation. But this situation is slowly improving. Crime scene patrol officers are some of the most trained individuals in this area of expertise. They are first to produce and store (or destroy and approve the destruction of) valuable digital evidence. Ideally, all members of the justice system should receive basic information technology education and, better yet, the level of training that these officers have. However, this goal cannot be achieved in a short time period, but requires revamping the system of guides that are followed by officials (Mansfield-Devine, 2016).

As for the results of scientific methods used: businesses in particular are interested in ensuring the security of their data, documents and files, as the damages can be overwhelming. This has led to the development of different plans meant to resolve possible issues. Among them, as we have noted, is insurance along side file backup. Insurance is a form of "temporary solution", as the criminals are still able to gain their desired resources. Backups on the other hand, do not resolve the issue of "bricked" hardware, as it allows to replace previous systems with newer. However, this has the potential to save a business large funds compared to insurance or plainly paying the ransom. Moreover, insurance-paid ransom is not guaranteed to be unlocked – backups are more reliable in this situation.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

This brings us to arguably the most important point of the study – preventing ransomware attacks from happening in the first place. This is obviously the most beneficial situation, but it requires training and increased attention from users – a change in their behavior in cyberspace in general.

Users are capable to prevent thousands of dollars in damages if they simply add discipline, control, awareness to their browsing and Internet-surfing experience. This is the exact reason many organizations that have faced ransomware attacks intensify their programs to educate employees – as they, individuals, are also responsible for vulnerability exploitation (Ye et al., 2016).

6. Conclusion

Nowadays, very few organizations, governments and persons work and function without the use of gadgets, IT devices, computer systems. Because technology has integrated in to our lives as much as it has, it becomes progressively more important to invest in making cyberspace safe.

The study has reviewed how different methods of resolving the attack impacts the spread of ransomware across the Internet – be it insurance policy, backups or simply paying the ransom. Furthermore, the possible gateways to infection have been analyzed and examined. A strong connection between e-mail spam and phishing has been found, which reinforces these two methods of infection as one of the most common – making them essential to be learned in group seminars and courses about safety in cyberspace.

The research paper has also drawn results from interviewing persons with first-hand experience of facing ransomware attacks. These attacks emphasize vulnerabilities in the organization's computer system and can lead to permanent damage and file-loss. In the aftermath of the attack, organizations' and persons' weak spots are put on display, and they begin to take cybersecurity in a more serious manner, as it is an urgent manner – no one can know if they will be attacked today, tomorrow or in a month.

Despite paying much attention to ways that ransomware can be dealth with, this study values prevention tactics the most: making sure that infections do not occur in the first place. There are

This study, just as any other, has its limitations. For example, there are other common ways users can get infected with unwanted virii, such as visiting suspicious websites and downloading hazardous files and documents. these methods were reviewed, but were not researched in further detail. Furthermore, mobile users have been facing the issues of ransomware infections at an increasing alarming rate. This type of virus has become more common on gadgets and this should be a topic for future extensive research. There are numerous studies discussing machine learning methods of detecting ransomware, which is a topic that can be successfully utilizied by big corporations as well as governments.

7. Contribution to the body of knowledge

This paper summarizes the literature review on the growing problem of ransomware attacks across the world. The principals of infection have also been discussed and analyzed. Furthermore, the article emphasizes the causes and sources of users' vulnerability. It has evaluated that the industry of Information Technology has potential to become safer not only through means of regulation, but also by changing the mentality that people have when browsing the internet. The research paper has reported on actions to prevent the spread of ransomware can and should be done by all social institutions: governments, organizations and households. Governments have numerous levers to not only detect attacks and resolve issues, but bring criminals to justice. The state has a monopoly on this, as no other institution, be it a business or individual person, can "get revenge" for the damages. In order to do this, laws must be passed to build a legislative base for counteracting cybercrime and punishments

for misdemeanors. Furthermore, governments have the opportunity to cooperate on and international level to ensure a level playing field all over the globe.

References:

Al-rimy, B. A. S., Maarof, M. A., Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. − Computers & Security 74: 144-166. https://doi.org/10.1016/j.cose.2018.01.001

Alwaelya, S.A., Yousif N.B.A., Mikhaylov A. (2020). Emotional Development in Preschoolers and Socialization. Early child development and care, 190(6). https://doi.org/10.1080/03004430.2020.1717480

An, J., Dorofeev, M. (2019). Short-term FX forecasting: decision making on the base of expert polls. Investment Management and Financial Innovations, 16(4), 72-85. https://doi.org/10.21511/imfi.16(4).2019.07

An, J., Dorofeev, M., Zhu, S. (2020c). Development of Energy Cooperation Between Russia and China. International Journal of Energy Economics and Policy, 10(1), 134-139.

An, J., Mikhaylov, A., Jung, S.-U. (2020b). The Strategy of South Korea in the Global Oil Market. Energies, 13(10), 2491; https://doi.org/10.3390/en13102491

An, J., Mikhaylov, A., Kim, K. (2020a). Machine Learning Approach in Heterogeneous Group of Algorithms for Transport Safety-Critical System. Applied Sciences, 10(8), 2670; https://doi.org/10.3390/app10082670

An, J., Mikhaylov, A., Moiseev, N. (2019c). Oil Price Predictors: Machine Learning Approach. International Journal of Energy Economics and Policy, 9(5), 1-6. https://doi.org/10.32479/ijeep.7597

An, J., Mikhaylov, A., Sokolinskaya, N. (2019a). Machine learning in economic planning: ensembles of algorithms. Journal of Physics: Conference Series, 1353, 012126 https://doi.org/10.1088/1742-6596/1353/1/012126

An, J., Mikhaylov, A., Sokolinskaya, N. (2019b). Oil incomes spending in sovereign fund of Norway (GPFG). Investment Management and Financial Innovations, 16(3), 10-17. https://doi.org/10.21511/imfi.16(3).2019.02

Aurangzeb, S., Aleem, M., Iqbal, M. A., Islam, M. A. (2017). Ransomware: a survey and trends. Computer Fraud & Security, 6(2), 48-58. https://doi.org/10.1016/S1361-3723(17)30089-1

Bešinović, N., Goverde, R.M.P. (2019), Stable and robust train routing in station areas with balanced infrastructure capacity occupation. Public Transport, 11(2), 211-236. https://doi.org/10.1007/s12469-019-00202-3

Bhardwaj, A., Avasthi, V., Sastry, H., Subrahmanyam, G. V. B. (2016). Ransomware digital extortion: a rising new age threat. Indian Journal of Science and Technology 9(14), 1-5. https://www.researchgate.net/profile/Hanumat_Sastry/publication/286301708_Ransomware_A_Rising_Threat_of_new_age_Digital_Extortion/links/5763ae5908ae9964a16badd0/Ransomware-A-Rising-Threat-of-new-age-Digital-Extortion

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), 5-9. dhttps://doi.org/10.1016/S1353-4858(16)30086-1

Candelieri, A., Galuzzi, B.G., Giordani, I., Archetti, F. (2019), Vulnerability of public transportation networks against directed attacks and cascading failures. Public Transport, 11(1), 27-49. https://doi.org/10.1007/s12469-018-00193-7

Chiabaut, N., Barcet, A. (2019). Demonstration and evaluation of an intermittent bus lane strategy. Public Transport, 11(3), 443-456. https://doi.org/10.1007/s12469-019-00210-3

Chung, M. (2019). Why employees matter in the fight against ransomware. Computer Fraud & Security 2019(8), 8-11. https://doi.org/10.1016/S1361-3723(19)30084-3

Connolly, L. Y., Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security 87: 101568. https://doi.org/10.1016/j.cose.2019.101568
Covic, F., Voß, S. (2019), Interoperable smart card data management in public mass transit. Public Transport, 11(3), 523-548. https://doi.org/10.1007/s12469-019-00216-x

Czioska, P., Kutadinata, R., Trifunović, A., Winter, S., Sester, M., Friedrich, B. (2019), Real-world meeting points for shared demand-responsive transportation systems. Public Transport, 11(2), 341-377. https://doi.org/10.1007/s12469-019-00207-y

Dayong, N, Mikhaylov, A, Bratanovsky, S, Shaikh, Z.A., Stepanova, D. (2020). Mathematical modeling of the technological processes of catering products production. Journal of Food Process Engineering, 43(2). https://doi.org/10.1111/jfpe.13340

Denisova, V., Mikhaylov, A., Lopatin, E. (2019). Blockchain Infrastructure and Growth of Global Power Consumption. International Journal of Energy Economics and Policy, 9(4), 22-29. https://doi.org/10.32479/ijeep.7685

Dooyum, U.D., Mikhaylov, A., Varyash, I. (2020). Energy Security Concept in Russia and South Korea. International Journal of Energy Economics and Policy, 10(4), 102-107. https://doi.org/10.32479/ijeep.9116

Dorantes-Argandar, G., Rivera-Vázquez, E.Y., Cárdenas-Espinoza, K.M. (2019), Measuring situations that stress public bus users in Mexico: a case study of Cuernavaca, Morelos. Public Transport, 11(3), 577-587. https://doi.org/10.1007/s12469-019-00215-y

Downward, A., Chowdhury, S., Jayalath, C. (2019), An investigation of route-choice in integrated public transport networks by risk-averse users. Public Transport, 11(1), 89-110. https://doi.org/10.1007/s12469-019-00194-0

Elizarov, M., Ivanyuk, V., Soloviev, V., Tsvirkun, A. (2017). Identification of high-frequency traders using fuzzy logic methods. Proceedings of 2017 10th International Conference Management of Large-Scale System Development, MLSD 2017. https://doi.org/10.1109/MLSD.2017.8109615

Enayatollahi, F., Idris, A.O., Atashgah, M.A.A. (2019), Modelling bus bunching under variable transit demand using cellular automata. Public Transport, 11(2), 269-298. https://doi.org/10.1007/s12469-019-00203-2

Everett, C. (2016). Ransomware: to pay or not to pay?.Computer Fraud & Security 2016(4), 8-12. https://doi.org/10.1016/S1361-3723(16)30036-7

Fagioli, A. (2019). Zero-day recovery: the key to mitigating the ransomware threat. Computer Fraud & Security 2019(1), 6-9. https://doi.org/10.1016/S1361-3723(19)30006-5

Furnell, S., Emm, D. (2017). The ABC of ransomware protection. Computer Fraud & Security 2017(10): 5-11. https://doi.org/10.1016/S1361-3723(17)30089-1

Genç, Z. A., Lenzini, G., Ryan, P. Y. (2018). Next generation cryptographic ransomware. Nordic Conference on Secure IT Systems 385-401. http://158.64.76.181/bitstream/10993/37569/1/next_gen_rw.pdf

Gonzalez, D., Hayajneh, T. (2017). Detection and prevention of crypto-ransomware. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) 472-478. https://doi.org/10.1109/UEMCON.2017.8249052

Gordon, S., Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20. https://doi.org/10.1007/s11416-006-0015-z

Gura, D., Mikhaylov, A., Glushkov, S., Zaikov, M., Shaikh Z.A. (2020). Model for estimating power dissipation along the interconnect length in single on-chip topology. Evolutionary Intelligence. https://doi.org/10.1007/s12065-020-00407-7

Habib, K.N., Hasnine, S. (2019), An econometric investigation of the influence of transit passes on transit users' behavior in Toronto. Public Transport, 11(1), 111-133. https://doi.org/10.1007/s12469-019-00195-z

Hadiuzzaman, M., Malik, D.M.G., Barua, S., Qiu, T.Z., Kim, A. (2019), Modeling passengers' perceptions of intercity train service quality for regular and special days. Public Transport, 11(3), 549-576. https://doi.org/10.1007/s12469-019-00213-0

Heyken Soares, P., Mumford, C.L., Amponsah, K., Mao, Y. (2019), An adaptive scaled network for public transport route optimization. Public Transport, 11(2), 379-412. https://doi.org/10.1007/s12469-019-00208-x

Huang, W., Shuai, B., Antwi, E. (2019), A two-stage optimization approach for subscription bus services network design: the China case. Public Transport, 11(3), 589-616. https://doi.org/10.1007/s12469-018-0182-6

Iliopoulou, C., Kepaptsoglou, K., Vlahogianni, E. (2019). Metaheuristics for the transit route network design problem: a review and comparative analysis. Public Transport, 11(3), 487-521. https://doi.org/10.1007/s12469-019-00211-2

ISTR (2019). Internet Security Threat Report, Volume 24, February 2019 http://book.itep.ru/depository/security/surveys/ISTR_24_2019_en.pdf.

Ivanyuk, V. (2018).Econometric Forecasting Models Based on Forecast Combination Methods. Proceedings of 2018 11th International Conference Management of Large-Scale System Development, MLSD 2018. https://doi.org/10.1109/MLSD.2018.8551825

Ivanyuk, V., Soloviev, V. (2019). Efficiency of neural networks in forecasting problems. Proceedings of 2019 12th International Conference Management of Large-Scale System Development; MLSD 2019. https://doi.org/10.1109/MLSD.2019.8911046

Jasti, P.C., Ram, V.V. (2019), Sustainable benchmarking of a public transport system using analytic hierarchy process and fuzzy logic: a case study of Hyderabad, India. Public Transport, 11(3), 457-485. https://doi.org/10.1007/s12469-019-00219-8

Jevinger, Å., Persson, J.A. (2019), Exploring the potential of using real-time traveler data in public transport disturbance management. Public Transport, 11(2), 413-441. https://doi.org/10.1007/s12469-019-00209-w

Kolodenker, E., Koch, W., Stringhini, G., Egele, M. (2017). Paybreak: Defense against cryptographic ransomware. − Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security 599-611. http://dx:doi:org/10:1145/3052973:3053035

Kurpjuhn, T. (2019). The guide to ransomware: how businesses can manage the evolving threat. Computer Fraud & Security 2019(11), 14-16. https://doi.org/10.1016/S1361-3723(19)30117-4

Lopatin, E. (2019). Assessment of Russian banking system performance and sustainability. Banks and Bank Systems, 14(3), 202-211. https://doi.org/10.21511/bbs.14(3).2019.17

Lopatin, E. (2020). Cost of Heating Pump Systems in Russia. International Journal of Energy Economics and Policy, 10(3). https://doi.org/10.32479/ijeep.9056

Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. Computer Fraud & Security 2019(3), 8-10. https://doi.org/10.1016/S1361-3723(19)30028-4

Malucelli, F., Tresoldi, E. (2019), Delay and disruption management in local public transportation via real-time vehicle and crew re-scheduling: a case study. Public Transport, 11(1). https://doi.org/10.1007/s12469-019-00196-y

Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. − Network Security 2016(10), 8-17. https://doi.org/10.1016/S1353-4858(16)30096-4

Mercaldo, F., Nardone, V., Santone, A. (2016). Ransomware inside out. − In 2016 11th International Conference on Availability, Reliability and Security (ARES) 628-637. https://doi.org10.1109/ARES.2016.35

Meynkhard, A. (2019). Energy Efficient Development Model for Regions of the Russian Federation: Evidence of Crypto Mining. International Journal of Energy Economics and Policy, 9(4), 16-21. https://doi.org/10.32479/ijeep.7759

Meynkhard, A. (2020a). Long-term prospects for the development energy complex of Russia. International Journal of Energy Economics and Policy, 10(3), c. 224-232.

Meynkhard, A. (2020b). Priorities of Russian Energy Policy in Russian-Chinese Relations. International Journal of Energy Economics and Policy, 10(1), 65-71. https://doi.org/10.32479/ijeep.8507

Mikhaylov A, Tarakanov, S. (2020). Development of Levenberg-Marquardt theoretical approach for electric network. Journal of Physics: Conference Series, 1515, 052006 https://doi.org/10.1088/1742-6596/1515/5/052006

Mikhaylov A., Danish M.S.S., Senjyu T. (2020). New stage in evolution of cryptocurrency market: analysis by Hurst method. In S. Yuksel and H. Dincer (Ed.), Strategic Outlook in Business and Finance Innovation: Multidimensional Policies for Emerging Economies (pp. 14-16). London, United Kingdom: Emerald.

Mikhaylov, A, Sokolinskaya, N. (2019). Russian banks after sanctions of 2014. Orbis, 15(44), 55-65. http://www.revistaorbis.org.ve/pdf/44/art5.pdf

Mikhaylov, A. (2018a). Pricing in Oil Market and Using Probit Model for Analysis of Stock Market Effects. International Journal of Energy Economics and Policy, 8(2), 69-73. https://www.econjournals.com/index.php/ijeep/article/view/5846

Mikhaylov, A. (2018b). Volatility Spillover Effect between Stock and Exchange Rate in Oil Exporting Countries. International Journal of Energy Economics and Policy, 8(3), 321-326. https://www.econjournals.com/index.php/ijeep/article/view/6307

Mikhaylov, A. (2019). Oil and Gas Budget Revenues in Russia after Crisis in 2015. International Journal of Energy Economics and Policy, 9(2), 375-380. https://doi.org/10.32479/ijeep.6635

Mikhaylov, A. (2020a). Geothermal Energy Development in Iceland. International Journal of Energy Economics and Policy, 2020, 10(4), 31-35. https://doi.org/10.32479/ijeep.9047

Mikhaylov, A. (2020b). Lichens as indicators of atmospheric pollution in urban ecosystems. Israel Journal of Ecology & Evolution, 10016, 1-9. http://dx.doi.org/10.1163/22244662-bja10016

Mikhaylov, A., Moiseev, N., Aleshin, K., Burkhardt, T. (2020). Global climate change and greenhouse effect. Entrepreneurship and Sustainability Issues, 7(4), 2897-2913. http://doi.org/10.9770/jesi.2020.7.4(21)

Mikhaylov, A., Sokolinskay, N., Lopatin, E. (2019). Asset allocation in equity, fixed-income and cryptocurrency on the base of individual risk sentiment. Investment Management and Financial Innovations, 16(2), 171-181. https://doi.org/10.21511/imfi.16(2).2019.15

Mikhaylov, A., Sokolinskaya, N., Nyangarika, A. (2018) Optimal Carry Trade Strategy Based on Currencies of Energy and Developed Economies. Journal of Reviews on Global Economics, 7, 582-592. https://doi.org/10.6000/1929-7092.2018.07.54

Mohri, S.S., Akbarzadeh, M. (2019), Locating key stations of a metro network using bi-objective programming: discrete and continuous demand mode. Public Transport, 11(2), 321-340. https://doi.org/10.1007/s12469-019-00205-0

Mohurle, S., Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. – International Journal of Advanced Research in Computer Science 8(5). https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Moiseev, N., Mikhaylov, A., Varyash, I., Saqib, A. (2020). Investigating the relation of GDP per capita and corruption index. Entrepreneurship and Sustainability Issues, 8(1), 780-794. http://doi.org/10.9770/jesi.2020.8.1(52)

Nguyen, P., Diab, E., Shalaby, A. (2019), Understanding the factors that influence the probability and time to streetcar bunching incidents. Public Transport, 11(2), 299-320. https://doi.org/10.1007/s12469-019-00201-4

Nie, D., Panfilova, E., Samusenkov, V., Mikhaylov, A. (2020) E-Learning Financing Models in Russia for Sustainable Development. Sustainability, 12(11), 4412. https://doi.org/10.3390/su12114412

Nyangarika, A., Mikhaylov, A., Richter, U. (2019b). Oil Price Factors: Forecasting on the Base of Modified Auto-regressive Integrated Moving Average Model. International Journal of Energy Economics and Policy, 9(1), 149-160. https://doi.org/10.32479/ijeep.6812

Nyangarika, A., Mikhaylov, A., Tang, B.-J. (2018). Correlation of Oil Prices and Gross Domestic Product in Oil Producing Countries. International Journal of Energy Economics and Policy, 8(5), 42-48. Retrieved from https://www.econjournals.com/index.php/ijeep/article/view/6802

Nyangarika, A., Mikhaylov, A., Richter, U. (2019a). Influence Oil Price towards Economic Indicators in Russia. International Journal of Energy Economics and Policy, 9(1), 123-129. https://doi.org/10.32479/ijeep.7597

O'Kane, P., Sezer, S., Carlin, D. (2018). Evolution of ransomware. − IET Networks 7(5): 321-327. https://doi.org/10.1049/iet-net.2017.0207

Paquet-Clouston, M., Haslhofer, B., Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. Journal of Cybersecurity 5(1). https://doi.org/10.1093/cybsec/tyz003

Plėta, T., Tvaronavičienė, M., Della Casa, S., Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 2(3), 703-715. https://doi.org/10.9770/IRD.2020.2.3(7)

Pope, J. (2016). Ransomware: minimizing the risks. − Innovations in clinical neuroscience 13(11-12), 37. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/

Prosekov S., Danish M.S.S., Senjyu T. (2020). Long-Term Memory Models for Predicting Dynamics of Cryptocurrencies. In S. Yuksel and H. Dincer (Ed.), Strategic Outlook in Business and Finance Innovation: Multidimensional Policies for Emerging Economies (pp. 24-34). London, United Kingdom: Emerald.

Radosteva, M., Soloviev, V., Ivanyuk, V., Tsvirkun, A.(2018). Use of neural network models in market risk management. Advances in Systems Science and Applications, 18(2), 53-58. https://doi.org/10.25728/assa.2018.18.2.582

Sun, B., Apland, J. (2019), Operational planning of public transit with economic and environmental goals: application to the Minneapolis–St. Paul bus system. Public Transport, 11(2), 237-267. https://doi.org/10.1007/s12469-019-00199-9

Sunchalin, A.M., Kochkarov, R.A., Levchenko, K.G., Kochkarov, A.A., Ivanyuk, V.A. (2019). Methods of risk management in portfolio theory. Espacios, 40(16), 8 p.

Szlosarek, R., Yan, C., Kröger, M., Nußbaumer, C. (2019), Energy efficiency of ropeways: a model-based analysis. Public Transport, 11(3), 617-635. https://doi.org/10.1007/s12469-019-00212-1

Varyash, I., Mikhaylov, A., Moiseev, N., Aleshin, K. (2020). Triple bottom line and corporate social responsibility performance indicators for Russian companies. Entrepreneurship and Sustainability Issues, 8(1), 313-331. http://doi.org/10.9770/jesi.2020.8.1(22

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks 129, 444-458. https://doi.org/10.1016/j.comnet.2017.09.003
Ye, H., Dai, W., Huang, X. (2016). U.S. Patent No. 9,317,686. Washington, DC: U.S. Patent and Trademark Office. https://patentimages.storage.googleapis.com/2b/e0/d3/7ac0a4bd166bff/US9317686.pdf

Yumashev, A., Ślusarczyk, B., Kondrashev, S., Mikhaylov, A. (2020). Global Indicators of Sustainable Development: Evaluation of the Influence of the Human Development Index on Consumption and Quality of Energy. Energies, 13, 2768. https://doi.org/10.3390/en1311276

Yumashev, A., Mikhaylov, A. (2020) Development of Polymer Film Coatings with High Adhesion to Steel Alloys and High Wear Resistance. Polymer Composites, 41(7), 2875-2880. https://doi.org/10.1002/pc.25583

Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., Sangaiah, A. K. (2019). Classification of ransomware families with machine learning based on N-gram of opcodes. Future Generation Computer Systems, 90, 211-221. https://doi.org/10.1016/j.future.2018.07.052

Zimba, A., Wang, Z., Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. Ict Express, 4(1), 14-18. https://doi.org/10.1016/j.icte.2017.12.007

Appendix

Answer classification of analysis' phases.

1.1.1.1 we responded methodically	3.1.3.7 scanning vulnerable IPs on Internet is simple
1.1.1.2 processes were documented in the incident response plan	3.1.3.8 vulnerable Internet facing servers
	3.1.3.2 we voluntary enabled RDP
1.1.2.1 we handled media invasion very well	3.1.3.3 RDP brute-force due to weak password
1.1.2.2 we were able to inform staff immediately	3.1.3.4 RDP system is not brilliant
1.2.1.1 breach coach helped enormously with recovery	3.1.3.5 Microsoft ignored our RDP concerns
1.2.1.2 cyber insurance provided information we needed	3.1.4.1 escalated privileges
1.2.1.3 cyber insurance reimbursed many expenses	3.1.4.2 poor management of admin passwords

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

1.2.1.4 security vendor was helpful	3.1.4.3 infected domain controller
1.2.1.5 cyber experts are needed to find patient zero	3.1.4.4 disregard for proper network structures
1.2.1.6 IT contractors worked very hard	3.1.4.5 root access
1.2.1.7 IT contractor decrypted scrambled data	3.2.1.1 ransomware came in via vulnerable server
1.2.1.8 internal staff is the key to successful recovery	3.2.1.2 some of our servers were very old
1.2.2.1 timely reporting led to fast reaction to the threat	3.2.1.3 out-of-date software
1.2.2.2 it is important to let people know what is happening	3.2.1.4 SMB vulnerability
1.2.2.3 people were compassionate and determined	3.2.1.5 out-of-date Flash
1.2.2.4 despite of challenging conditions, people were amazing	3.2.2.1 low-level protection firewall
1.2.3.1 security-savvy IT manager	3.2.3.1 new malware signature
1.2.3.2 knowing what to expect helps	3.2.3.2 out-of-date anti-virus
1.2.3.3 prior experience with ransomware attacks helps	3.2.3.3 drive-by-download
1.3.1.1 early reporting gave us advantage of time	3.2.4.1 infection came through browsing Internet
1.4.1.1 we had sophisticate detection software	3.2.5.1 ransomware stayed undetectable for days
1.4.1.2 anti-virus was up-to-date	3.3.5.1 signs ‘please do not turn computer on’
1.4.2.1 we frequently test backups	3.3.5.2 Friday ransomware attacks
1.4.2.2 our offline backups saved us	3.4.1.1 aging employee
2.2.1.1 centrally-managed vulnerability management	3.4.1.2 apathy
2.2.1.2 scheduled vulnerability management	3.4.1.3 you are as vulnerable as your least savvy user
2.2.1.3 removing Flash	3.4.1.4 convincing email
2.2.1.4 business applications update	3.4.1.5 well-crafted email
2.2.2.1 blocking certain attachments and links	3.4.1.6 it starts with user
2.2.2.2 email identification	4.1.1.1 a lot of critical systems did not have backups
2.2.2.3 malicious code analysis platform	4.1.1.2 Time Machine was encrypted
2.2.3.1 centrally-controlled upgrades	4.1.1.3 backups got deleted by ransomware
2.2.3.2 upgrading legacy systems	4.1.1.4 backups were not particularly clever
2.2.3.3 OS upgrade	4.1.1.5 insufficient backups forced us to pay
2.2.4.1 implementation of detection system	4.1.1.6 servers were not affected, only desktops and laptops
2.2.4.2 monitoring software	4..1.1.7 backup software was only grabbing chunks of files
2.2.5.1 advanced protection firewall	4.1.1.8 sensitive information was encrypted
2.2.5.2 securely-configured firewall	4.1.1.9 too many nodes got encrypted
2.2.6.1 testing backups	4.1.1.10 IT provider failed to ensure efficient backups
2.2.6.2 offline backups	4.1.1.11 networked backups
2.2.7.1 higher protection anti-virus	4.3.1.1 lack of proper funding
2.4.1.1 considering loss of IT	4.3.1.2 IT team is absolutely tiny
2.4.1.2 informing staff via text messages	4.3.1.3 too many servers for such small IT team
2.5.1.1 applications roles and responsibilities	4.3.2.1 inappropriate background leading to poor governance
2.5.1.2 least privileges approach	4.3.2.2 senior management incompetence led to further infections
2.5.2.1 retiring old machines	4.3.2.3 not understanding the importance of IT
2.5.5.1 disabling RDP	4.3.2.4 senior management should have been more involved
2.5.5.2 robust VPN to replace RDP	4.3.2.5 underappreciation of IT
3.1.1.1 we do not know who connects to network	4.5.1.1 phone calls from other organisation caused disruption
3.1.1.2 we do not know amount of ransom notes received	4.5.1.2 media invasion
3.1.1.3 no control over upgrading/updating OS	4.5.1.3 security vendors invasion
3.1.1.4 it was like a fog when we got infected	4.5.2.1 we did not realise email will be down
3.1.2.1 legacy systems could not be upgraded	4.5.2.2 we did not have mobile phones of senior management
3.1.2.2 legacy systems could not be retired	4.5.2.3 no one thought of IT resources being unavailable
3.1.3.1 we do not know who connects via RDP	4.5.3.1 we did not know how to do both investigation and recovery
3.1.3.6 RDP enabled by default	

Source: author

Ransomware mail spam rate by country.

Email spam	%
Saudi Arabia	66,8
China	62,2

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

Brazil	60,8
Sri Lanka	60,6
Norway	59,1
Oman	58,6
Sweden	58,3
Mexico	58,1
UAE	58,1
USA	57,5
Colombia	56,8
Belgium	56,2
Serbia	55,8
Singapore	55,4
UK	54,8
Germany	54,8
Taiwan	54,5
Austria	54,4
Finland	54,4
Hungary	54,4
Greece	54,2
Israel	54,1
Denmark	54,1
France	54
Netherlands	53,9
Australia	53,9
New Zealand	53,4
Canada	53,4
Italy	53,4
Poland	53,2
Spain	52,9
Qatar	52,6
South Korea	52,4
Portugal	52,1
Luxembourg	51,4
Malaysia	51,4
Thailand	51,1
Ireland	51
India	50,9
South Africa	50,8

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

Switzerland	50,8
Hong Kong	50,5
Papua New Guinea	50
Philippines	49,5
Japan	48,7

Source: ISTR (2019).

Ransomware mail phishing rate by country.

Email spam	%
Saudi Arabia	66,8
China	62,2
Brazil	60,8
Sri Lanka	60,6
Norway	59,1
Oman	58,6
Sweden	58,3
Mexico	58,1
UAE	58,1
USA	57,5
Colombia	56,8
Belgium	56,2
Serbia	55,8
Singapore	55,4
UK	54,8
Germany	54,8
Taiwan	54,5
Austria	54,4
Finland	54,4
Hungary	54,4
Greece	54,2
Israel	54,1
Denmark	54,1
France	54
Netherlands	53,9
Australia	53,9
New Zealand	53,4
Canada	53,4
Italy	53,4
Poland	53,2

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

Spain	52,9
Qatar	52,6
South Korea	52,4
Portugal	52,1
Luxembourg	51,4
Malaysia	51,4
Thailand	51,1
Ireland	51
India	50,9
South Afrika	50,8
Switzerland	50,8
Hong Kong	50,5
Papua New Guinea	50
Philippines	49,5
Japan	48,7

Source: ISTR (2019).

Mafura UANDYKOVA is currently Accociate Professor at Narxoz University, Kazakhstan. She is an author of 3 scientific publications and conference papers indexed in SCOPUS and Web of Science. She has extensive research work addressing challenging in System modeling in the development of a model of scenario control of the regional innovative development level. Her Research Interest Areas: Business, Management and Accounting Decision Sciences Economics, Econometrics and Finance Agricultural and Biological Sciences Computer Science Veterinary.
ORCID ID: https://orcid.org/0000-0001-5229-335X

Anton LISIN is Laboratory assistant of the Department of Financial Markets and Banks (2019) in the Financial University under the Government of the Russian Federation. He is the author of several articles that have been published by journals indexed in SCOPUS, addressing topics, such as economic relations, policy and energy potential. Main scientific interests are: energy, resource conservation, region, energy-efficient development, energy indicators, modeling, forecasting, strategic planning, independence of network operation.
ORCID ID: https://orcid.org/0000-0002-8708-132X

Diana STEPANOVA is Associate Professor of the Department of Finance and Prices, a leading researcher at the Plekhanov Russian University of Economics, Moscow, Russia. She is the author of more than 50 scientific papers and conference materials indexed in Russian and international scientific databases (more than 20 SCOPUS and WoS articles in total) on problems of Economics and Finance both at the macro level and at the level of individual industries and companies. She teaches the cources: Finance, Global financial markets, Foreign exchange market, Company credit policy, International finance, International financial market, Pricing, Financial markets and financial instruments, International pricing.
ORCID ID: https://orcid.org/0000-0001-5981-6889

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 8 Number 2 (December)
http://doi.org/10.9770/jesi.2020.8.2(47)

Laura BAITENOVA is currently Accociate Professor at Narxoz University, Kazakhstan. She is an author of sevaral scientific publications and conference papers indexed in SCOPUS and Web of Science. She has extensive research work addressing challenging in analysis and forecast of the main trends of world economy, foreign sector of the Russian economy; analysis of the country's balance of payments; competitiveness of the national economy; macroeconomic forecasting. Her Research Interest Areas: Business, Management and Accounting Decision Sciences Economics, Econometrics and Finance Agricultural and Biological Sciences Computer Science Veterinary.
ORCID ID: https://orcid.org/0000-0002-1591-2235

Lyailya MUTALIYEVA is currently Accociate Professor at L. N. Gumilyov Eurasian National University, Kazakhstan. She is an author of sevaral scientific publications and conference papers indexed in SCOPUS and Web of Science. She has extensive research work addressing challenging in analysis and forecast of the main trends of world economy, foreign sector of the Russian economy; analysis of the country's balance of payments; competitiveness of the national economy; macroeconomic forecasting. Her Research Interest Areas: Business, Management and Accounting Decision Sciences Economics, Econometrics and Finance Agricultural and Biological Sciences Computer Science Veterinary.
ORCID ID: https://orcid.org/0000-0002-9681-1515

Serhat YUKSEL is currently an Associate Professor at Istanbul Medipol University, Turkey. He is an author of 53 scientific publications and conference papers indexed in SCOPUS and Web of Science and author of several scientific monographs. He has extensive research work addressing challenging in the Field of Econometric Modeling, Climate Policy & Climate Change, Energy, and Finance. His Research Interest Areas: energy efficiency, renewable energy investment projects, energy policy, energy economics, energy consumption, fuzzy logic, multi-criteria decision-making models.
ORCID ID: https://orcid.org/0000-0002-9858-1266

Hasan DINCER is currently Full Professor at Istanbul Medipol University, Turkey. He is an author of more than 100 scientific publications and conference papers indexed in SCOPUS and Web of Science. He has extensive research work addressing challenging in the Field of Econometric Modeling, Climate Policy & Climate Change, Energy, and Finance. His Research Interest Areas: energy efficiency, renewable energy investment projects, energy policy, energy economics, energy consumption, fuzzy logic, multi-criteria decision-making models, regional economics, macroeconomic stability, economic equality, energy policy, renewable energy investment projects.
ORCID ID: https://orcid.org/0000-0002-8072-031X