**Elvin Balajanov. Analysıs of jurısdıctıonal challenges ın the fıght agaınst cybercrıme // Azərbaycan Prokuroru Jurnalı, Law Journal, 2022, səh. 57-63**

**Elvin Balajanov (e.balajanov.edu@gmail.com; ebalajanov@akta.az)**
**Chairman of Association of Cybersecurity Organizations of Azerbaijan, PhD in Law**

# ANALYSIS OF JURISDICTIONAL CHALLENGES IN THE FIGHT AGAINST CYBERCRIME

*The rise of cybercrime as a global menace has presented significant challenges to law enforcement agencies and legal systems worldwide. This article explores the complex jurisdictional issues surrounding cybercriminal offenses, shedding light on the unique dynamics introduced by cybercrime within the broader context of transnational crimes. While various forms of transnational criminal activities have required international cooperation in the past, cybercrime's distinctive characteristics, including its borderless nature and the dispersion of evidence and actors across the globe, have added a layer of complexity to the jurisdictional landscape. This article emphasizes the imperative for collaboration among diverse law enforcement agencies, both within and across international borders, in the fight against cybercrime. The exchange of critical data and intelligence is central to this collaborative effort. However, it also underscores the need for nations to grapple with intricate jurisdictional challenges to ensure the effective and efficient combatting of cybercrime. In a world where cybercriminals can operate with impunity across borders, addressing jurisdictional dilemmas has become increasingly critical, leading to a proliferation of concurrent or competing claims to jurisdiction. This article serves as a comprehensive analysis of these jurisdictional intricacies within the context of cybercrime, highlighting the urgency of global cooperation in the face of this evolving threat.*

***Keywords:*** *cybercrime, jurisdiction, international cooperation, the principle of territoriality, the principle of nationality.*

## 1. Introduction

Cybercrime effortlessly transcends geographical boundaries and often evades state control. Nevertheless, cybercrime is not the first nor the sole category of criminal activity that can cross state borders, presenting investigative and prosecutorial challenges. In recent decades, global efforts have been necessary to combat various forms of transnational crimes, including illicit drug and firearm trafficking, terrorist actions, theft of art and cultural artifacts, human trafficking and commercial sex trade, maritime crime and piracy, and money laundering (1). However, cybercrime introduces distinctive complexities to national criminal justice systems. This is due to the widespread dispersion of evidence, perpetrators, and victims on a global scale, as well as the rapidly growing demand for specialized technical expertise essential for investigation and prosecution (2).

Cybercrime is often regarded as having a 'transnational dimension’. Therefore, it is essential to clarify the meaning of cybercrime acts that exhibit 'transnational dimensions’. According to the United Nations Convention against Transnational Organised Crime, an offence is ‘transnational in nature’ if:

> ‘(a) it is committed in more than one state; (b) it is committed in one state but a substantial part of its preparation, planning, direction or control takes place in another state; (c) it is committed in one state but involves an organised criminal group that engages in criminal activities in more than one state; (d) it is committed in one state but has substantial effects in another state.’ (3, Article 3.2)

While this approach has indeed highlighted crucial elements, it may not entirely align with cybercrime acts. This is because 'organized criminal groups' are not a focal point in cybercrime, and the transnational 'dimension' can manifest without involving 'preparation, planning, direction, or control' within another state (4). In its most basic form, transnational crime can be defined as crimi-

nal activities that cross borders, violate the laws of multiple states, or possess actual or potential cross-border impacts of national or international significance. Therefore, cybercrime can be classified as a typical transnational crime because it often impacts and implicates various jurisdictions. In practice, a significant proportion of cybercrime incidents include a 'transnational element,' as indicated by a UN study (note: according to a study conducted by United Nations Office on Drugs and Crime, percentage of cybercrime acts involving a transnational dimension was over 70% in responded European countries) (5), and Azerbaijan is no different in this regard, as many reported cybercrime cases under investigation by law enforcement agencies (LEAs) also exhibit transnational dimensions.

The inherently global nature of cybercrime underscores the imperative for collaboration among diverse law enforcement agencies (LEAs), spanning both domestic and international boundaries. This collaboration revolves around the exchange of critical data and intelligence. Nevertheless, to ensure the effective and efficient combatting of cybercrime, nations must confront the intricate challenges related to jurisdiction. It is essential to acknowledge that the landscape of cybercrime has given rise to intricate jurisdictional dilemmas, leading to a proliferation of concurrent or competing claims to jurisdiction.

## 2. Jurisdictional challenges in the realm of combatting cybercrime

The concept of jurisdiction within a state primarily pertains to the authority of a sovereign nation to govern, adjudicate, and enforce specific norms or regulations, which extends over its territory, citizens, and activities occurring within its borders, allowing the state to maintain order, ensure compliance with its laws, and protect the rights and interests of its residents (6, Annex E, 517). In the context of prosecuting and investigating cybercrime, 'jurisdiction' assumes a critical role and can be comprehensively defined as the legal authority conferred upon a state to both assert and exercise its domestic laws in response to cybercrimes committed within or impacting its boundaries (7, p. 5-6).

The location of the criminal act stands out as the most commonly employed determinant within jurisdictional provisions, a principle explicitly underscored as the primary factor for jurisdictional establishment by the Convention on Cybercrime (8, pp 10). The jurisdiction clause outlined in Article 22 of the Convention acknowledges the principle of territoriality by mandating that Parties exercise jurisdiction over any offense established in accordance with the Convention when said offense occurs within the state's geographical territory (9). Furthermore, States Parties are obligated to establish criminal jurisdiction over offenses committed on ships flying their flag or aircraft registered under their laws (9, Article 22 (1)(b)(c)).

Much like the Convention, the Code of Criminal Procedure and the Criminal Code of the Republic of Azerbaijan incorporate jurisdictional clauses that adhere to this principle. According to Article 11 of the Criminal Code, individuals who commit crimes within the territory of the Republic of Azerbaijan are liable for criminal prosecution under the Criminal Code (10, Article 11). Within the Republic's territory, as well as on ships bearing its flag or aircraft registered under its laws, only the criminal procedure legislation of the Republic of Azerbaijan shall apply, unless stipulated otherwise by international treaties to which the nation is a party (11, Article 3). Furthermore, it is firmly established that any criminal act that is initiated, conducted, or concluded within the territorial boundaries of the country shall unequivocally be considered a crime committed within the Republic of Azerbaijan (10, Article 11). This legal doctrine, rooted in the principle of territoriality, forms the bedrock of the nation's jurisdictional framework, empowering it to exercise its sovereign authority over offenses occurring within its geographical borders. This provision embodies the concept that for the country to assert territorial jurisdiction, it is not obligatory for the entire offense to occur within the country. In other words, the application of territorial jurisdiction does not necessitate that all elements of the crime transpire within the state's territory.

This approach finds support in the Explanatory Report to the Convention on Cybercrime, which elucidates that under the principle of territoriality, a party can assert territorial jurisdiction if the computer system targeted is within its territory, even if the attacker is not physically present within that territory. This principle applies not only when the attacker is targeting a computer system and victim system both located within its territory but also when the attacker targets a system within its territory from elsewhere (12, para. 233).

The location where a crime has an impact has long been recognized as one of the essential elements of the offense within the criminal context (13). This critical aspect not only helps determine the jurisdiction of the legal proceedings but also plays a pivotal role in shaping the legal and investigative processes associated with the alleged criminal activity. According to Ryngaert, international law appears to have settled for the condition that either the criminal act itself or its repercussions must occur within a state's territory for that state to legitimately exercise territorial jurisdiction (14, p. 278). This principle is likewise evident in the Criminal Code, where it is specified that foreign citizens and stateless individuals who have committed a crime outside the territorial boundaries of the Republic of Azerbaijan against its citizens or interests can be subject to criminal liability within Azerbaijan, particularly if these individuals have not previously been convicted for the same offense in the foreign state (10, Article 12.2). This underscores the country's commitment to upholding justice and safeguarding its interests beyond its borders. Hence, Azerbaijani law enforcement agencies (LEAs) have the authority to issue indictments when the consequences or effects of a crime occur within its territory, even if the actions and whereabouts of the perpetrator are beyond its borders. Nevertheless, enforcing this provision presents significant challenges and could potentially lead to a complex scenario of concurrent jurisdiction. This dynamic underscore the need for precise legal frameworks and international cooperation to effectively address cross-border criminal activities Furthermore, both national laws and the Convention on Cybercrime often overlook the complexities of jurisdictional concurrency. Consequently, there is a pressing need for more straightforward and precise solutions to resolve existing ambiguities and intricacies in concurrent jurisdictions. Addressing these issues is vital to ensure a more effective and streamlined response to cross-border cybercrimes. Otherwise as articulated by Kohl, 'territorially centred criminal law is edging closer to a tipping point, not because it is excessively intricate, but because it is equitable neither for individuals nor for states' (15, p. 106).

The nationality of the perpetrator is broadly acknowledged as the second primary determinant of jurisdiction in cybercrime cases, following territoriality (8, p. 24). This principle of nationality is also explicitly included in the Convention, compelling Parties to assert jurisdiction when the act is carried out 'by one of its nationals if the offense is punishable under criminal law where it was committed, or if the offense occurs outside the territorial jurisdiction of any State' (9, Article 22 (1)(d)).

Azerbaijan has a comparable clause, incorporating the prerequisites of dual criminality and the *'ne bis in idem'* principle within its legal framework (*Ne bis in idem* principle has been described as a fundamental principle of law, which restricts the possibility of a defendant being prosecuted repeatedly based on the same offence, act, or facts) (16). As outlined in Article 12 of the Criminal Code, Azerbaijani citizens who commit a crime outside the nation's borders, along with stateless individuals permanently residing within the country, are liable to face criminal prosecution under the Criminal Code. This prosecution is contingent upon specific conditions: firstly, the act in question must be recognized as a criminal offense both in the Azerbaijan Republic and in the state where it was committed. Secondly, the individuals in question should not have been previously convicted for the same offense in the foreign state. This provision demonstrates Azerbaijan's commitment to ensuring that its citizens and residents are held accountable for their actions, even when those actions transpire beyond its territorial boundaries. It also underscores the significance of aligning the legal standards of both the Republic of Azerbaijan and the foreign state where the crime occurred,

thus upholding the principle of dual criminality. Moreover, the inclusion of the 'ne bis in idem' principle reflects the nation's dedication to preventing double jeopardy, ensuring that individuals are not subjected to multiple prosecutions for the same offense, both domestically and abroad.

In the realm of cybercrime, the principle of nationality assumes a somewhat diminished significance compared to traditional crimes, primarily because cybercrime doesn't necessitate the physical presence of the perpetrator in another country to commit an offense abroad. Nevertheless, Arnell contends that the principle of nationality should be considered on par with territoriality as a fundamental basis for criminal jurisdiction, given the limitations of the existing territorial jurisdictional framework. This is especially pertinent in an era where borders and territorial boundaries are losing their once-central role in jurisdiction due to the increasing capacity of individuals to commit crimes from remote locations (17, pp 955-962). Arnell's proposition highlights the need for legal frameworks to adapt to this changing landscape by considering the principle of nationality as a key determinant of jurisdiction in cybercrime cases. It recognizes that individuals, regardless of their physical location, can inflict substantial harm and commit crimes against other states and their citizens through digital means. Thus, emphasizing the principle of nationality in the context of cybercrime jurisdiction helps ensure that cybercriminals are not immune from prosecution solely due to the intangible nature of their actions.

These factors appear to hold practical significance in underlining the importance of the nationality principle, particularly from an enforcement standpoint. Simultaneously, it underscores the collective interest of individuals in having an effective criminal law system in place, which elucidates the state's normative authority to impose penalties. Inhabitants of a state may indeed feel a sense of shock or dismay when a co-national commits a crime outside its borders. However, these offenses do not invariably erode their confidence in the criminal justice system under which they reside (18, p. 60-61). In essence, one could contend that unless the actions of its citizens abroad directly impact the state's interests, the government may exhibit limited interest in intervening or prosecuting such individuals. This reluctance could stem from a desire to sidestep the inconvenience, complexity, and substantial costs associated with mutual legal assistance that invariably accompany cross-border criminal cases. Consequently, Brenner posits a thought-provoking perspective in the context of cybercrime: that the perpetrator's nationality should be considered as a factor that discourages, rather than encourages, the assertion of jurisdiction (19, 202). Brenner's argument highlights the need for a balanced and pragmatic approach to jurisdiction in cybercrime cases. While nationality can be a relevant factor, it should not be the sole determinant in asserting jurisdiction. Rather, a more comprehensive assessment that considers the impact on the state's interests, the severity of the offense, and the potential for international cooperation should guide jurisdictional decisions. This approach ensures that nations can effectively address cybercrimes while minimizing unnecessary impediments and complexities in the pursuit of justice across borders.

An examination of the two primary determinants of jurisdiction reveals that multiple countries may assert jurisdiction over a specific cybercrime offense. It can be reasonably posited that within the realm of cybercrime, jurisdictional conflicts are poised to escalate even more rapidly in the near future. This escalation is propelled by the expansive nature of cyberspace and the architecture of the internet, which has empowered states with the capacity to conduct extraterritorial investigations and, consequently, assert jurisdiction over a broad spectrum of offenses.

Hence, there is a compelling need for the development of specific legislation in this domain, notably absent in Azerbaijan's legal framework. Addressing this gap, Article 22 of the Convention on Cybercrime presents a mechanism for consultation in cases of overlapping jurisdiction. According to the Convention, with the aim of enhancing the efficiency and fairness of legal proceedings, when more than one Party asserts jurisdiction over an alleged offense, the concerned State Parties are encouraged to engage in consultations to determine the most suitable jurisdiction for prosecution (9, Article 22). It is important to note that this consultation is not an absolute obligation but is

expected to occur 'where appropriate,' allowing a Party the flexibility to postpone or decline consultation if it believes it could hamper its ongoing investigations or proceedings (9, Article 22).

It is evident that the Convention does not offer specific criteria for resolving jurisdictional overlaps in cybercrime cases, nor does it provide clear directives on the circumstances under which multiple parties can or should assert jurisdiction over the same offender or offense (19, p. 197). In light of this, there is a recognized need for a mechanism to prioritize jurisdictional claims, even though certain traditional factors used for prioritization, such as the location of the crime, the perpetrator's custody, the extent of harm, nationality, the strength of the case against the perpetrator, punishment considerations, as well as considerations of fairness and convenience, appear to have diminished applicability in the context of the Internet (7, p. 25).

The borderless nature of the digital realm and the unique characteristics of cybercrimes pose significant challenges to the conventional principles governing jurisdiction. Consequently, the development of innovative and adaptable criteria for prioritizing jurisdictional claims in cybercrime cases is essential. Such criteria should align with the realities of the digital age, accounting for the global reach of cybercrimes, the ability of perpetrators to operate remotely, and the interconnectedness of cyberspace.

This evolving landscape underscores the importance of international collaboration, legal harmonization, and the establishment of clear guidelines for addressing jurisdictional challenges in cybercrime. As nations grapple with these complexities, there is a growing recognition that traditional jurisdictional principles must be adapted to effectively combat cyber threats and uphold justice in the online environment.

## 3. Conclusion

The dynamic and ever-evolving landscape of cyberspace, marked by its borderless nature, has provided a fertile breeding ground for complex jurisdictional challenges. As nations increasingly wield their authority to investigate and prosecute cybercrimes that transcend their territorial boundaries, conflicts over jurisdiction have become a pressing concern. These disputes are poised to escalate in intensity as the internet's global interconnectedness continues to erode traditional geographical boundaries. This evolution grants states the ability to assert jurisdiction over a broad spectrum of cyber offenses committed by individuals situated virtually anywhere in the world.

In response to these challenges, there is a growing recognition of the need to establish innovative and adaptable criteria for prioritizing jurisdictional claims in cybercrime cases. These criteria should align with the realities of the digital age, acknowledging the global reach of cybercrimes, the capacity of perpetrators to operate remotely, and the inherent interconnectedness of the digital realm.

Within this context, the imperative for robust international cooperation, the development of clear legal frameworks, and the establishment of shared standards for addressing jurisdictional issues in cyberspace becomes paramount. These measures are indispensable for promoting collaboration among nations, mitigating conflicts, and ensuring that cybercriminals do not exploit jurisdictional ambiguities to evade accountability on the global stage. The proactive pursuit of these initiatives is essential to uphold the rule of law and combat cyber threats effectively in this rapidly evolving landscape.

**The list of sources:**

1. United Nations Office on Drugs and Crime, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations, 2010).
2. Brenner, S. W., *Cyberthreats and the Decline of the Nation-State* (Routledge, Taylor & Francis Group 2014).
3. *United Nations Convention against Transnational Organized Crime* (2000).
4. Lavorgna A., 'Cyber-Organised Crime. A Case of Moral Panic?' (2018) *Trends in Organized Crime*.
5. United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (United Nations 2013).
6. *United Nations Report of the International Law Commission*, 58th session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E.
7. Kaspersen, H., *Cybercrime and Internet Jurisdiction* (Council of Europe Report Draft, 2009).
8. Brenner, S. W., Koops, Bert-Jaap, 'Approaches to Cybercrime Jurisdiction' (2004) 4 *Journal of High Technology Law*).
9. *Council of Europe Convention on Cybercrime* (2001) ETS No. 185.
10. *Criminal Code of the Republic of Azerbaijan* (https://e-qanun.az/framework/46947).
11. *Code of Criminal Procedure of the Azerbaijan Republic* (https://e-qanun.az/framework/46950).
12. Council of Europe, *Explanatory Report to the Convention on Cybercrime* (2001) ETS 185.
13. *SS Lotus (France v Turkey)* [1927] PCIL Reports, Series A No. 10, [55].
14. Ryngaert, C., *Jurisdiction in International Law* (Oxford: Oxford University Press, 2nd edn, 2015).
15. Kohl, U., Jurisdiction and the Internet (1st edn, Cambridge: Cambridge University Press 2007).
16. Bockel, B., *The Ne Bis in Idem Principle in EU Law* (1st edn, Austin: Wolters Kluwer Law & Business, 2010).
17. Arnell, P., 'The Case for Nationality Based Jurisdiction' (2001) 50 *International & Comparative Law Quarterly*.
18. Chehtman, A., *The Philosophical Foundations of Extraterritorial Punishment* (1st edn, Oxford: Oxford University Press, 2010).
19. Brenner, S. W., 'Cybercrime jurisdiction' (2006) 46 *Crime, Law and Social Change*.

**Elvin Balacanov (e.balajanov.edu@gmail.com; ebalajanov@akta.az)**
**Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyasının sədri,**
**hüquq üzrə fəlsəfə doktoru**

## KİBERCINAYƏTKARLIĞA QARŞI MÜBARİZƏDƏ YURİSDİKSİYA PROBLEMLƏRİNİN TƏHLİLİ

*Kibercinayətlərin qlobal səviyyədə sürətlə artması hüquq mühafizə orqanları və hüquq sistemləri qarşısında bir sıra mühüm çətinliklərin yaranması ilə nəticələnmişdir. Bu məqalə transmilli cinayətlərin daha geniş kontekstində kibercinayətkarlığın yaratdığı unikal dinamikaya işıq salmaqla kibercinayətkarlıq cinayətləri ilə bağlı mürəkkəb yurisdiksiya məsələlərini araşdırır. Transmilli cinayətkarlığın digər formalarından fərqli olan kibercinayətlərin bir sıra özünəməxsus xüsusiyyətlərə malik olması, xüsusilə də fiziki sərhədlərlə məhdudlaşmaması və zəruri sübutların əldə olunması ilə bağlı yaratdığı çətinliklər bu cinayətlərlə mübarizədə beynəlxalq əməkdaşlığı və qarşıya çıxan yurisdiksiya məsələlərini bir az da mürəkkəbləşdirmişdir. Məqalədə kibercinayətlərlə mübarizədə müxtəlif hüquq mühafizə orqanları arasında həm milli, həm də beynəlxalq səviyyədə*

*əməkdaşlığın, o cümlədən zəruri məlumat mübadilənin həyata keçirilməsinin önəmi qeyd olunur. Kritik məlumatların və kəşfiyyatın mübadiləsi bu əməkdaşlıq səyinin mərkəzidir. Eyni zamanda, kibercinayətkarlıqla effektiv və səmərəli mübarizənin təmin edilməsi məqsədilə dövlətlər tərəfindən mürəkkəb yurisdiksiya problemlərinin həll edilməsinin zəruriliyi diqqətə çatdırılır. Kibercinayətkarların sərhədləri aşaraq cəzasız fəaliyyət göstərə bildiyi bir dünyada yurisdiksiya ilə bağlı dilemmaların həlli getdikcə kritik hala gəldi və bu, yurisdiksiyaya paralel və ya rəqabət aparan iddiaların çoxalmasına səbəb oldu. Bu məqalə kibercinayətkarlıq kontekstində bu yurisdiksiya incəliklərinin hərtərəfli təhlilinə xidmət edir və bu inkişaf edən təhlükə qarşısında qlobal əməkdaşlığın aktuallığını vurğulayır.*

***Açar sözlər:*** *kibercinayət, yurisdiksiya, beynəlxalq əməkdaşlıq, ərazi prinsipi, vətəndaşlıq prinsipi.*

**Эльвин Баладжанов (e.balajanov.edu@gmail.com; ebalajanov@akta.az)**
**Председатель Ассоциации организаций кибербезопасности Азербайджана,**
**доктор философии по праву**

## АНАЛИЗ ПРОБЛЕМ ЮРИСДИКЦИИ В БОРЬБЕ ПРОТИВ КИБЕРПРЕСТУПНОСТИ

*Быстрый рост киберпреступности на глобальном уровне привел к возникновению ряда серь-езных проблем для правоохранительных органов и правовых систем. В этой статье исследуются сложные юрисдикционные вопросы, связанные с киберпреступлениями, и проливается свет на уникальную динамику, которую киберпреступность привносит в более широкий контекст транснациональных преступлений. Хотя различные формы транснациональной преступной деятельности в прошлом требовали международного сотрудничества, отличительные характеристики киберпреступности, в том числе ее безграничный характер и рассеяние доказательств и субъектов по всему миру, еще больше усложнили юрисдикционную среду. В статье отмечается важ-ность сотрудничества между различными правоохранительными органами на национальном и международном уровне, включая обмен необходимой информацией в борьбе с киберпреступно-стью. Обмен критически важными данными и разведданными занимает центральное место в этих совместных усилиях. Отмечается, что для обеспечения эффективной и действенной борьбы с киберпреступностью государствам необходимо решить сложные юрисдикционные проблемы. В мире, где киберпреступники могут действовать безнаказанно за рубежом, решение юрисдикцион-ных дилемм становится все более важным, что приводит к увеличению количества одновременных или конкурирующих претензий на юрисдикцию. Эта статья представляет собой всесторонний анализ этих юрисдикционных сложностей в контексте киберпреступности, подчеркивая без-отлагательность глобального сотрудничества перед лицом.*

***Ключевые слова:*** *киберпреступление, юрисдикция, международное сотрудничество, территориальный принцип, принцип гражданства.*