HUKUK FAKÜLTESİ DERGİSİ LAW REVIEW

Research Article

e-ISSN: 2667-5714
https:dergipark.org.trenpubinuhfd

CYBERCRIME ENFORCEMENT ON THE DARK WEB: PRIVACY CHALLENGES AND INVESTIGATIVE POWERS UNDER THE CYBERCRIME CONVENTION

Abdurrahman GÖREN, Istanbul Medeniyet University, İstanbul, Türkiye

Uğur AŞKIN, Inonu University, Faculty of Law, Department of Criminal and Criminal Procedure Law, Malatya, Türkiye

Corresponding Author: *Uğur AŞKIN, ugur.askin@inonu.edu.tr*

Citation Gören, A. & Aşkın, U. (2026). Cybercrime enforcement on the dark web: privacy challenges and investigatıve powers under the cybercrime convention. *Journal of İnönü University Faculty of Law,17*, 1, 72–88.

doi 10.21492/inuhfd.1906102

Received Date: March 10, 2026 **Accepted Date:** April 15, 2026 **Published Date:** May 12, 2026

Abstract

The rapid development of digital technologies and the widespread use of anonymity tools have significantly altered the nature of cybercrime. In particular, the emergence of the Dark Web has provided criminals with an environment in which they can operate anonymously, making the detection and prosecution of cybercrime increasingly complex. In response to these challenges, the Convention on Cybercrime has established an international legal framework aimed at strengthening inter-state cooperation in combating cybercrime and facilitating investigation procedures related to digital evidence.

It examines the provisions of the Convention on Cybercrime relating to Dark Web investigations and the protection of data privacy. First, it analyses the procedural mechanisms introduced by the Convention, particularly those relating to data retention, the search and seizure of stored computer data, and the interception of traffic data. It then addresses the development of data protection standards within the European Union, particularly Directive (EU) 2016/680 in the field of criminal law and police cooperation and its relationship with the General Data Protection Regulation (GDPR). Contemporary investigative methods used by law enforcement agencies, including technological tools such as Network Investigation Techniques (NIT), are evaluated. While these methods can increase the effectiveness of cybercrime investigations, they also raise significant legal concerns regarding compliance with jurisdiction, cross-border investigations, and international legal principles, particularly the protection of state sovereignty and privacy rights.

Although the Convention on Cybercrime plays an important role in promoting international cooperation in combating cybercrime, it has been concluded that its provisions face difficulties in responding to technological developments and anonymous online environments such as the Dark Web. Therefore, clearer legal regulations and stronger international cooperation mechanisms are necessary to sufficiently protect fundamental rights, particularly the right to privacy, while maintaining the effectiveness of cybercrime investigations.

Keywords: Cybercrime Convention, Dark Web, Data Privacy, Network Investigative Technique (NIT), Cross-Border Investigation.

EXTENDED SUMMARY

This study examines the legal and practical challenges of cybercrime enforcement on the Dark Web within the framework of the European Convention on Cybercrime. It focuses on the intersection between investigative powers and data privacy, evaluating whether the existing international legal framework is capable of addressing the complexities arising from anonymised digital environments. The analysis is structured around three core issues: the adequacy of the Convention's procedural provisions, the evolving standards of data protection in criminal law, and the effectiveness and legality of contemporary investigative techniques, particularly in cross-border contexts.

At the outset, the study highlights the significance of the Convention as the most comprehensive international instrument regulating cybercrime. By establishing common definitions of cyber offences and introducing procedural tools such as data preservation, search and seizure, and interception of communications, the Convention provides a foundational framework for international cooperation. Its provisions on mutual legal assistance and extradition further reinforce its role in facilitating cross-border investigations. However, despite its broad acceptance and practical importance, the Convention has been subject to sustained criticism, particularly regarding its ability to respond to rapid technological developments and its limited engagement with data privacy concerns.

A central argument of the study is that the Convention's treatment of privacy remains insufficient in light of contemporary human rights standards. Although Article 15 requires States Parties to implement safeguards for fundamental rights, including privacy, the Convention does not provide detailed or specific guidance on how these safeguards should be operationalised. Instead, it relies on general clauses that defer to external human rights instruments. This indirect approach creates uncertainty and may lead to inconsistent application at the domestic level. The analysis of Articles 16 and 17 demonstrates that the obligation to preserve data and the expedited disclosure of traffic data, while essential for effective investigations, may risk excessive interference with individual privacy if not accompanied by clear limitations and robust oversight mechanisms. Similar concerns arise in relation to Articles 19 to 21, where the broad scope of investigative powers and the lack of differentiation between categories of data increase the likelihood of disproportionate surveillance practices.

The study further situates these concerns within the broader evolution of data protection law. By examining Directive (EU) 2016/680 and its relationship with the GDPR, it illustrates the emergence of more comprehensive and structured approaches to data protection in the field of criminal law enforcement. While the directive strengthens safeguards and promotes harmonisation, the coexistence of multiple regulatory regimes also generates legal complexity and uncertainty. This tension underscores the inadequacy of the Convention's relatively limited and outdated privacy framework when compared to more recent legal developments.

In addition to normative deficiencies, the study emphasizes the structural challenges posed by the Dark Web. Originally designed to protect privacy and enable secure communication, the Dark Web has evolved into a significant platform for criminal activity, including drug trafficking and the dissemination of child exploitation material. The anonymity provided by technologies such as Tor complicates the identification of offenders and the determination of jurisdiction, thereby limiting the effectiveness of traditional investigative methods. The analysis of high-profile cases, such as Silk Road and Playpen, demonstrates both the persistence of illicit networks and the limitations of conventional enforcement strategies.

Within this context, the study evaluates contemporary investigative techniques, focusing in particular on the Network Investigative Technique (NIT). Compared to methods such as server seizure or data indexing, NIT offers a more targeted approach by enabling law enforcement authorities to identify users engaging with illegal content while minimising interference with lawful users. This characteristic renders NIT a potentially more proportionate and effective tool in combating cybercrime on the Dark Web. However, its use raises complex legal questions, particularly in relation to jurisdiction and international law.

The study identifies significant challenges arising from the cross-border deployment of NIT. Domestic legal frameworks, such as the United States' Federal Rules of Criminal Procedure, have struggled to accommodate the extraterritorial dimensions of cyber investigations. Judicial decisions in cases like Playpen reveal inconsistencies in the interpretation of jurisdictional limits and the validity of warrants extending beyond territorial boundaries. Although amendments such as Rule 41(b)(6) attempt to address some of these issues, they remain limited to domestic contexts and do not resolve the broader challenges of international enforcement.

From the perspective of international law, the use of NIT raises questions concerning state sovereignty and the prohibition of extraterritorial enforcement without consent. While some scholars argue that cross-border cyber operations may constitute violations of international law, others contend that existing legal principles, developed prior to the digital age, are not directly applicable to remote electronic investigations. The study highlights this doctrinal uncertainty by examining competing interpretations advanced by scholars such as Ahmet Ghappour, Orin S. Kerr, and Sean D. Murphy. It further explores the role of customary international law and state practice in shaping the legal status of such investigative methods.

INTRODUCTION

The Cybercrime Convention adopted by the Council of Europe has long been considered one of the most significant international legal instruments in the field of cybercrime. The Convention establishes a legal framework for international cooperation and provides common standards regarding the investigation and security of activities conducted on the Internet[1]. In addition to the member states of the Council of Europe, the Convention has also been signed by non-member countries such as the United States, Canada, Japan, and South Africa. Due to this wide participation, the Convention is widely regarded as the principal international agreement guiding cooperation between governments in the fight against crimes committed in cyberspace.

The Convention aims to strengthen cooperation among states in combating cybercrime by introducing common definitions of certain cyber offences and by setting out procedural mechanisms that enable authorities to investigate such crimes effectively. It also includes provisions on mutual legal assistance, extradition, and other forms of international cooperation designed to facilitate cross-border criminal investigations. Nevertheless, despite its importance, the Convention has also been subject to criticism. In particular, concerns have been raised regarding its practical effectiveness and the potential impact of some investigative measures on the protection of data privacy. These concerns are addressed in this study through a detailed examination of the relevant provisions of the Convention.

The Dark Web, on the other hand, was initially developed as a technological environment intended to support the exercise of democratic freedoms such as freedom of expression and secure communication. In particular, journalists and activists operating in restrictive political environments used such networks to share information and communicate safely. Over time, however, the Dark Web also became a platform used by criminal groups. As a result, various forms of cybercrime began to emerge within this environment, including the illegal trade of drugs and weapons, as well as the distribution of child sexual exploitation material. The anonymity provided by technologies used within the Dark Web makes it considerably more difficult to identify offenders and determine their physical locations, thereby complicating both investigation and prosecution processes. Consequently, governments have increasingly sought to develop new investigative techniques that go beyond traditional law enforcement methods.

Within this framework, Chapter 2 of this study examines the provisions of the Cybercrime Convention in relation to Dark Web activities and privacy concerns. Chapter 3 provides a brief analysis of Directive (EU) 2016/680 concerning data protection in the context of criminal law enforcement and compares its approach with that of the GDPR. Chapter 4 offers a more detailed examination of the structure and functioning of the Dark Web. Finally, Chapter 5 discusses both traditional and contemporary investigative methods used in cybercrime cases and analyzes the challenges associated with the use of Network Investigative Techniques in such investigations.

I. CONVENTION ON CYBERCRIME

The protection of personal data and privacy is widely recognized as a fundamental component of modern human rights law. Within the framework of the Cybercrime Convention, issues related to privacy are primarily addressed in its second section, which regulates several procedural powers available to law enforcement authorities, including search, seizure, and the interception of digital data[2]. These provisions establish the legal basis for investigative measures in cybercrime cases while simultaneously emphasizing the need to respect fundamental rights during their implementation.

1 POUNDER, Chris, 'The Council Of Europe Cyber-Crime Convention', Computers & Security, S. 20 (5), 2001, s. 380.

2 Türkiye signed the Convention on Cybercrime, prepared within the framework of the Council of Europe, in Strasbourg on 10 November 2010, and following the completion of the ratification process, the Convention entered into force on 29 September 2014, thereby rendering Türkiye an official party thereto. Bkz. ALİUSTA, Cahit/BENZER, Recep, 'Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci', Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C. 4, No:2, S:35-- 42, 2018, 38.

Article 15 of the Convention specifically requires States Parties to incorporate adequate safeguards for the protection of human rights and fundamental freedoms when implementing the Convention in their domestic legal systems. In doing so, states are expected to comply with established international human rights instruments, including the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe and the 1966 United Nations International Covenant on Civil and Political Rights, as well as other relevant international legal agreements[3].

Despite these references to broader human rights obligations, the Convention has been criticized for not providing sufficiently detailed provisions regarding the protection of data privacy. While the right to privacy has gradually gained stronger recognition in subsequent international legal instruments and regulatory frameworks, the Convention itself addresses this issue only indirectly through general safeguard clauses. Consequently, some commentators argue that the Convention does not fully reflect the evolving importance of personal data protection within contemporary human rights law, leading to concerns about the adequacy of privacy safeguards in the context of cybercrime investigations[4].

Articles 16 and 17 of the Cybercrime Convention require States Parties to adopt legal measures that enable law enforcement authorities to request the preservation of specific computer data. Under these provisions, individuals or service providers may be obligated to retain certain data when it is necessary for a criminal investigation. For example, during an investigation into illegal online drug trafficking, authorities such as the FBI may request relevant institutions to preserve information related to the suspected activity. Article 16(2) also limits this preservation obligation to a specific period, generally up to ninety days or until the investigation reaches a particular stage. In addition, the article includes a confidentiality requirement that prevents the disclosure of the preservation order to the public. In addition to these provisions, Article 17 introduces the mechanism of expedited preservation and partial disclosure of traffic data[5]. This rule allows authorities to secure relevant traffic data quickly, even when multiple service providers are involved in the communication process. Through this procedure, investigators can identify the service providers connected to a communication and obtain the necessary information regarding data transmission[6]. Consequently, these provisions aim to facilitate cybercrime investigations by enabling the preservation of traffic data and the controlled sharing of certain information with competent authorities during the investigative process.

Nevertheless, Articles 16 and 17 have attracted criticism for potentially failing to maintain an appropriate balance between effective criminal investigation and the protection of individual privacy. According to the Internet Alliance, certain provisions contained in these articles may conflict with the principles of data protection established under the 1995 European Union Data Protection Directive. One of the primary concerns is that states lacking comprehensive data protection frameworks could potentially apply these powers beyond the intended purpose of the Convention, including for broader governmental surveillance activities or the identification of political opponents. In the absence of clear procedural limitations, such investigative tools may extend beyond the pursuit of cybercriminals and enable authorities to monitor individuals with opposing political views[7]. Given that the internet often functions as a platform through which individuals anonymously express political opinions or religious beliefs, the misuse of these investigative powers could undermine fundamental privacy protections. If the mechanisms established by the Convention are employed for purposes other than combating cybercrime, they may contradict the principles of personal data protection emphasized in the Data Protection Directive and weaken the legitimacy of the Convention itself.

Articles 19 to 21 of the Convention regulate investigative powers such as the search, seizure, monitoring, collection,

3 Convention on Cybercrime, 15.

4 BARON, Ryan M F, 'A Critique of the International Cybercrime Treaty', Common Law Conspectus, S.10, 2002, s. 263.

5 Convention on Cybercrime 16(2).

6 Convention on Cybercrime 17.

7 'Internet Alliance Comments On Council Of Europe's Draft Convention On Cyber-Crime No. 19' (*Center for Democracy & Technology*, 2000) <https://old.cdt.org/international/cybercrime/001000ia.shtml> accessed 1 January 2025.

and interception of computer data, building upon the procedural measures introduced in the preceding provisions. Article 19 primarily addresses the search and seizure of stored computer data, reflecting investigative techniques similar to those used in traditional criminal procedures. In contrast, Articles 20 and 21 provide the legal basis for law enforcement authorities to collect traffic data and intercept communications in order to examine and obtain information related to criminal activities conducted through digital networks[8]. However, these provisions have also raised concerns regarding the protection of personal data. Ryan M. F. Baron argues that the wording of these articles may pose risks to privacy because they do not clearly distinguish between different categories of data that should receive varying levels of protection during monitoring or seizure processes[9]. In particular, the broad use of the term "traffic data" suggests that a wide range of digital information could potentially be targeted for investigative purposes. As a result, the lack of precise limitations may increase the likelihood of disproportionate interference with individuals' data privacy.

With regard to international cooperation, the Convention outlines several mechanisms intended to facilitate collaboration among states in combating cybercrime. First, it emphasizes that cooperation between States Parties should be carried out to the widest extent possible. Second, the Convention also allows international cooperation in relation to offences involving computer systems and data, even when such offences are not explicitly defined within the Convention itself. Third, it clarifies that the provisions of the Convention do not replace or invalidate previously existing international agreements addressing similar matters[10]. These principles are also reflected in the provisions governing mutual legal assistance. The repetition of these rules in different sections of the Convention highlights the importance attached to international collaboration in addressing cybercrime. Overall, the relevant provisions demonstrate that the Convention seeks to maximize opportunities for cooperation among states in order to ensure a more effective response to crimes committed in cyberspace.

Regarding mutual legal assistance and cross-border law enforcement, the rapid advancement of technology and the ability of the internet to transcend physical borders have made international legal cooperation increasingly important in combating crime. Mutual legal assistance mechanisms enable states to cooperate in several areas, including the expedited preservation of stored computer data, the rapid disclosure of protected information, and faster access to digital evidence necessary for criminal investigations[11]. In this context, Amalie M. Weber argues that the Convention may implicitly permit extraterritorial access to publicly available digital data stored across borders without requiring a formal mutual legal assistance request[12]. Consequently, mutual legal assistance has become a significant legal instrument through which states coordinate their efforts to combat cybercrime, particularly within the context of the Dark Web.

The utilization of advanced technological tools has become essential for effectively addressing cybercrime, particularly offenses committed anonymously on the Dark Web. As discussed later, the Network Investigative Technique (NIT) serves a critical function in identifying the locations of perpetrators who exploit anonymity online. Despite being the sole international instrument regulating cross-border digital access, the Convention explicitly prohibits governments from conducting investigations across national borders[13]. This restriction is grounded in the principle of state sovereignty, which forbids investigators from operating within another country's territory without its consent[14]. Consequently, this limitation hinders the deployment of highly effective investigative tools, such as NIT, in combating

8 Convention on Cybercrime 19, 20, 21.

9 BARON, s. 263-264.

10 Convention on Cybercrime 23.

11 Convention on Cybercrime from 29 to 34.

12 WEBER, Amalie M, 'The Council of Europe's Convention on Cybercrime', Berkeley Technology Law Journal & Berkeley Center for Law and Technology, S. 18, 2003, s. 425-426.

13 WEBER, s. 426.

14 GHAPPOUR, Ahmed, 'Searching Places Unknown: Law Enforcement Jurisdiction On The Dark Web' Stanford Law Review, S. 69, 2017, s. 1119

cybercrime conducted on the Dark Web.

II. DATA PRIVACY

Globally, privacy has been increasingly recognized as a fundamental component of human freedom under various human rights instruments. In 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights, and shortly thereafter, the Organization of American States promulgated the American Declaration of the Rights and Duties of Man. Subsequently, in 1950, the Council of Europe introduced the European Convention for the Protection of Human Rights and Fundamental Freedoms, which sought to codify the principles outlined in the Universal Declaration[15]. Collectively, these instruments safeguard individuals' rights to privacy in both their family and personal spheres.

Considering the developments that followed the earliest data privacy conventions, the first structured regulation specifically addressing criminal law and policing was the 2008 Framework Decision[16]. Later, in 2016, the European Union adopted the Police and Criminal Justice Authorities Directive, which covers a similar field but introduces a more comprehensive framework[17]. Although the broad scope of the GDPR has raised questions about the directive's relevance, it continues to apply within the field of criminal law.

Regarding its effectiveness, the directive has a wider scope than the earlier Framework Decision. One key feature is that it applies not only to cross-border situations but also to processing within domestic contexts[18]. In addition, it strengthens data protection standards, improves safeguards against data breaches, and supports cooperation between states[19]. Overall, it advances the Framework Decision by promoting greater consistency, stronger data protection, and a higher level of harmonisation through more effective implementation mechanisms[20].

Despite the directive's advantages, certain tensions remain between the directive and the General Data Protection Regulation. In some situations, the regulation establishes stronger data protection guarantees and imposes stricter obligations on data controllers than those provided under the directive[21]. The coexistence of two different data protection regimes and sets of obligations also raises concerns about legal certainty and may lead to the application of incorrect rules[22]. Consequently, this dual framework can create practical difficulties and confusion for police and other law enforcement authorities, while similar uncertainty may also affect data subjects and third-party organisations.

III. DARK WEB

The Dark Web emerged gradually and was initially developed with ideals such as protecting privacy and supporting democratic freedoms. However, its use has increasingly expanded beyond these original purposes. For instance, the developers of Tor (The Onion Router) designed the system primarily to enable secure communication for military personnel operating abroad. Similarly, the creators of Hidden Wiki established a directory intended to help ordinary internet users navigate this hidden part of the internet. As noted by Michael Chertoff, although the technologies were

15 VOGT, Sophia Dastagir, 'The Digital Underworld: Combating Crime On The Dark Web In The Modern Era', Santa Clara Journal of International Law, S. 15, 2017, s. 104-105.

16 MARQUENIE, Thomas, 'The Police And Criminal Justice Authorities Directive: Data Protection Standards And Impact On The Legal Framework', Computer Law & Security Review, S. 33, 2017, s. 324-325.

17 MARQUENIE, s. 325.

18 Art. 1–2 Police and Criminal Justice Directive.

19 MARQUENIE, s. 328.

20 MARQUENIE, s. 328.

21 CARUANA, Mireille M., 'The Reform Of The EU Data Protection Framework In The Context Of The Police And Criminal Justice Sector: Harmonisation, Scope, Oversight And Enforcement', International Review of Law, Computers & Technology, S. 33, 2017, s. 249-250.

22 CARUANA, s. 250.

created with legitimate and non-malicious intentions, they have nevertheless provided an environment in which illegal activities can expand[23]. Consequently, the Dark Web has become attractive to individuals engaged in unlawful conduct who seek to conceal their identities and locations.

A significant portion of activity on the Dark Web is associated with unlawful conduct. Although only about 1.5% of internet users accessing Tor (The Onion Router) are estimated to visit hidden services, this relatively small group generates a considerable volume of illicit traffic across tens of thousands of hidden sites[24]. As a result, the Dark Web provides an environment in which numerous criminal activities may occur[25]. Research conducted by Gareth Owen and Nick Savage indicates that material related to child exploitation accounts for a substantial share of traffic directed to hidden services on the network. In addition, drug trafficking represents another major form of illegal activity, with a large proportion of hidden websites dedicated to the sale of narcotics[26]. These developments highlight the growing need for law enforcement authorities to develop effective strategies to combat cybercrime within the Dark Web environment.

IV. CONTEMPORARY METHODS IN COMBATING CYBERCRIME ON THE DARK WEB

The prosecution of Ross Ulbricht, the creator of Silk Road (dark web marketplace), brought the Dark Web to wider public attention. Federal investigators eventually identified the platform's servers and obtained a warrant from local authorities to seize them[27]. During the trial, Ulbricht's defence argued that the investigation had violated his privacy rights, contending that the Federal Bureau of Investigation lacked lawful authority both to discover the servers and to examine the data stored on them[28]. Although the agency did not disclose the precise methods used to locate the servers, law enforcement officials maintained that Ulbricht's own operational mistakes enabled investigators to uncover the platform without resorting to unlawful or highly advanced techniques[29]. Ultimately, the court rejected the defence's objections regarding the legality of the investigation. While the operation succeeded in dismantling Silk Road, it did not eliminate demand for similar services. As noted by Michael Chertoff, the case failed to discourage continued use of the Dark Web; despite the criminal liability associated with operating such platforms, subsequent marketplaces—including Silk Road 2.0, Silk Road 3.0, and Sheep Marketplace—quickly emerged, demonstrating the persistence of this illicit ecosystem[30].

Another governmental approach to addressing crime on the Dark Web is the development of Memex (DARPA program). This search tool was created by the Defense Advanced Research Projects Agency to assist in identifying criminal activities within hidden online networks[31]. The system collects and indexes large volumes of data from web pages that are not accessible through conventional search engines. Rather than revealing the IP addresses of users on Tor (The Onion Router), Memex focuses on analysing online content and mapping connections between websites and actors[32]. Through this analytical approach, law enforcement authorities can better understand patterns of activity on the

23 CHERTOFF, Michael, 'A Public Policy Perspective Of The Dark Web', Journal of Cyber Policy, S. 2, 2017, s. 26-27.

24 WARD, Mark, 'Child Porn Tops Tor Hidden Site Visits' (*BBC News*, 2014) <https://www.bbc.co.uk/news/technology-30637010> accessed 23 December 2025.

25 OWEN, Gareth/SAVAGE, Nick, 'The Tor Dark Net' (*Centre for International Governance Innovation*, 2015) <https://www.cigionline.org/publications/tor-dark-net> accessed 26 December 2025.

26 OWEN/SAVAGE, 'The Tor Dark Net'.

27 HAASZ, Amanda, Underneath It All: Policing International Child Pornography On The Dark Web', Syracuse Journal of International Law and Commerce, S. 43, 2016, s. 353-354.

28 GREENBERG, Andy, "The FBI Finally Says How It 'Legally' Pinpointed Silk Road's Server' (*WIRED*, 2014) <https://www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/> accessed 21 December 2025.

29 VOGT, s. 117.

30 CHERTOFF, s. 35

31 CUTHBERTSON, Anthony, 'Death Of The Dark Web? DARPA\'S Memex Search Engine Allows Tor Tracking' (*International Business Times UK*, 2015) <https://www.ibtimes.co.uk/death-dark-web-darpas-memex-search-engine-allows-tor-tracking-1488124> accessed 20 December 2025.

32 CUTHBERTSON, 'Death Of The Dark Web.

network and detect potentially suspicious behaviour without broadly infringing upon the privacy rights of all users[33].

Another notable yet contentious investigative approach is the Network Investigative Technique (NIT), developed by H. D. Moore. NIT operates as a form of malware designed to de-anonymize users who access child exploitation websites on Tor (The Onion Router) [34]. In the high-profile Playpen case, the Federal Bureau of Investigation deployed NIT under a warrant issued by a federal magistrate, successfully taking down the site and identifying roughly 1,500 IP addresses of users worldwide who visited the platform[35]. As noted by Michael Chertoff, the method's effectiveness stemmed from its targeted nature: only users of the illicit site were identified, while other Tor users remained unaffected[36]. Consequently, individuals accessing illegal material on the Dark Web cannot assume anonymity, whereas users of Tor for lawful purposes retain their privacy unless they intentionally interact with illicit hidden services.

When evaluating these three approaches, the Network Investigative Technique (NIT) appears to be the most effective. The Silk Road investigation, for instance, demonstrated that traditional methods lacked a sustained deterrent effect on users. Although earlier approaches, such as server seizure and content indexing, produced some positive outcomes, they did not fully safeguard the privacy of individuals lawfully using Tor (The Onion Router). In contrast, NIT enables investigators to target only those engaging with illegal sites, thereby maximising protection for the privacy of other Tor users while still obtaining critical identifying information from offenders. Consequently, this method represents a more precise and rights-conscious strategy for law enforcement operations on the Dark Web.

V. CHALLENGES ABOUT USING NETWORK INVESTIGATIVE TECHNIQUE

While the Network Investigative Technique (NIT) has proven effective, its use has attracted significant criticism, primarily concerning three areas: the legal framework, international law, and national sovereignty. Although scholars generally agree that broad, cross-border cyber investigations by a single state may strain international relations and potentially contravene international law, there is less agreement on whether the targeted application of NIT specifically constitutes such violations[37]. Consequently, developing practical solutions to address these contested issues could help ensure the lawful and responsible deployment of NIT in future investigations.

From a legal framework perspective, gaps in regulation have complicated the proper conduct of NIT-based investigations. A notable controversy arose in the Playpen case regarding whether a federal magistrate in the Eastern District of Virginia had the authority to issue a search warrant extending beyond its territorial jurisdiction. In that instance, the magistrate authorized the Federal Bureau of Investigation to deploy NIT to access the computers of Playpen users located outside the district[38]. The FBI defended the warrant's validity by arguing that the site's server fell within the court's jurisdiction. However, of the nine courts that have considered evidence obtained through this method, only three have upheld the FBI's position[39]. As a result, despite the agency's success in dismantling a major child exploitation platform and identifying its users, most courts have deemed the operation legally problematic due to these regulatory shortcomings.

---

33 CUTHBERTSON, 'Death Of The Dark Web.

34 EASTTOM, Chuck, 'Conducting Investigations On The Dark Web', Journal of Information Warfare S. 17, 2018, s. 31-32.

35 COX, Joseph, 'The FBI's 'Unprecedented' Hacking Campaign Targeted Over A Thousand Computers' (*Vice*, 2019) <https://www.vice.com/en_us/article/qkj8vv/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers> accessed 29 December 2025.

36 CHERTOFF, s. 35.

37 KERRY, Orin S./MURPHY, Sean D., 'Government Hacking To Light The Dark Web: What Risks To International Relations And International Law?, Standford Law Rewiev Online, S. 70, 2017-2018, s. 58-59.

38 SATTERFIELD, Jamie, 'FBI Tactic In National Child Porn Sting Under Attack' (*usatoday*, 2016) <https://eu.usatoday.com/story/news/nation-now/2016/09/05/fbi-tactic-child-porn-sting-under-attack/89892954/> accessed 31 December 2025.

39 KERRY/ MURPHY, s. 59.

In light of the criticisms and judicial rulings discussed above, which effectively constrain NIT use to the physical jurisdiction of a federal magistrate court, legal reforms are necessary to allow the FBI to deploy NIT more reliably and efficiently. These challenges stem from the absence of explicit provisions in the United States' Federal Rules of Criminal Procedure, specifically Rule 41(b)(1), which governs search and seizure[40]. Consequently, courts have reached differing conclusions. For example, U.S. Magistrate Clifford Shirley ruled that the FBI's warrant process exceeded its legal authority and violated federal procedure rules, yet he admitted the evidence under the federal good-faith exception. This exception permits the use of evidence when law enforcement reasonably believes it is acting pursuant to a valid court order and no misconduct occurs[41]. The court's acceptance of this evidence underscores the need for clear statutory guidance regarding the FBI's use of NIT beyond the magistrate court's district or in cross-border contexts.

The jurisdictional limitation on search warrants under Rule 41 was addressed through an amendment. Specifically, Rule 41(b)(6) permits magistrates to issue a warrant for a device whose location is obscured by technological means, even if it ultimately appears to be outside the issuing district[42]. However, this amendment does not authorize U.S. courts to issue warrants for devices located abroad; it only allows investigations within the United States targeting devices whose physical location is hidden. As Ahmet Ghappour notes, this framework presumes that the target devices are situated within U.S. territory, yet approximately 80% of Dark Web devices are located internationally[43]. Consequently, while the amendment resolves jurisdictional challenges for domestic investigations, significant difficulties persist when attempting to conduct searches outside the United States.

When the digital target is located outside the United States, investigators must rely on cross-border evidence-gathering mechanisms. According to Ahmet Ghappour, the most established and least contested method in such situations is the Mutual Legal Assistance Treaty (MLAT) [44]. MLATs facilitate cooperation between law enforcement agencies, supporting ongoing investigations and prosecutions. These treaties typically govern procedures such as identifying persons and property, serving legal documents, executing search warrants, taking witness statements, summoning witnesses, and seizing assets[45]. In addition, federal authorities often exchange investigative information through informal networks designed to enhance interstate collaboration and streamline access to evidence[46]. The extraterritorial location of the evidence underscores the critical role of bilateral agreements and diplomatic relations in enabling law enforcement to obtain proof abroad.

Criminal use of the Dark Web complicates traditional evidence-gathering methods, as investigators often cannot determine the physical location of the targeted devices. In such cases, conventional procedures for obtaining evidence are ineffective, leaving law enforcement with NIT as the only viable option. The Network Investigative Technique allows investigators to access computers without prior knowledge of their geographic location[47]. However, this capability also amplifies the previously noted challenges related to international law and the sovereignty of other states.

International law imposes clear limits on a state's authority to issue search warrants or enforce laws beyond its own borders, and there is ongoing debate about whether the cross-border deployment of NIT falls within these constraints. This discussion arises from the principle that states cannot unilaterally exercise prescriptive, judicial, or enforcement

40 Fed. R. Crim. P. 41 - Search and Seizure.
41 Fed. R. Crim. P. 41 - Search and Seizure**.**
42 Fed. R. Crim. P. 41(b)(6).
43 GHAPPOUR, s. 1080
44 GHAPPOUR, s. 1092.
45 7 U.S. DEP'T OF STATE, FOREIGN AFFAIRS MANUAL § 962.1 (2013).
46 'Frequently Asked Questions Regarding Evidence Located Abroad' (*The United States Department of Justice*, 2015) <https://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-evidence-located-abroad> accessed 6 January 2025.
47 GHAPPOUR, s. 1093

powers over the territorial sovereignty of another state[48]. At the same time, international law allows a state to define conduct occurring outside its territory as criminal if that conduct produces effects within its jurisdiction[49]. Accordingly, it is generally accepted that states possess the authority to establish criminal liability under prescriptive law for acts that have an extraterritorial impact.

With respect to judicial and enforcement authority, international law imposes strict territorial limits. As Hannah L. Buxbaum observes, while a state's legislative or prescriptive powers are not strictly confined by geography, its capacity to enforce laws remains largely restricted to its own territory[50]. Similarly, Ahmet Ghappour notes that there is broad consensus among states that no country may exercise coercive authority within another state's borders without explicit consent. Consequently, conducting searches for evidence or arresting suspects inside a foreign state without that state's permission would constitute a violation of international law.

The cross-border deployment of NIT by investigators raises concerns under international law, as it may be viewed as an unauthorized intrusion into another state's territory, which traditionally requires the host state's consent. Ahmet Ghappour argues that the use of NIT in such contexts could conflict with the principle prohibiting interference in the jurisdiction of foreign states. However, his position has faced criticism for its lack of clarity[51]. Rather than asserting definitively that extraterritorial NIT operations violate international law, Ghappour contends that the introduction of NIT "begins to unravel" the established alignment between conventional evidence-gathering methods and international legal norms[52]. Scholars Orin S. Kerr and Sean D. Murphy have pointed out that the phrase "begins to unravel" is ambiguous, leaving Ghappour's argument open to interpretation[53]. The limited evidentiary support he provides regarding actual violations of international law further contributes to the uncertainty surrounding his position.

Nonetheless, Ghappour's argument aligns closely with the perspective that employing NIT to gather evidence in a foreign jurisdiction could potentially contravene international law. He particularly highlights the principle articulated in the American Law Institute's 1987 Restatement, which states that "a state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state" [54]. Ghappour also contends that applying existing domestic legal frameworks to investigations targeting anonymous actors creates awkward and inconsistent regulatory outcomes. While U.S. courts can issue warrants to deploy NIT within national borders, the use of NIT extraterritorially relies either on broad executive powers to enforce U.S. law or on statutory authority granted to the Department of Justice and Federal Bureau of Investigation to investigate violations of U.S. law[55]. According to Ghappour, this absence of explicit legal authority for cross-border NIT operations raises the possibility of conflicting with international law, though he stops short of asserting a definitive violation.

The principle articulated in the 1987 Restatement, which prohibits a state from conducting investigations or exercising law enforcement within the territory of another state without that state's consent, can be interpreted differently from Ghappour's reading. Orin S. Kerr and Sean D. Murphy argue that this prohibition likely applies to physical law enforcement operations rather than to electronic investigations, such as those involving Tor (The Onion Router), where

48 GOLDSMITH, Jack L., 'The Internet And The Abiding Significance Of Territorial Sovereignty', Indiana Journal of Global Legal Studies, S. 5, 1998, s. 475- 476

49 *UNITED STATES v ALUMINUM CO OF AMERICA et al* [1945] US Court of Appeals for the Second Circuit, 148 F2d (US Court of Appeals for the Second Circuit) 416, 443

50 BUXBAUM, Hannah, 'Territory, Territoriality, And The Resolution Of Jurisdictional Conflict', American Journal of Comparative Law, S. 57, 2008, s. 631-632.

51 GHAPPOUR, s. 1106.

52 GHAPPOUR, s. 1106.

53 KERRY/MURPHY, s. 66.

54 Restatement (Thırd) Of Foreign Relations Law Of The United States § 432(2) (Am. Law Inst. 1987).

55 GHAPPOUR, s. 1106.

no physical presence in the foreign state occurs. Their interpretation is grounded in the 1987 Restatement reporters' notes, which illustrate the rule exclusively through examples of physical entry into another country[56]. In the absence of contrary practice, this reading appears logical and reasonable, as it reflects the original lawmakers' intent and the manner in which the rule is applied both domestically and internationally.

Under the assumption that the 1987 Restatement extends beyond mere physical entry into another state's territory, questions arise regarding its applicability in today's technologically advanced environment. Modern law enforcement agencies frequently conduct investigations through international communications or by accessing websites hosted abroad, often without obtaining explicit consent from the foreign states involved. Orin S. Kerr and Sean D. Murphy argue that, because the 1987 rule was drafted before the development of the internet, its direct application to contemporary digital investigations is problematic, and they contend that Ghappour's analysis does not fully account for these limitations[57]. Nevertheless, contrary to their assertion, Ghappour does not claim that U.S. authorities may arbitrarily collect evidence outside their territory; he merely describes how such practices are currently conducted in the United States. Indeed, these considerations highlight the urgent need for updated legal frameworks that align with modern technological realities, ensuring that investigative methods are both effective and compliant with domestic and international law.

Debates regarding cross-border investigations also extend into the realm of international customary law. According to Ahmet Ghappour, there is a general agreement among scholars that conducting operations across borders without consent may constitute an internationally wrongful act, entitling the targeted state to respond with countermeasures under customary international law. Ghappour cites several cases to illustrate this point[58]. For example, in 2002, Russian authorities accused an FBI agent of violating domestic laws on intrusion and espionage after accessing a computer located in Russia and collecting data[59]. Similarly, in 2014, U.S. officials charged members of the Chinese military under U.S. economic espionage statutes for extracting intellectual property from the U.S. military[60]. These instances demonstrate that individual states can criminalize cross-border cyber activities within their own legal frameworks. Nevertheless, as these examples show, actions considered criminal by one state may, in practice, be cross-border cyber operations undertaken for purposes other than crime prevention.

When viewed as a dynamic system, international customary law evolves in response to the changing cultural and technological contexts of states. In this regard, Orin S. Kerr and Sean D. Murphy argue that customary international law cannot be considered in isolation from state practice; rather, it adapts and takes shape through the actions of governments[61]. They further suggest that the principle articulated in the 1987 Restatement has effectively been extended to the contemporary use of NITs. In practice, governments typically employ NITs in TOR investigations to determine the location of a user before seeking consent from the relevant foreign authority for further action. However, when TOR is used to conceal a user's location, applying the 1987 rule becomes problematic: it is unclear from which state permission must be obtained, rendering the deployment of NIT effectively unfeasible under a strict reading of the rule.

The deployment of NIT plays a crucial role in identifying suspects who conceal their location using Tor (The Onion Router), and consequently in determining the appropriate state from which consent must be obtained. While Ahmet Ghappour raises legitimate concerns that cross-border use of NIT could, in some circumstances, conflict

56 KERRY/MURPHY, s. 66.

57 KERRY/MURPHY, s. 66.

58 GHAPPOUR, s. 1084

59 BRUNKER, Mike, 'FBI Agent Charged With Hacking' (*nbcnews.com*, 2013) <http://www.nbcnews.com/id/3078784#.XiRGwoj7TDc> accessed 19 January 2025.

60 'U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage' (*Justice.gov*, 2020) <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> accessed 19 January 2025.

61 KERRY/MURPHY, s. 68.

with international law, he also emphasizes the need for regulatory measures to facilitate its responsible use. As Orin S. Kerr and Sean D. Murphy note, employing NIT solely to identify the jurisdiction from which permission should be requested does not, in itself, constitute a violation of international law. Therefore, by addressing legal gaps and enhancing intergovernmental cooperation, it is possible to ensure that NIT operations remain consistent with international legal standards while maintaining investigative effectiveness.

CONCLUSION

This study has examined the effectiveness and limitations of the European Convention on Cybercrime as the principal international legal instrument governing cybercrime enforcement, with a particular focus on Dark Web activities, data privacy concerns, and contemporary investigative powers. The analysis demonstrates that, although the Convention has played a pioneering role in harmonising legal standards and fostering international cooperation, it falls short of adequately addressing the complex challenges posed by rapidly evolving digital technologies and anonymisation tools

The findings indicate that the Convention establishes a necessary procedural framework through provisions on data preservation, search and seizure, interception of communications, and mutual legal assistance. These mechanisms have significantly contributed to facilitating cross-border investigations and enhancing cooperation among states. However, the study also reveals that these provisions are formulated in broad and sometimes ambiguous terms, which may lead to inconsistent application and insufficient protection of fundamental rights. In particular, the Convention's approach to data privacy remains limited, as it relies primarily on general safeguard clauses rather than detailed and enforceable standards. As a result, it does not fully reflect the growing importance of personal data protection within contemporary human rights law, especially when compared to more recent regulatory instruments.

Moreover, the study highlights that the Dark Web constitutes a distinct and challenging environment for law enforcement authorities. Its inherent anonymity and decentralised structure significantly impede traditional investigative techniques, making it difficult to identify offenders and determine jurisdiction. In this context, the analysis of cases such as Silk Road and Playpen demonstrates both the necessity and the effectiveness of advanced investigative tools. Among these, the Network Investigative Technique (NIT) emerges as a particularly effective method, as it enables targeted identification of offenders while minimising unnecessary interference with the privacy of lawful users. Nevertheless, the use of such techniques raises substantial legal concerns, particularly with respect to jurisdictional limits, the principle of state sovereignty, and compliance with international law.

The study further demonstrates that the absence of clear and harmonised rules governing cross-border digital investigations creates significant legal uncertainty. Divergent judicial interpretations, especially in the context of United States practice, illustrate the difficulties in reconciling domestic procedural rules with the transnational nature of cybercrime. While mechanisms such as mutual legal assistance treaties provide an established basis for cooperation, they often prove inadequate in addressing the speed and technical complexity of cyber investigations conducted on the Dark Web. At the same time, unilateral cross-border investigative actions risk conflicting with fundamental principles of international law, particularly the prohibition on exercising enforcement jurisdiction within another state's territory without consent.

In light of these findings, this study concludes that the current framework of the Convention, while indispensable, is not fully equipped to respond to the demands of modern cybercrime enforcement. There is a clear need for the development of more precise and technologically informed legal standards, particularly concerning the use of advanced investigative techniques such as NIT and the regulation of cross-border evidence-gathering. In addition, stronger and more explicit safeguards are required to ensure that the exercise of investigative powers remains consistent with the protection of fundamental rights, especially the right to privacy.

Ultimately, combating cybercrime on the Dark Web requires a more coherent, adaptive, and balanced international legal framework. Such a framework should enhance the effectiveness of law enforcement while simultaneously safeguarding individual rights and respecting state sovereignty. Strengthening and potentially updating the European Convention on Cybercrime in line with contemporary technological realities will be essential to achieving a sustainable and legitimate system of cybercrime governance in the digital age.

Author's Declaration

Financial Support: Authors has not received any financial support for the research, authorship, or publication of this study.

The Declaration of Conflict of Interest / Common Interest: No conflict of interest or common interest has been declared by the author.

The Declaration of Ethics Committee Approval: The study doesn't need any ethics committee approval or any special permission.

The Declaration of Research and Publication Ethics: The author declares that heshe complies with the scientific, ethical, and quotation rules of InULR in all processes of the paper and that heshe does not make any falsification of the data collected. In addition, heshe declares that Inonu University Law Review and its editorial board have no responsibility for any ethical violations that may be encountered, and that this study has not been evaluated or published in any academic publication environment other than Inonu University Law Review.

Kaynakça

Police and Criminal Justice Directive, Directive (EU) 2016/680.

Restatement (Thırd) of Foreıgn Relatıons Law Of The Unıted States § 432(2) (Am. Law Inst. 1987).

U.S. Dept. Of State, Foreıgn Affaırs Manual § 962.1 (2013).

Federal Rules of Criminal Procedure*, Effective March 21, 1946, as amended to December 1, 2013.*

EU Charter of Fundamental Rights, OJ, C 364/10, 18.12.2000; European Convention of Human Rights, www.echr.coe.int.

Council of Europe Convention on Cybercrime. Budapest, 23/11/2001.

ALİUSTA, Cahit/BENZER, Recep, 'Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci', Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C. 4, No:2, S:35-- 42, 2018.

BARON, Ryan M F, 'A Critique of the International Cybercrime Treaty', Common Law Conspectus, S.10, 2002.

BUXBAUM, Hannah, 'Territory, Territoriality, And The Resolution Of Jurisdictional Conflict', American Journal of Comparative Law, S. 57, 2008.

CARUANA, Mireille M., 'The Reform Of The EU Data Protection Framework In The Context Of The Police And Criminal Justice Sector: Harmonisation, Scope, Oversight And Enforcement', International Review of Law, Computers & Technology, S. 33, 2017.

CHERTOFF, Michael, 'A Public Policy Perspective Of The Dark Web', Journal of Cyber Policy, S. 2, 2017.

EASTTOM, Chuck, 'Conducting Investigations On The Dark Web', Journal of Information Warfare S. 17, 2018.

GHAPPOUR, Ahmed, 'Searching Places Unknown: Law Enforcement Jurisdiction On The Dark Web' Stanford Law Review, S. 69, 2017.

GOLDSMITH, Jack L., 'The Internet And The Abiding Significance Of Territorial Sovereignty', Indiana Journal of Global Legal Studies, S. 5, 1998.

HAASZ, Amanda, Underneath It All: Policing International Child Pornography On The Dark Web', Syracuse Journal of International Law and Commerce, S. 43, 2016.

Internet Alliance Comments On Council Of Europe's Draft Convention On Cyber-Crime No. 19' (*Center for Democracy &Technology*, 2000) <https://old.cdt.org/international/cybercrime/001000ia.shtml> accessed 1 January 2025.

KERRY, Orin S./MURPHY, Sean D., 'Government Hacking To Light The Dark Web: What Risks To International Relations And International Law?, Standford Law Rewiev Online, S. 70, 2017-2018.

MARQUENIE, Thomas, 'The Police And Criminal Justice Authorities Directive: Data Protection Standards And Impact On The Legal Framework', Computer Law & Security Review, S. 33, 2017.

OWEN, Gareth/SAVAGE, Nick, 'The Tor Dark Net' (Centre for International Governance Innovation, 2015) <https://www.cigionline.org/publications/tor-dark-net> accessed 26 December 2025.

POUNDER, Chris, 'The Council Of Europe Cyber-Crime Convention', Computers & Security, S. 20 (5), 2001.

UNITED STATES v ALUMINUM CO OF AMERICA et al [1945] US Court of Appeals for the Second Circuit, 148 F2d (US Court of Appeals for the Second Circuit) 416.

VOGT, Sophia Dastagir, 'The Digital Underworld: Combating Crime On The Dark Web In The Modern Era', Santa Clara Journal of International Law, S. 15, 2017.

WEBER, Amalie M, 'The Council of Europe's Convention on Cybercrime', Berkeley Technology Law Journal & Berkeley Center for Law and Technology, S. 18, 2003.

BRUNKER, Mike, 'FBI Agent Charged With Hacking' (*nbcnews.com*, 2013) <http://www.nbcnews.com/id/3078784#.XiRGwoj7TDc> accessed 19 January 2025.

COX, Joseph, 'The FBI's 'Unprecedented' Hacking Campaign Targeted Over A Thousand Computers' (*Vice*, 2019) <https://www.vice.com/en_us/article/qkj8vv/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers> accessed 29 December 2025.

CUTHBERTSON, Anthony, 'Death Of The Dark Web? DARPA\'S Memex Search Engine Allows Tor Tracking' (*International Business Times UK*, 2015) <https://www.ibtimes.co.uk/death-dark-web-darpas-memex-search-engine-allows-tor-tracking-1488124> accessed 20 December 2025.

GREENBERG, Andy, 'The FBI Finally Says How It 'Legally' Pinpointed Silk Road's Server' (*WIRED*, 2014) <https://www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/> accessed 21 December 2025.

SATTERFIELD, Jamie, 'FBI Tactic In National Child Porn Sting Under Attack' (*usatoday*, 2016) <https://eu.usatoday.com/story/news/nation-now/2016/09/05/fbi-tactic-child-porn-sting-under-attack/89892954/> accessed 31 December 2025.

'U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage' (*Justice.gov*, 2020) <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage against-us-corporations-and-labor> accessed 19 January 2025.

WARD, Mark, 'Child Porn Tops Tor Hidden Site Visits' (*BBC News*, 2014) <https://www.bbc.co.uk/news/technology-30637010> accessed 23 December 2025.