The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: September 29, 2020 | **Pages:** 62-66
Doi: https://doi.org/10.37547/tajpslc/Volume02Issue09-11

IMPACT FACTOR
2020: 5. 453

Journal Website: http://usajournalshub.com/index,php/tajpslc

The Issues Of Ensuring International Security In The Virtual Space: Problems And Solutions

Sabyrbaeva Aynura Baxit Kizi
PhD Doctoral Student Of Faculty Of Postgraduate Education, Academy Of The MIA, Tashkent, Uzbekistan

ABSTRACT

The article discusses the problems of countering cybercrime, the issues of ensuring international security in the virtual space and the problems of international cooperation between states during the investigation and identification of criminals. Conclusions and proposals are made to eliminate occurred problems and to strengthen international cooperation, which will optimize the forces of states in the fight against cybercrime by establishing territorial boundaries in the virtual space and creating a single body under the United Nations Organization with representatives of all countries of the world.

KEYWORDS

International cooperation, international security, United Nations Organization, Convention, law enforcement agencies, virtual space, territorial boundaries, cyber threat, information and communication technologies.

INTRODUCTION

In a period of rapidly developing technologies, the introduction of modern innovations in every sphere of the country's life, along with the positive moments of technological progress, the growth and sophistication of methods of committing fraud presupposes

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: September 29, 2020 | **Pages:** 62-66
Doi: https://doi.org/10.37547/tajpslc/Volume02Issue09-11

IMPACT FACTOR
2020: 5. 453

strengthening international cooperation between law enforcement agencies of foreign countries.

One of the main goals of foreign law enforcement agencies is the fight against international crime, especially using social networks and the Internet, which has allowed modern criminals to expand their geographic coverage, diversify their goals and activities, often without the need for interactive communication or physical presence.

Cybercrimes are especially dangerous types of criminal attacks. But what is cybercrime? According to UN experts, the term "cybercrime" covers any crime that may be committed using a computer system or network, within a computer system or network, or against a computer system or network [1.29].

According to Symantec Security, an international cyber security service, 12 people are attacked globally every second, and about 556 million cybercrimes are committed annually worldwide, causing more than $ 100 billion in damage [2.46].

The international community has long begun to sound the alarm about the danger of cybercrimes, since, unlike other crimes, they are distinguished by a high level of latency, the transnational nature of the encroachment, and the difficulty of locating criminals.

A special danger among crimes in the virtual space is occupied by economic crimes, one of which is cyber fraud. OSCE experts estimate the annual damage to the world economy from industrial espionage, theft and fraud on the Internet at $ 100 billion [3.114].

Cybercrime is becoming a big problem around the world, so many countries are starting to enact laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime [4.87]. Each country is fighting this socially dangerous phenomenon in different ways based on the norms of national legislation, mentality and the level of threat to national security.

Taking into account the factor of globalization of computer crime, it becomes more obvious that today no state is able to independently resist this threat. At the same time, a significant role in such cooperation belongs to the international legal mechanisms of regulation and interaction of law enforcement agencies on the issues of countering and investigating computer crimes [5.225]. Agreeing with the opinion of Buraeva L.A. it is necessary to note the importance of the statements of Bulay Yu.G., Bulai R.I. about the need to fight at three levels: national, regional and international [6.35]. After all, the creation of a single international mechanism for regulating the Internet space and centers for coordinating cooperation between law enforcement agencies of foreign states will help prevent the commission of cyber fraud at an early stage.

RESULTS AND ITS DISCUSSION

Fraudsters, using the virtual space for their own selfish purposes, mistakenly consider themselves inaccessible to law enforcement agencies, but they are wrong. To effectively counter these challenges, it is important to establish strong legal relationships in cooperation between law enforcement agencies of foreign countries in order to create a global network with a single database.

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: September 29, 2020 | **Pages:** 62-66
Doi: https://doi.org/10.37547/tajpslc/Volume02Issue09-11

IMPACT FACTOR
2020: 5. 453

Report of the UN Secretary General to the 74th session "Countering the use of information and communication technologies for criminal purposes", which highlighted the difficulties that UN member states face in the fight against cybercrime.

One of the main problems in the investigation of cybercrime, referred to by countries, is the difficulty in gaining access to data, in particular regarding information on social networks such as Facebook, Telegram, Whatsapp, Instagram, as they refuse to provide the user's personal information, referring to violation of their rights. However, in situations where this evidence is necessary for resolution in court and can play an important evidentiary decision, it is deemed appropriate to obtain it by a court decision. However, since these social messengers do not have licenses to carry out activities on the territory of any country, they do not obey the laws of this or that country. Due to the fact that they provide services outside the state, where they store all data about users. To resolve this issue, it seems appropriate to oblige to obtain a state license to carry out activities on the territory of a certain country with a written consent to provide an important judicial information on the relevant decision of the judicial authority and in case of refusal to prohibit the operation of this social messenger in the country. An example of such harsh but appropriate measures from the point of view of criminal policy is the example of China, which banned the use of such social messengers as Telegram, Instagram, WhatsApp. Botswana also pointed out the problems of obtaining evidence from social messengers in its UN report.

It is dangerous that cybercriminals can use the user's data stolen from the Internet and commit crimes on his behalf, “transferring all the atrocities to his account”. In addition to tougher punishment for cybercrime, there is a need to focus on raising public awareness of cybersecurity, especially in the private sector, and improve law enforcement practices in this area. There is a need to focus on strengthening the mental and technical capacity of law enforcement agencies.

As an example, Australia can be cited, which in its letter to the UN referred to the problems they face in the implementation of cooperation in the fight against cybercrime. In some countries, the issues of countering cybercrime were not legally enshrined, let alone technical potential.

A significant shift in the international fight against cybercrime was the adoption by the UN General Assembly of the resolution of the Russian Federation on the establishment by the UN of a special intergovernmental committee of experts with representatives of all countries, whose main task will be to develop a single international convention on countering all forms of cybercrime, including cyber fraud.

This document will help coordinate the work of law enforcement agencies in all countries. However, when developing this document, it is necessary to take into account the importance of establishing the digital sovereignty of countries over their information space, as well as create a single International Center with sub-centers in the field as an international organization "Interpol" with a single database, equipment and qualified specialists.

Based on the above, it can be noted that one of the main problems in the fight against cybercrime is:

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: September 29, 2020 | **Pages:** 62-66
Doi: https://doi.org/10.37547/tajpslc/Volume02Issue09-11

IMPACT FACTOR
2020: 5. 453

- Lack of a single international document regulating the issues of countering cybercrime and binding on all its participants
- Non-regulation of the virtual space, lack of a mechanism to ensure cooperation in the investigation of cybercrime and the procedure for the transfer of evidence (including electronic)
- Insufficient qualification of law enforcement agencies in matters of cybercrime, criminal schemes and methods of its commission, as well as in the implementation of its prevention
- Inadequate awareness of Internet users about possible cyberattacks, cybersecurity measures and actions when cybercrime is committed against them
- Difficulty in determining the exact location of the offender and his detention, if an international agreement on the extradition of the offender is not concluded with the country in which he is located
- Lack of promptness in the investigation of cybercrimes, including cyber fraud and mass cyberattacks, due to differences in legislation and even the absence, in some cases, of a legislatively regulated mechanism for combating cybercrime
- Lack of a single concept of "electronic evidence" and a single legal mechanism for their selection, execution, scope and transfer to another country, the initiator of the request
- The lack of settlement of the issue of criminal prosecution for committing cybercrime (an international request for obtaining electronic evidence in a criminal case may be rejected by the other party due to the non-recognition of such an act as a crime on its territory)

CONCLUSIONS

Taking into account the increasing prevalence of fraud in cyberspace, the degree of its public danger, transnational nature and international scale, in order to further close cooperation among the law enforcement agencies of UN member states in the fight against cybercrime, proposals are made:
on the creation on the territory of all UN member states of a single database (a communication point operating 24 hours 7 days a week) for recording and registering cybercrimes and to develop a simplified mechanism for information exchange;

on the development of a single international document "On cooperation in the field of cybercrime" on the basis of the UN, which is binding on all UN member states while maintaining state sovereignty and national regulation boundaries in the virtual space;

on the obligatory introduction by all UN member states of amendments to the existing criminal legislation with the establishment of types of cybercrime, the commission of which entails criminal liability on the basis of a single international document;

on the creation of a single communication point operating 24 hours 7 days a week on the territory of all UN member states and the development of a simplified mechanism for information exchange;

on the establishment of uniform concepts of criminal acts, the commission of which entails criminal or administrative responsibility.

REFERENCES

1. Valko D.V. Cybercrime in Russia and the World: A Comparative Analysis.

Published: September 29, 2020 | **Pages:** 62-66
Doi: https://doi.org/10.37547/tajpslc/Volume02Issue09-11

Management in modern systems No. 3 (10) 2016. 2311-1313. P. 29

2. Karpova D.N. Cybercrime is a global problem and its solution. Power. No. 8. 2014. Moscow, P. 46
3. The Bank of Russia (2014). On the procedure for investing the insurer's own funds (capital) and the list of assets allowed for investment: Bank of Russia instruction No. 3445-U dated 16.11.2014. Bank of Russia Bulletin. P.114.
4. Cherkasov D. Yu., Ivanov V. V., Lubova E. S. Cybercrime in the modern world. Moscow Institute of Radio Engineering, Electronics and Automation, Moscow. 2016 P.87
5. Buraeva L.A. Transnational computer crimes as a global threat to the world community. Business within the law. Economic and legal journal №5. 2016. P. 225
6. Yu.G. Bulay and RI Bulay Prevention and counteraction to cybercrime, as well as international cyberthreats. Network publication "Academic Thought" No. 1. P.35
https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam