Погорецький М. А.,
доктор юридичних наук, професор,
проректор з науково-педагогічної роботи
Київського національного університету імені Тараса Шевченка
ORCID ID: *0000–0003–0936–0929*

Лисаченко Є. І.,
доктор філософії, адвокат
ORCID ID: *0000–0003–0937–2110*

DOI: *https://doi.org/10.17721/2413-5372.2023.1-2/54-73*

УДК 343.14

ВСТАНОВЛЕННЯ ДОСТОВІРНОСТІ ЦИФРОВИХ ДОКАЗІВ МІЖНАРОДНИМ КРИМІНАЛЬНИМ СУДОМ: ОКРЕМІ ПРОБЛЕМНІ ПИТАННЯ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Анотація. *Стаття присвячена дослідженню деяких проблемних питань оцінки цифрових доказів під час розгляду справ Міжнародним кримінальним судом.*

Авторами зазначено, що у цифрову епоху нові технології та розвиток обчислювальних потужностей змінили характер потенційно релевантних доказів, які оцінюються в міжнародному кримінальному праві. Міжнародний кримінальний суд наразі має ряд проблемних питань у правозастосовній практиці під час оцінки цифрових доказів, а саме визначення достовірності вказаного виду доказів.

Метою статті визначено: (1) окреслення викликів та небезпеки поточного підходу МКС до встановлення достовірності цифрових доказів; (2) дослідження наукових підходів щодо оцінки цифрових доказів у кримінальному судочинстві; та (3) необхідність встановлення найбільш прагматичного підходу до визначення достовірності цифрових доказів у майбутньому.

У статті окреслено виклики та небезпеки поточного підходу МКС до автентифікації та верифікації цифрових доказів, досліджено дискусії серед науковців щодо окресленої проблематики, а також визначено рекомендації щодо покращення роботи Суду та його можливостей перевірки достовірності цифрових доказів.

Визначено загальний підхід МКС до прийнятності доказів, який передбачає послідовний трискладовий тест, в якому кожен з наведених нижче критеріїв має бути виконаний: 1) належність: Відповідно до статей 64(9)(a) та 69(4) Римського статуту, а також Правил процедури та залучення доказів, докази вважаються належними, якщо «надані докази роблять існування факту, що розглядається, більш-менш вірогідним». Іншими словами, докази можуть вважатися належними, якщо вони «prima facie» («на перший погляд») стосуються справи; 2) достатність: Під доказовою цінністю зазвичай розуміють те, чи є доказ достатньо корисним для доведення важливої частини судового процесу. По суті, доказова цінність вимірює ступінь, до якого запропонований доказ може вплинути на встановлення факту або питання. Суд повинен збалансувати доказову цінність предмета з його шкідливим впливом на обвинувачених; 3) зважування доказової цінності та преюдиціального ефекту: Відповідно до Правил 69(4) та 63(2), надані докази повинні бути «достатньо доречними та доказовими, щоб переважати будь-який преюдиціальний вплив або ефект, який може спричинити їх прийняття». Іншими словами, вага, що надається доказам, повинна повністю поважати права

всіх сторін і не бути явно несправедливою щодо сторони обвинувачення чи захисту, а також не завдавати шкоди загальній справедливості судового розгляду.

Зроблено висновок, що для подальшої ефективної роботи необхідно: (1) призначити Групу користувачів електронного суду для керівництва зусиллями з удосконалення алгоритмів і постійного розвитку питань автентифікації; (2) розширити технологічну консультативну роль Науково-консультативної ради; (3) створити регулярні тренінги та семінари для підвищення технічної компетентності суддів; і (4) підвищити прозорість діяльності Науково-консультативної ради та Групи користувачів електронного суду.

Ключові слова: *Міжнародний кримінальний суд, докази, доказування, автентифікація, достовірні докази.*

Постановка проблеми. У цифрову епоху нові технології та розвиток обчислювальних потужностей змінили те, як потенційно релевантні докази будуть оцінюватися в міжнародному кримінальному праві. Нові технології уможливлюють агрегування даних, пов'язаних зі збройним конфліктом, з широкого кола джерел, зокрема, супутникових і геопросторових зображень, систем глобального позиціонування (GPS), даних мобільних телефонів, відео, фотографій, соціальних мереж та інших інтернет-джерел[1]. Міжнародний кримінальний суд («МКС» або «Суд») наразі стикнувся з викликами, пов'язаними з визначенням достовірності цифрових доказів, які набувають все більшого значення, і намагається адаптуватися до цих змін.

МКС є першим у світі постійно діючим міжнародним кримінальним судом, який займається розслідуванням і судовим переслідуванням найтяжчих злочинів, що викликають занепокоєння міжнародної спільноти: геноциду, злочинів проти людяності, воєнних злочинів, тощо. На момент створення МКС, можливо, не можна було передбачити майбутню революцію в цифрових технологіях та її вплив на діяльність Суду. Однак понад два десятиліття потому доказові процедури Суду та процеси судового перегляду для перевірки достовірності доказів не відповідають вимогам сучасності. Хоча нові технології багато в чому обіцяють трансформувати судовий процес, пов'язаний з міжнародними злочинами, Суд наразі недостатньо підготовлений до виконання складного завдання автентифікації та перевірки цифрових доказів[2], що і обумовлює актуальність обраної теми дослідження.

Аналіз останніх наукових досліджень та публікацій. Окремі теоретичні та практичні питання оцінки доказів у кримінальному судочинстві були предметом наукових пошуків таких вчених, як: Ю.П. Аленіна, І.В. Гловюк, В.О. Гринюка, І.Г. Івасюка, І.Г. Каланчі, О.В. Капліної, Ю.Ю. Орлова, А.І. Палюха, І.Г. Рогатюка, С.В. Свириденка, Д.Б. Сергєєвої, Х.Р. Слюсарчук, І.А. Смаль, О.С. Старенького, А.В. Столітнього, О.Ю. Татарова, А.Р. Туманянц, О.В. Фараон, В.І. Фаринника, В.Г. Хахановського, Д.М. Цехана, М.Ю. Черкова, С.С. Чернявського, А.В. Шевчишена, Л.В. Юрченко та інших. Низка робіт вказаних та інших авторів присвячена, зокрема, проблемам злочинів в кіберпросторі та їх доказуванню[3]. Вказані

[1] Koenig, Alexa, Emma Irving, Yvonne McDermott, and Daragh Murray, New Technologies and the Investigation of International Crimes: An Introduction (2021) 19 (1): 1–7 *Journal of International Criminal Justice* 14–21 <https://doi.org/10.1093/jicj/mqab040> accessed 23.04.2023.

[2] Koenig, Alexa, Emma Irving, Yvonne McDermott, and Daragh Murray, New Technologies and the Investigation of International Crimes: An Introduction (2021) 19 (1): 1–7 *Journal of International Criminal Justice* 14-21 <https://doi.org/10.1093/jicj/mqab040> accessed 23.04.2023.

[3] М А Погорецький, В П Шеломенцев, Поняття кіберпростору як середовища вчення злочину (2009) 2 (2) *Інформаційна безпека людини, суспільства, держави* 77–81; М А Погорецький, В П Шеломенцев, Кіберзлочини: до визначення поняття (2012) 8 *Вісник прокуратури* 89–96; І А Смаль, Проблемні аспекти застосування електронних доказів у кримінальному судочинстві (2021) 4 *Науковий журнал «Право і суспільств»* 226–232; С С Чернявський, Ю Ю Орлов, Електронне відображення як джерело доказів у кримінальному провадженні (2017) 2 *Вісник кримінального судочинства* 112–124; Використання електронних (цифро-

вчені зробили значний внесок у дослідження доказів у кримінальному судочинстві України і, зокрема, визначенню достовірності електронних доказів у кримінальному провадженні. Проте, міжнародні аспекти встановлення достовірності цифрових доказів, зокрема Міжнародним кримінальним судом, було досліджено не в повній мірі, що обумовлює необхідність проведення більш ґрунтовного аналізу окресленої проблематики.

Слід зазначити, що міжнародні суди, такі як МКС, вже давно намагаються оцінювати складні сфери, що знаходяться поза межами їхньої компетенції, включаючи, зокрема, криміналістику, балістику, ДНК тощо[1]. Належний рівень судового контролю, який повинен здійснюватися в таких справах, залишається важливим питанням. Тому **метою цієї статті є:** (1) окреслити виклики та небезпеки поточного підходу МКС до встановлення достовірності цифрових доказів; (2) дослідити наукові підходи щодо автентифікації цифрових доказів у кримінальному судочинстві; та (3) визначити найбільш прагматичний підхід до визначення достовірності цифрових доказів у майбутньому.

Виклад матеріалу дослідження та його основні результати. Незважаючи на існування значної кількості проблемних питань, пов'язаних із поданням цифрових доказів до Суду, насамперед, з їх подальшою оцінкою, основна увага в статті буде зосереджена на визначенні достовірності цифрових доказів. Вважаємо за доцільне в межах запропонованого наукового дослідження розглянути прагматичні питання щодо того, як палатам Суду слід починати підходити до визначення достовірності та перевірки цифрових доказів. Адже, по-перше, існують негайні та серйозні заходи, яких Суд може і повинен вжити для вдосконалення своїх процедур перевірки достовірності цифрових файлів. По-друге, хоча МКС ще не доводилося вирішувати справу, в якій цифрові докази відіграють центральну роль, це, безсумнівно, станеться в найближчому майбутньому.

Хоча нові технології багатообіцяюче трансформують судовий процес, пов'язаний з міжнародними злочинами, Суд наразі немає єдності правозастосовної практики при виконанні складного завдання з визначення достовірності та перевірки цифрових доказів.

У контексті окресленої проблематики важливо пояснити терміни, які будуть використані нами під час наукового дослідження.

Цифровий доказ (в англомовних джерелах використовується термін «digital evidence»): а) дані, які можуть підтвердити факт скоєння злочину або можуть встановити зв'язок між злочином та його жертвою або злочином та особою, яка його вчинила (Eoghan Casey); цифрові дані, які підтверджують або спростовують гіпотезу про настання цифрових подій або про стан цифрових даних (Brian Carrier)[2]; б) інформація, що зберігається або передається в бінарній формі і яку можна використати в суді (визначення, запропоноване Міжнародною організацією комп'ютерних доказів)[3]. Слід зазначити, що в доктрині кримінального процесуального права України відсутня єдність підходів до визначення поняття досліджуваного виду доказів. Так, наявна дискусія щодо обрання найбільш точної назви таких доказів (пропонуються такі

вих) доказів у кримінальних провадженнях, метод. реком / за заг. ред. О В Корнейка. Вид. 2-ге, доп. (Київ, Вид-во Нац. акад. внутр. справ, 2020) 104; А В Столітній, І Г Каланча, Формування інституту електронних доказів у кримінальному процесі України (2019) 146 *Проблеми законності* 179–191.

[1] The Human Rights Center at the University of California, Berkeley, School of Law. 2012. "Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court." Workshop Report. <https://www.law.berkeley.edu/files/HRC/HRC_Beyond_Reasonable_Doubt_FINAL.pdf> accessed 23.04.2023.

[2] Digital evidence and computer crime: forensic science, computers and the internet / by Eoghan Casey; with contributions from Susan W. Brenner … [et al.]. 3rd ed. London: Elsevier. 837 <https://booksite.elsevier.com/9780123742681> accessed 24.04.2023.

[3] Там само.

назви, як «електронні докази», «електронно-цифрові докази», «комп'ютерні докази», «цифрові докази», «електронні відображення та ін.). Зважаючи на обмежений обсяг статті, визначення поняття та видів доказів у кримінальному процесуальному праві України не буде предметом нашого наукового дослідження. З огляду на зазначене та проведене нами дослідження саме англомовних джерел, в рамках цієї наукової статті вважаємо за необхідне використовувати термін «цифрові докази», що, на наш погляд, є найбільш релевантним до терміну «digital evidence», який використовується у правозастосовній практиці Міжнародного кримінального суду.

Автентифікація – це юридичний термін, який використовується як у сфері кібербезпеки, так і для опису процесу доведення того, що цифровий файл є справжнім, а не підробленим. По суті, автентифікація гарантує, що об'єкт, про який йде мова, є саме тим, за що він видається, і не піддавався маніпуляціям або змінам[1].

Верифікація – це процес забезпечення надійності та/або правдивості твердження або заяви в певному засобі комунікації[2].

Верифікація та автентифікація тісно пов'язані між собою, але відрізняються один від одного. Наприклад, автентичний цифровий файл може бути як правдивим, так і неправдивим; однак неавтентичний доказ слід вважати таким, що не підлягає перевірці, оскільки було встановлено, що цей цифровий файл був підроблений, маніпульований або змінений.

У МКС судді мають широкі повноваження приймати докази на власний розсуд. Римський статут (далі – «Статут») є основоположним договором МКС і слугує керівним правовим документом Суду. Правила процедури та залучення доказів, що додаються до Статуту, містять додаткові деталі щодо допуску доказів та поводження з ними. Правило 63(2) зазначає: «Палата має право, відповідно до дискреційних повноважень, описаних у пункті 9 статті 64, вільно оцінювати всі подані докази з метою визначення їх належності або допустимості відповідно до статті 69»[3]. Іншими словами, судді мають право вирішувати будь-які питання, що виникають щодо автентичності або можливості перевірки цифрових доказів. Суд значною мірою покладається на розсуд і досвід суддів, щоб належним чином зважити прийняті докази. Такий гнучкий підхід до прийняття доказів також є наслідком обмеженості повноважень МКС. На відміну від національних кримінальних розслідувань, де правоохоронні органи можуть застосувати примус, наприклад, за допомогою приводу, отримання ордерів на обшук тощо, слідчі групи МКС не мають таких повноважень[4].

Загальний підхід МКС до прийнятності доказів передбачає послідовний трискладовий тест[5], в якому кожен з наведених нижче критеріїв має бути виконаний:

–Належність: Відповідно до статей 64(9)(а) та 69(4) Римського статуту, а також Правил процедури та залучення доказів, докази вважаються належними, якщо «надані докази роблять існування факту, що розглядається, більш-менш вірогідним»[6]. Іншими словами, докази можуть вважатися належними, якщо вони

[1] S Dubberley, A Koenig and D Murray, Introduction: The Emergence of Digital Witnesses. In Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1st ed. (Oxford, United Kingdom: Oxford University Press, 2020) 3–11.

[2] Там само

[3] Rules of Procedure and Evidence. ICC, Rule 63(2) <https://www.icc-cpi.int/sites/default/files/Publications/Rules-of-Procedure-and-Evidence.pdf> accessed 24.04.2023.

[4] L Freeman, Lindsay. 2020. Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court. In Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1st ed. (Oxford, United Kingdom, Oxford University Press, 2020) 48–67.

[5] N Mehandru and A Koenig, n.d. Open Source Evidence and the International Criminal Court (2019) *Harvard Human Rights Journal* <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/> accessed 24.04.2023.

[6] Case Prosecutor v. Germain Katanga. Trial Chamber II. Judgment pursuant to article 74 of the Statute. ICC-

«prima facie» («на перший погляд») стосуються справи[1].

–Достатність: Під доказовою цінністю зазвичай розуміють те, чи є доказ достатньо корисним для доведення важливої частини судового процесу[2]. По суті, доказова цінність вимірює ступінь, до якого запропонований доказ може вплинути на встановлення факту або питання[3]. Відповідно до статті 69(4) Статуту, доказова сила предмета повинна бути оцінена до того, як він може бути прийнятий як доказ[4]. Не існує вичерпного переліку критеріїв, за якими оцінюється доказова цінність. Натомість, «доказова сила визначається на основі низки міркувань, що стосуються невід'ємних характеристик доказів»[5]. Таким чином, Суд повинен збалансувати доказову цінність предмета з його шкідливим впливом на обвинувачених[6].

–Зважування доказової цінності та преюдиціального ефекту: Відповідно до Правил 69(4) та 63(2), надані докази повинні бути «достатньо доречними та доказовими, щоб переважати будь-який преюдиціальний вплив або ефект, який може спричинити їх прийняття»[7]. Іншими словами, вага, що надається доказам, повинна повністю поважати права всіх сторін і не бути явно несправедливою щодо сторони обвинувачення чи захисту, а також не завдавати шкоди загальній справедливості судового розгляду[8].

У центрі уваги цієї статті – механізми та виклики автентифікації цифрових доказів і відповідні процеси судового розгляду. Однак концепції верифікації та автентичності можуть заплутатися, коли судді починають приймати рішення про допустимість, релевантність, доказову цінність та вагу цифрових доказів.

Однією з ключових причин зближення автентичності та верифікації є гнучкий підхід МКС до допустимості доказів. У той час як Римський статут намагається збалансувати традиції романо-германського (кодифікований правовий кодекс) і загального права (некодифіковане і залежне від правових прецедентів) у своїй концепції справедливого судового розгляду та належної правової процедури, Суд значною мірою спирається на підхід системи романо-германського права до процедури доказування[9]. Романо-германська правова традиція, а отже, і МКС, віддає перевагу системі «максимальної гнучкості» з дуже невеликою кількістю обмежень щодо видів доказів, які можуть бути прийняті[10]. У МКС немає суду присяжних. На противагу цьому, традиція загального права покладається на систе-

01/04-01/07. (2014) <https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/KatangaEng.pdf> accessed 24.04.2023.

[1] *Prosecutor v. Thomas Lubanga Dyilo*. Trial Chamber I, Decision on the admissibility of four documents. ICC-01/04-01/06-1399. (2008) 27-32 < https://www.icc-cpi.int/node/29611> accessed 24.04.2023.

[2] Wex. n.d. Pobative Value. Wex Legal Information Institute (LII), Cornell Law School <https://www.law.cornell.edu/wex/probative_value> accessed 24.04.2023.

[3] N Mehandru and A Koenig, Open Source Evidence and the International Criminal Court (2019) *Harvard Human Rights Journal* <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/> accessed 24.04.2023.

[4] Rome Statute, Art 69(4).

[5] Case Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui. Trial Chamber II. Decision on the Prosecutor's Bar Table Motions. ICC-01/04–01/07. (2010) 13 https://www.icc-cpi.int/court-record/icc-01/04–01/07–717 >

[6] Judgment pursuant to article 74 of the Statute. ICC-01/04-01/07. (2014) 11 < https://www.icc-cpi.int/court-record/icc-01/04-01/06-2842 > accessed 24.04.2023.

[7] Case Prosecutor v. Jean-Pierre Bemba Gombo. Trial Chamber III. Decision on the admission into evidence of items deferred in the Chamber's 'Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute. ICC-01/05-01/08. (2013) 13 < https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/ BembaEng.pdf > accessed 24.04.2023.

[8] B Krzan, Admissibility of Evidence and International Criminal Justice (2021) 7 (1) *Revista Brasileira de Direito Processual Penal* 161 <https://doi.org/10.22197/rbdpp.v7i1.492> accessed 24.04.2023.

[9] J D Jackson and J S Sarah (eds.), The Common Law Tradition. In *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*. Law in Context. (Cambridge, Cambridge University Press, 2012) 30-36 <https://doi.org/10.1017/CBO9781139093606.005> accessed 24.04.2023.

[10] B Krzan, Admissibility of Evidence and International Criminal Justice (2021) 7 (1) *Revista Brasileira de Direito Processual Penal* 161 <https://doi.org/10.22197/rbdpp.v7i1.492> accessed 24.04.2023.

му присяжних, де члени суду присяжних не повинні бути експертами в галузі права, а це означає, що є вагомі підстави обмежувати тип доказів, які допускаються до розгляду, через побоювання, що деякі з них можуть завдати надмірної шкоди обвинуваченій стороні або сторонам[1]. Це не той підхід, якого дотримується МКС. Замість цього сторони подають запропоновані докази до Палати, а потім суддя розглядає прийнятність доказів. Якщо докази прийняті, суддя несе відповідальність за належну оцінку доказів, встановлення фактів у справі та застосування відповідного правового кодексу[2].

На практиці цей гнучкий стандарт прийнятності означає, що більшість доказів, які навіть віддалено стосуються справи, ймовірно, будуть прийняті[3]. Наприклад, у справі «Прокурор проти Жан-П'єра Бемба Гомбо» (Prosecutor v. Jean-Pierre Bemba Gombo), Офіс прокурора надав десять аудіозаписів радіопередач для встановлення передісторії та контексту конфлікту. Коли захист висунув заперечення проти допуску цих записів, Палата постановила, що «записи, які не були автентифіковані в суді, все ще можуть бути допущені, оскільки автентифікація в суді є лише одним із факторів, які Палата повинна враховувати при визначенні автентичності та доказової цінності об'єкта»[4]. Однак визначення допустимості будь-якого доказу не впливає на доказову силу, яку Палата надає цьому доказу[5]. Доказова сила – це відносна важливість, яка надається прийнятому доказу при вирішенні питання про те, чи було доведено певне питання, чи ні. Таким чином, на відміну від доказової сили, достатність доказів оцінюється суддями наприкінці судового розгляду, після заслуховування всієї сукупності доказів, допущених у справі[6]. Враховуючи гнучкий підхід Суду до доказів, визначення достовірності доказів в кінцевому підсумку залишається на розсуд суддів. Це стає проблематичним при оцінці цифрових доказів.

У справі «Прокурор проти Жан-П'єра Бемба Гомбо» (Prosecutor v. Jean-Pierre Bemba Gombo) МКС підтвердив, що судді не зобов'язані виносити окремі рішення щодо достовірності представлених доказів[7]. Основною аргументацією Палати у цій справі було сприяння справедливому та швидкому судовому розгляду, як того вимагає стаття 64(2) Статуту[8]. Якщо предмети, що подаються на розгляд, на перший погляд є достатньо автентичними або надійними, цього достатньо для того, щоб предмет був прийнятий[9]. Однак, якщо між сторонами виникають розбіжності, автентичність доказів має бути перевірена[10].

Відповідно до Регламенту Суду 26, Суд розпорядився створити «надійну, безпечну, ефективну електронну систему, яка підтримує його повсякденне судове та оперативне управління, а також провадження у справах»[11]. Згодом було створено Єдиний технічний протокол або («Протокол електронного суду» або

[1] J D Jackson and J S Sarah (eds.), The Common Law Tradition. In *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*. Law in Context. (Cambridge, Cambridge University Press, 2012) 30-36 <https://doi.org/10.1017/CBO9781139093606.005> accessed 24.04.2023.

[2] Apple, James G. and Deyling, Robert P. 1995. *A Primer on the Civil-Law System*. Washington, D.C.: Federal Judicial Center. < https://famguardian.org/PublishedAuthors/Govt/FJC/CivilLaw.pdf

[3] B Krzan, Admissibility of Evidence and International Criminal Justice (2021) 7 (1) *Revista Brasileira de Direito Processual Penal* 161 <https://doi.org/10.22197/rbdpp.v7i1.492> accessed 24.04.2023.

[4] Case Prosecutor v. Jean-Pierre Bemba Gombo. Trial Chamber III. Decision on the admission into evidence of materials contained in the prosecution's list of evidence. ICC-01/05–01/08. (2010) 17.

[5] Там само, 17.

[6] Там само, 17.

[7] Там само, 9.

[8] Там само, 9.

[9] A Ashouri, B Caleb and W Cherrie, An Overview of the Use of Digital Evidence in International Criminal Courts (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115–27 <https://doi.org/10.14296/deeslr.v11i0.2130> accessed 26.04.2023.

[10] Там само.

[11] Regulations of the Court. Regulation 26. International Criminal Court. ICC-BD/01–05–16.

«Протокол»), який слугував технічними протоколами та засобами для визначення автентичності цифрових доказів[1].

Зазначимо, що більша частина Протоколу про електронний суд є відносно стандартним описом угод про найменування та процедур підготовки і подання документів в електронній системі Суду. Однак, передбачені Протоколом методи автентифікації потребують подальшого ретельного вивчення.

Неспроможність Суду оновити свої застарілі та ненадійні процедури автентифікації свідчить про те, що Суд все ще вкрай недостатньо підготовлений до викликів автентифікації, з якими він стикається в цифрову епоху. Це підриває довіру до МКС та його здатність розглядати майбутні справи, в яких цифрові докази гарантовано відіграватимуть центральну роль.

На відміну від традиційних форм доказів: речових, документів, показань та висновків експертів, цифрові докази набагато більше піддаються компрометації, підробці, зміні, маніпуляціям та видаленню[2]. Хоча підробка може бути проблемою для речових доказів, документів та показань, більшість цифрових доказів сьогодні є «народженими в цифрі», а це означає, що для визначення автентичності може не існувати аналогових документів чи обладнання. У судовому процесі проти конголезького воєначальника Томаса Лубанги було використано відеозапис, зроблений між 2002 і 2003 роками, щоб показати, що дітей, яким явно не виповнилося 15 років, вербували як солдатів і військових охоронців[3]. Слідчі змогли підтвердити часові рамки відеозапису на основі специфічної форми касети VHS, на яку було записано відео[4]. Такий вид автентифікації та верифікації неможливий для відео, завантажених в Інтернеті та розміщених у соціальних мережах. Крім того, інформаційна епоха уможливила створення забрудненої інформаційної екосистеми, в якій дезінформація (навмисне поширення оманливої або неправдивої інформації) є звичним явищем[5]. Ці складнощі стосуються і даних, отриманих під час збройного конфлікту, коли обставини, що швидко змінюються, роблять автентифікацію та перевірку інформації надзвичайно складною справою.

У збройному конфлікті воюючі сторони використовують неправдиві заяви, дезінформацію на свою користь, неправильно приписуючи атаки, маніпулюючи цифровими зображеннями чи відео, а також цілеспрямовано спотворюючи контекст зображень, відео чи мови у двозначний чи оманливий спосіб. Наприклад, під час Тиграянського конфлікту в Ефіопії сторони маніпулювали зображеннями, додаючи до фотографій прапори інших країн, додаючи до зображень системи озброєння, а також публікуючи в соціальних мережах старі зображення з інших конфліктів і приписуючи їх супротивникам[6]. У 2015 році група журналістів Bellingcat провела ґрунтовне дослідження та вказала, що Міністерство оборони Росії маніпулювало геопросторовими зображеннями, пов'язаними зі збиттям рейсу MH17 Малайзійських авіаліній, включаючи зміну рельєфу місцевості, видалення присутності російської військової техніки

[1] L Freeman, and R V Llorente, Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age (2021) 19 (1) *Journal of International Criminal Justice* 163–88 <https://doi.org/10.1093/jicj/mqab023> accessed 26.04.2023.

[2] Там само.

[3] Ng Yvonne, How to Preserve Open Source Information Effectively." In *Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, 1st ed., (Oxford, United Kingdom, Oxford University Press, 2020) 143–164.

[4] Там само.

[5] L Freeman, and R V Llorente, Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age (2021) 19 (1) *Journal of International Criminal Justice* 163–88 <https://doi.org/10.1093/jicj/mqab023> accessed 26.04.2023.

[6] Ethiopia's Tigray Conflict Sparks Spread of Misinformation (2020) BBC News <https://www.bbc.com/news/world-africa-54888234> accessed 27.04.2023.

та приховування важливих особливостей місця падіння літака за допомогою фальшивих хмар[1]. Крім того, у 2014 році вірусним стало онлайн відео під назвою «Сирійський хлопчик-герой», на якому нібито зображений молодий сирійський хлопчик, який рятує дівчинку, що опинилася в пастці під час активних бойових дій у Сирії під час громадянської війни. Відео було поширене кількома провідними засобами масової інформації, включаючи BBC, і отримало подальше поширення в соціальних мережах. Однак пізніше з'ясувалося, що відео було знято на зйомках фільму «Гладіатор» норвезьким режисером[2].

Сприйнятливість до поширення неправдивої інформації авторитетними ЗМІ є значним викликом для МКС. На ранніх стадіях судового розгляду судді можуть заслуховувати докази, отримані з повідомлень ЗМІ, які вважаються легітимними, таких як BBC та New York Times, щоб визначити контекст або допомогти встановити достовірність інших доказів. Хоча судді можуть зважувати доказову цінність повідомлень ЗМІ, що знаходяться в «нижній частині ланцюжка доказів», ці ЗМІ допомагають формувати домінуючий наратив, пов'язаний з міжнародними злочинами, ризикуючи закріпити потенційно оманливу або неправдиву інформацію в свідченнях очевидців, слідчих і суддів[3]. Неправдиві факти можуть мати серйозні наслідки в правовій сфері. У кримінальних провадженнях недостовірна інформація може призвести до неправомірних вироків, незасудження винних у скоєнні тяжких злочинів та інших серйозних судових помилок[4]. З огляду на величезну кількість потенційно важливих даних, що генеруються під час збройного конфлікту в цифрову епоху, ніколи ще не було так важливо і складно відрізнити, яка інформація є правдивою, а яка – фейковою.

Ще однією суттєвою проблемою для автентифікації та перевірки цифрових доказів є часові рамки багатьох міжнародних кримінальних справ. Більшість міжнародних кримінальних процесів розпочинаються лише через роки або десятиліття після того, як були зібрані первинні цифрові докази. Це означає, що ризики втрати даних та/або маніпуляцій з ними з часом значно зростають[5]. Брюстер Кале, засновник Internet Archive, підрахував, що середня тривалість життя веб-сторінки становить дев'яносто два дні[6]. Гіперпосилання можуть «згнивати», веб-сторінки видаляються, апаратне забезпечення виходить з ладу або застаріває, і інформація може бути втрачена назавжди[7]. Контент на платформах соціальних мереж завжди ризикує бути видаленим алгоритмами машинного навчання за порушення умов надання послуг, особливо при документуванні

[1] E Higgins, New July 17th Satellite Imagery Confirms Russia Produced Fake MH17 Evidence (2015) *Bellingcat* <https://www.bellingcat.com/news/uk-and-europe/2015/06/12/july-17-imagery-mod-comparison/> accessed 27.04.2023.

[2] Y McDermott, A Koenig and D Murray, Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations (2021) 19 (1) *Journal of International Criminal Justice* 85–105 <https://doi.org/10.1093/jicj/mqab006> accessed 27.04.2023.

[3] Y McDermott, D Murray and A Koenig, Digital Accountability Symposium: Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations (2019) *Opinio Juris* <http://opiniojuris.org/2019/12/19/digital-accountability-symposium-whose-stories-get-told-and-by-whom-representativeness-in-open-source-human-rights-investigations/> accessed 27.04.2023.

[4] L Freeman, Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court. In Digital Witness : *Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, 1 (Oxford, United Kingdom, Oxford University Press, 2020) 48-67 <https://opil.ouplaw.com/display/10.1093/law/9780198836063.001.0001/law-9780198836063-chapter-4> accessed 27.04.2023.

[5] A Koenig, E Irving, Y McDermott, and D Murray, New Technologies and the Investigation of International Crimes: An Introduction (2021) 19 (1) *Journal of International Criminal Justice* 1–7 <https://doi.org/10.1093/jicj/mqab040> accessed 27.04.2023.

[6] F Carlson, Internet History Is Fragile. This Archive Is Making Sure It Doesn't Disappear (2017) *PBS NewsHour* <https://www.pbs.org/newshour/show/internet-history-fragile-archive-making-sure-doesnt-disappear> accessed 27.04.2023.

[7] Там само.

серйозних порушень прав людини, які можуть містити насильницький контент[1]. У відео для New York Times сирійський активіст Хаді Аль-Хатіб звернувся до таких платформ, як YouTube і Facebook, із закликом удосконалити системи модерації контенту після того, як у 2017 році десять відсотків архіву, що документує насильство під час громадянської війни в Сирії, а це десятки тисяч відеороликів, було втрачено внаслідок автоматичного видалення YouTube[2]. Ризики втрати даних зменшують здатність МКС виконувати свої основні судові функції. Без доступу до критично важливих доказів Суд ризикує уможливити передчасні виправдувальні вироки, фальшиві звинувачення або інші втрачені можливості для забезпечення підзвітності та правосуддя.

Використання криптографії для автентифікації цифрових доказів також не є статичним завданням, оскільки галузеві стандарти автентифікації сьогодні можуть швидко застаріти в майбутньому[3]. Алгоритми шифрування прив'язані до технологічної складності та відомих векторів атак на момент їх написання, а це означає, що з часом ці алгоритми можуть бути скомпрометовані новими способами, не підтримуватися виробником або бути незахищеними з інших причин[4]. МКС наразі використовує алгоритм шифрування під назвою MD5, який свого часу був широко поширений, але відтоді став небезпечно застарілим і вразливим[5].

Перевірка цифрових доказів також вимагає розуміння того, як культурний і соціальний контекст змінюється з часом. Яскравим прикладом того, наскільки важливим може бути розуміння контексту, є переслідування Міжнародним кримінальним трибуналом по Руанді (МКТР) справи «Прокурор проти Жан-Поля Акайєсу» щодо геноциду в Руанді[6]. Під час розгляду справи палата МКТР зазначила, що руандійські свідки часто неохоче або взагалі не бажали прямо стверджувати, що слово «cockroach» офіційною місцевою мовою означає «тарган»[7]. Лінгвістичні експерти допомогли Суду зрозуміти, що слово «cockroach», звичайне значення якого – «тарган», з часом набуло образливого відтінку, прикріпивши слово «тарган» до всього народу тутсі[8]. Не знаючи контексту, що це слово було використано для підбурювання до геноциду проти тутсі в 1990-х роках, Палата упустила б важливий компонент справи. У цифрову епоху неймовірна швидкість, з якою розвиваються норми і закодована мова в Інтернеті, означає, що соціальний і часовий контекст цифрового контенту, який потенційно може мати відношення до справи МКС, може бути легко пропущений або неправильно зрозумілий.

Меми також відіграють важливу роль у комунікації та створенні культурних наративів навколо чутливих геополітичних питань і, що важливо, про війну. Наприклад, на початку 2020 року, після вбивства Сполученими Штатами, Касема Сулеймані, соціальними мережами швидко поширилися меми,

[1] A Koenig, E Irving, Y McDermott, and D Murray, New Technologies and the Investigation of International Crimes: An Introduction (2021) 19 (1) *Journal of International Criminal Justice* 1–7 <https://doi.org/10.1093/jicj/mqab040> accessed 27.04.2023.

[2] H Al Khatib and D Kayyali, Video: Opinion | YouTube Is Erasing History (2019) The New York Times <https://www.nytimes.com/video/opinion/100000006702129/syria-youtube-content-moderation.html> accessed 27.04.2023.

[3] K Moriarty, Why Are Authentication and Authorization So Difficult? (2021) *Center for Internet Security* <https://www.cisecurity.org/blog/why-are-authentication-and-authorization-so-difficult/> accessed 27.04.2023.

[4] S Murrow, Security Risks of Outdated Encryption: Is Your Data Really Secure? (2020) *Infosec Resources* <https://resources.infosecinstitute.com/topics/cryptography/security-risks-of-outdated-encryption-is-your-data-really-secure/> accessed 27.04.2023.

[5] X Wang and H Yu, How to Break MD5 and Other Hash Functions. Advances in Cryptology – EUROCRYPT 2005 : Conference. Lecture Notes in Computer Science, vol 3494 (Springer, Berlin, Heidelberg) <https://doi.org/10.1007/11426639_2> accessed 27.04.2023.

[6] Case Prosecutor v. Jean-Paul Akayesu. International Criminal Tribunal for Rwanda (ICTR). Chamber I. "Judgment." ICTR-96-4-T. (1998) <https://www.refworld.org/cases,ICTR,40278fbb4.html> accessed 27.04.2023.

[7] Там само.

[8] Там само.

які висловлювали занепокоєння щодо потенційної війни між Іраном і США та перспективи військового призову[1]. Дослідник соціальних мереж і професор Мічиганського державного університету Салім Алхабаш сказав Vox в інтерв'ю 2020 року: «У будь-якій політичній напруженості – місцевій, регіональній, національній чи глобальній – соціальні мережі є частиною війни. І це те, що слід шукати в будь-якій майбутній кризі»[2]. На платформах соціальних мереж зростаюче явище «algospeak» змінює значення звичайних слів і те, як користувачі спілкуються на делікатні або насильницькі теми. Термін «algospeak», запропонований журналісткою Тейлор Лоренц, означає кодові слова або фрази, які користувачі використовують для того, щоб обійти алгоритми модерації контенту[3]. Користувачі, особливо в TikTok, зазвичай використовують такі слова, як «неживий» замість «мертвий» або «С.Н.» замість «сексуальне насильство», щоб уникнути видалення або зниження рейтингу контенту[4]. Зміни у формулюваннях, що стосуються чутливого або насильницького онлайн-контенту, є дуже важливими для Суду. Ці зміни можуть мати значний вплив на здатність суддів давати повну і точну оцінку достовірності цифрових доказів[5]. Якщо судді не зможуть перевірити твердження щодо цифрового контенту через нерозуміння значення або контексту доказів, вони можуть втратити значні можливості для правосуддя.

Нарешті, технологічні стрибки в обчислювальних потужностях і зберіганні даних, безсумнівно, триватимуть. За оцінками Всесвітнього економічного форуму, до 2025 року світ генеруватиме приблизно один мільярд гігабайтів щодня[6]. Щоб уявити це в перспективі, сукупність доказів Міжнародного кримінального трибуналу щодо колишньої Югославії (МТКЮ) створила безпрецедентні 8 мільйонів сторінок документів, пов'язаних з конфліктом[7]. Лише за вісім тижнів війни в Україні у 2022 році архівісти некомерційної організації Mnemonic зібрали та перевірили понад 500 000 відео[8]. Величезний обсяг даних, створених у цифрову епоху, створює значні виклики для слідчих МКС, яким необхідно збирати, автентифікувати, перевіряти та зберігати потенційно релевантні дані, які є дуже мінливими та вразливими. З огляду на це колосальне завдання, важливо, щоб Суд зробив усе можливе для забезпечення цілісності і безпеки цифрових доказів.

Ще однією значною зміною в автентифікації цифрових доказів є зростаюча практика розслідувань з відкритих джерел. Інформація з відкритих джерел – це «загальнодоступна інформація, яку будь-який представник громадськості може спостерігати, купувати або запитувати, не вимагаючи спеціального пра-

[1] A Romano, World War 3 Memes as Therapy: Coping with War and Crisis through Memes – *Vox* (2020) Vox <https://www.vox.com/2020/1/17/21065113/world-war-3-memes-iran-2020-saleem-alhabash-interview> accessed 27.04.2023.

[2] A Romano, World War 3 Memes as Therapy: Coping with War and Crisis through Memes – *Vox* (2020) Vox <https://www.vox.com/2020/1/17/21065113/world-war-3-memes-iran-2020-saleem-alhabash-interview> accessed 27.04.2023.

[3] T Lorenz, Internet 'Algospeak' Is Changing Our Language in Real Time, from 'Nip Nops' to 'Le Dollar Bean (2022) *Washington Post* <https://www.washingtonpost.com/technology/2022/04/08/algospeak-tiktok-le-dollar-bean/> accessed 27.04.2023.

[4] Там само.

[5] A Cole, Technology for Truth: The Next Generation of Evidence (2015) *International Justice Monitor* <https://www.ijmonitor.org/2015/03/technology-for-truth-the-next-generation-of-evidence/> accessed 27.04.2023.

[6] J Desjardins, How Much Data Is Generated Each Day? (2019) *World Economic Forum* <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/> accessed 27.04.2023.

[7] ICTY - UNICRI. 2009. ICTY Manual on Developed Practices.Turin, Italy: International Criminal Tribunal for the Former Yugoslavia (ICTY) and United Nations Interregional Crime and Justice Research Institute (UNICRI) <https://www.icty.org/> accessed 27.04.2023.

[8] I Lovett and N Ojewska, Citizens' Images of Potential War Crimes in Ukraine Flood the Internet, but Might Not Hold Up in Court (2022) *WSJ* <https://www.wsj.com/articles/citizens-images-of-potential-war-crimes-in-ukraine-flood-the-internet-but-might-not-hold-up-in-court-11651311001> accessed 27.04.2023.

вового статусу або несанкціонованого доступу»[1]. Розслідування з відкритих джерел використовують інформацію з відкритих джерел для отримання критично важливої інформації та збору потенційних доказів[2].

Традиційно МКС покладався на інформацію з відкритих джерел щодо конкретного конфлікту зі звітів, складених міжнародними та неурядовими організаціями (НУО). Однак Суд дедалі частіше критикує надмірну залежність від звітів НУО, які, на думку суддів, не мають достатньої доказової сили[3]. Розчарування досягло апогею у справі «Прокурор проти Гбагбо», коли слідчі представили звіти НУО, ООН та новин, засновані на значній кількості анонімних чуток, не вживши жодних додаткових слідчих дій для підтвердження їхньої достовірності та правдивості[4]. Палата зазначила, що, хоча ці звіти та новини допомагають встановити контекст, «такі докази жодним чином не можуть бути представлені як результати повного та належного розслідування»[5].

Таким чином, розслідування з відкритих джерел відкривають значні перспективи для більш плідного збору інформації та доказів. Розслідування з відкритих джерел дозволяють різним представникам громадянського суспільства відігравати активну роль у зборі, розслідуванні та аналізі цифрових доказів. Це відкриває нові двері до правосуддя для жертв масових звірств завдяки інноваційним методам і засобам отримання доказів і підтвердження свідчень свідків[6]. 2015 року дослідники з Amnesty International використали супутникові знімки Google Earth, щоб визначити точне місце розташування масового поховання в Бурунді, зафіксоване на створеному користувачем відео і підтверджене свідченнями очевидців. Ці докази спростували офіційні урядові наративи, які применшували або заперечували позасудові державні вбивства – подвиг, який був би неможливий без інформації з відкритих джерел[7].

Переваги нових методів і джерел розслідування з відкритих джерел очевидні. Останнім часом були зроблені обнадійливі кроки в напрямку професіоналізації розслідувань за допомогою відкритих джерел для документування порушень прав людини. У 2017 році Атлантична рада розробила інноваційні методи з використанням відкритих джерел для документування облоги Алеппо, Сирія[8]. Нещодавно ці методи були використані для аналізу російської тактики облоги, що застосовувалася під час російських атак на українське місто Маріуполь[9]. Мабуть, найбільш помітним є те, що у 2020 році Берклiський протокол про цифрові розслідування з використанням відкритих джерел створив стандарти та практичні рекомендації для практиків

[1] Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court. Workshop Report (2012) The Human Rights Center at the University of California, Berkeley, School of Law <https://www.law.berkeley.edu/files/HRC/HRC_Beyond_Reasonable_Doubt_FINAL.pdf> accessed 27.04.2023.

[2] Там само.

[3] L Freeman, Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court. In Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1 (Oxford, United Kingdom: Oxford University Press, 2020) 48–67 <https://www.academia.edu/95425352/Prosecuting_Atrocity_Crimes_with_Open_Source_Evidence_Lessons_from_the_International_Criminal_Court> accessed 27.04.2023.

[4] Там само.

[5] Case Prosecutor v. Laurent Gbagbo. ICC. Pre-Trial Chamber I. “Decision adjourning the hearing on the confirmation of charges pursuant to article 61(7)(c)(i) of the Rome Statute.” ICC-02/11-01/11 (2013) <https://www.icc-cpi.int/court-record/icc-02/11-01/11-656-red-0> accessed 27.04.2023.

[6] A Cole, Technology for Truth: The Next Generation of Evidence (2015) *International Justice Monitor* <https://www.ijmonitor.org/2015/03/technology-for-truth-the-next-generation-of-evidence/> accessed 27.04.2023.

[7] C Koettl, D Murray and S Dubberley, Open Source Investigation for Human Rights Reporting : A Brief History. In Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1st ed. (Oxford, United Kingdom, Oxford University Press, 2020) 12–31.

[8] M Czuperski, E Beals, F Itani, B Nimmo, and E Higgins. Breaking Aleppo (2017) *Washington: Atlantic Council.* <https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-aleppo/> accessed 27.04.2023.

[9] J Hendrix, Ukraine May Mark a Turning Point in Documenting War Crimes (2022) *Just Security* <https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/> accessed 28.04.2023.

щодо належного та етичного отримання та використання відкритої інформації[1]. Однак з появою великої кількості нових учасників розслідувань з використанням відкритих джерел зростає занепокоєння щодо їхньої надійності, цілісності та автентичності[2]. Багато інновацій у розслідуванні з використанням відкритих джерел були започатковані суб'єктами поза межами правового поля[3]. Журналісти, активісти та члени громадянського суспільства не мають належної підготовки щодо стандартів доказування і можуть ненавмисно підірвати зусилля слідства з отримання потенційних доказів[4]. Тому МКС повинен оцінювати інформацію з відкритих джерел з обережністю та скептицизмом, враховуючи, які суб'єкти беруть участь у розслідуванні, які технології вони використовують, а також можливості для підробок і маніпуляцій з цифровими доказами[5].

МКС вже почав розглядати питання про те, як оцінювати цифрові докази у двох відомих справах – Аль-Махді та Аль-Верфаллі[6].

У справі Аль-Махді відео з інтернету разом із супутниковими знімками були використані для висунення звинувачень проти ймовірного члена «Аль-Каїди» Ахмада Аль-Факі Аль-Махді у знищенні об'єктів культурної спадщини в Тімбукту, Малі[7]. Однак, оскільки обвинувачений визнав свою провину, автентичність доказів ніколи не ставилася під сумнів, а також не було викликано жодного технічного експерта-свідка, який би дав свідчення щодо представлених цифрових доказів[8]. Аналогічно, у справі 2017 року «Прокурор проти Махмуда Мустафи Бусифа аль-Верфаллі» суд значною мірою покладався на кілька відео, розміщених у Facebook, щоб видати ордер на арешт високопоставленого лівійського офіцера, майора Махмуда Мустафи Бусифа аль-Верфаллі, за вбивство 33 осіб[9]. Аль-Верфаллі наразі не перебуває під вартою МКС, тому ефект від запровадження доказів з соціальних мереж ще належить побачити. Справи аль-Махді та аль-Верфаллі демонструють готовність судів оцінювати цифрові докази у суттєво новий спосіб. У випадку з Аль-Верфаллі справи, ймовірно, взагалі не було б, якби не відеозаписи ймовірних злочинів, розміщені у Facebook[10]. Хоча цифрові докази

[1] The Human Rights Center, University of California, Berkeley, School of Law and United Nations High Commissioner for Human Rights. 2020. "Berkeley Protocol on Digital Open Source Investigation: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law." 2020. Advanced Version HR/PUB/20/2. New York and Geneva <https://www.ohchr.org/sites/default/f iles/Documents/Publications/OHCHR_BerkeleyProtocol.pdf> accessed 28.04.2023.

[2] J Hendrix, Ukraine May Mark a Turning Point in Documenting War Crimes (2022) *Just Security* <https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/> accessed 28.04.2023.

[3] L Freeman, Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court. In Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1 (Oxford, United Kingdom, Oxford University Press, 2020) 48–67.

[4] J Hendrix, Ukraine May Mark a Turning Point in Documenting War Crimes (2022) *Just Security* <https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/> accessed 28.04.2023.

[5] The Human Rights Center, University of California, Berkeley, School of Law and United Nations High Commissioner for Human Rights. 2020. "Berkeley Protocol on Digital Open Source Investigation: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law." 2020. Advanced Version HR/PUB/20/2. New York and Geneva <https://www.ohchr.org/sites/default/f iles/Documents/Publications/OHCHR_BerkeleyProtocol.pdf> accessed 28.04.2023.

[6] L Freeman and R V Llorente, Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age (2021) 19 (1) *Journal of International Criminal Justice* 163–88. <https://doi.org/10.1093/jicj/mqab023> accessed 28.04.2023.

[7] S Zarmsky, Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law (2021) 19 (1) *Journal of International Criminal Justice* 213–25. <https://doi.org/10.1093/jicj/mqab048> accessed 28.04.2023.

[8] Там само.

[9] L Freeman and R V Llorente, Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age (2021) 19 (1) *Journal of International Criminal Justice* 163–88. <https://doi.org/10.1093/jicj/mqab023> accessed 28.04.2023.

[10] L Freeman, Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court. In Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and

ще не відігравали центральної ролі в остаточному рішенні МКС, ці дві справи демонструють, що ця зміна неминуча[1].

Хоча МКС, безумовно, має багато викликів, пов'язаних з оцінкою цифрових доказів, Суд має потенціал для вирішення деяких з них шляхом перепрофілювання або перенаправлення наявних ресурсів та підвищення прозорості своїх процедур, пов'язаних з автентифікацією цифрових доказів. Такі рекомендації не закликають до радикальної перебудови основних обов'язків Суду, а також не мають на меті перевантажити і без того обмежену в ресурсах організацію. Однак ці рекомендації значною мірою сприятимуть усуненню недоліків нинішніх процедур цифрової автентифікації Суду.

Безпосереднє і нагальне занепокоєння викликає продовження використання Судом вкрай небезпечного і застарілого алгоритму цифрових підписів MD5. Ризики, пов'язані зі слабкою криптографією, наразі недостатньо добре усвідомлені Судом. Наслідки витоку даних, знищення або маніпуляції з цифровими доказами Суду будуть серйозними. Втрата конфіденційної інформації може поставити під загрозу життя потерпілих, свідків та слідчих. Крім того, витік, пошкодження або знищення даних загрожуватиме основній функції Палати – забезпеченню справедливого та швидкого судового розгляду[2]. Той факт, що МКС взагалі вимагає цифрових підписів, свідчить про те, що на певному рівні Суд визнає важливість цілісності та безпеки даних. Метою криптографії є захист конфіденційності, автентичності та цілісності цифрової інформації – функцій, які мають вирішальне значення для виконання завдань Суду[3]. Тому вкрай важливо, щоб МКС надавав пріоритет надійним стандартам криптографії для захисту своєї електронної системи подання заяв.

Міжнародні органи зі стандартизації, такі як Міжнародна організація зі стандартизації (ISO), Інститут інженерів з електротехніки та електроніки (IEEE) та Робоча група з питань інтернет-технологій (IETF), могли б запропонувати рекомендації, оскільки вони регулярно публікують актуальні списки безпечних алгоритмів, що використовуються організаціями в усьому світі. Як зазначалося раніше, Суд повинен працювати над впровадженням протоколів для досягнення гнучкості алгоритмів, мігруючи від одного набору алгоритмів до іншого в міру того, як криптографічні алгоритми стають слабкими або застарілими. Досягнення цієї мети узгоджувалося б з однією з МКС у Стратегічному плані Суду на 2019–2021 роки: «покращення організаційної діяльності», а конкретніше – «подальше зміцнення професіоналізму, відданості та доброчесності в усіх видах діяльності Суду»[4].

IETF пропонує розробникам протоколів використовувати «модульну» схему реалізації, що означає, що протокол може легко пристосовуватися до нових алгоритмів або наборів алгоритмів і безперешкодно виводити з експлуатації старі алгоритми[5]. Група користувачів електронного суду МКС може стати відповідним внутрішнім органом для виконання цього завдання. Група користувачів електронного суду була створена

Accountability, 1 (Oxford, United Kingdom, Oxford University Press, 2020) 48–67.

[1] L Freeman and R V Llorente, Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age (2021) 19 (1) *Journal of International Criminal Justice* 163–88. <https://doi.org/10.1093/jicj/mqab023> accessed 28.04.2023.

[2] Rome Statute, Article 64(2).

[3] A F Johnson and L I Millett (eds.), Cryptographic Agility and Interoperability: Proceedings of a Workshop. In Forum on Cyber Resilience: Workshop Series (The National Academies of Sciences, Engineering, and Medicine. Washington, D.C.,The National Academies Press, 2017) <https://doi.org/10.17226/24636> accessed 28.04.2023.

[4] Strategic Plan 2019-2021. International Criminal Court. 2019 <https://www.icc-cpi.int/sites/default/files/itemsDocuments/20190717-icc-strategic-plan-eng.pdf> accessed 28.04.2023.

[5] R Housley, Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms." BCP 201, RFC 7696, DOI 10.17487/RFC7696 Internet Engineering Task Force, 2015 <https://www.rfc-editor.org/info/rfc7696> accessed 28.04.2023.

для того, щоб дозволити користувачам збиратися та обговорювати практичні питання, пов'язані з функціонуванням електронного суду[1]. Роль групи користувачів у вирішенні цих питань може бути двоякою. По-перше, група користувачів може допомогти Суду прийняти рішення щодо вибору найкращого алгоритму (алгоритмів) криптографії на основі міжнародних стандартів та потреб МКС. По-друге, вони могли б колективно домовитися про те, як найкраще досягти алгоритмічної гнучкості у спосіб, який є найменш витратним і не порушує роботу всіх сторін, особливо сторін з обмеженими ресурсами або технічними можливостями. У більш широкому розумінні, протокол електронного суду повинен систематично перевірятися експертами з кібербезпеки на наявність інших вразливостей та переглядатися, щоб бути незалежним від постачальника, тобто не надавати перевагу жодному конкретному програмному чи апаратному рішенню у разі виявлення в майбутньому вразливостей кібербезпеки в конкретних програмах[2]. Гнучкість алгоритмів важлива не лише для належного захисту високочутливих даних, але й для посилення здатності суддів ефективно вирішувати розбіжності щодо автентичності та достовірності цифрових доказів.

Існує очевидна і значна потреба в підвищенні технологічної грамотності в МКС. Для суддів це має включати базові знання про безпеку даних, метадані, зберігання даних, цифрову криміналістику і те, як технології впливають на ступінь достовірності цифрових доказів. Стаття 7(3) Кодексу суддівської етики Суду говорить: «Судді повинні вживати розумних заходів для підтримання та вдосконалення знань, навичок та особистих якостей, необхідних для роботи на посаді судді»[3]. Судді в багатьох юрисдикціях загалом визнають необхідність «безперервної суддівської освіти»[4]. Професійний розвиток є нормою в багатьох інших країнах та вищих судах[5]. У Незалежному експертному огляді Заключного звіту МКС та Римського статуту, опублікованому в 2020 році, експерти рекомендують суддям використовувати щорічні виїзні засідання МКС як відправну точку для запровадження програми професійного розвитку[6]. Окрім того рекомендовано провести низку заходів у Гаазі, де судді зможуть поспілкуватися з експертами з міжнародного права та інших професій «для обговорення питань, що становлять інтерес для розвитку їхніх професійних, наукових і культурних знань, навичок і досвіду»[7].

Ці рекомендації можуть зустріти опір з боку деяких суддів. Деякі судді можуть вважати безперервну освіту надмірно обтяжливою для їхнього часу або навіть такою, що принижує їхні повноваження, знання чи навички як провідних експертів у галузі міжнародного права[8]. Але мета безперервної освіти суддів жодним чином не полягає в тому, щоб поставити під сумнів доброчесність або авторитет суддів. Навпаки, безперервна освіта суддів повинна розглядатися як важливий інструмент підвищення компетентності для забезпечення належного відправлення правосуддя. З огляду на значні технологічні виклики, з якими стикається Суд у цифрову епоху, для суддів як ніколи важливо бути обізнаними з технологічними концепціями. Судді мають

[1] M Dillon and D Beresford, Electronic Courts and the Challenges in Managing Evidence. A View From Inside The International Criminal Court (2014) 6 (1) *International Journal for Court Administration* 29–36. <https://doi.org/10.18352/ijca.132> accessed 28.04.2023.

[2] K Moriarty, Why Are Authentication and Authorization So Difficult? (2021) *Center for Internet Security* <https://www.cisecurity.org/blog/why-are-authentication-and-authorization-so-difficult/> accessed 28.04.2023.

[3] Code of Judicial Ethics. International Criminal Court. Article 7(2). ICC-BD/02–01–05.

[4] Independent Expert Review of the International Criminal Court and the Rome Statute System Final Report. 2020 <https://asp.icc-cpi.int/sites/asp/files/asp_docs/ASP19/IER-Final-Report-ENG.pdf> accessed 28.04.2023.

[5] Там само.

[6] Там само.

[7] Там само.

[8] Там само.

вирішальне слово у визначенні автентичності цифрових доказів. Тому вони є найбільшою надією і найслабшою ланкою у забезпеченні належного вирішення спорів щодо автентичності. З цих причин судді повинні підвищувати свою базову грамотність щодо автентифікації цифрових доказів.

Підвищення технологічної грамотності суддів вимагає перегляду найбільш перспективних ресурсів, які можуть допомогти Суду в цьому. У 2014 році МКС створив Науково-консультативну раду МКС, до складу якої увійшла міжнародна група експертів-криміналістів зі спеціалізованих наукових організацій для надання допомоги в слідчій та прокурорській роботі[1]. Відповідно до прес-релізів МКС, Рада зустрічається раз на рік з Офісом прокурора і готує щорічний звіт, в якому обговорюються наукові пріоритети Офісу прокурора[2]. Однак, як видається, ці щорічні звіти не є доступними для громадськості, а також МКС не публікує загальну інформацію про Раду та її діяльність.

Хоча Суд заснував Науково-консультативну раду, незрозуміло, чи скликав він коли-небудь групу експертів для розробки керівних принципів щодо соціальних мереж і відеодоказів. У прес-релізі 2020 року, присвяченому щорічній зустрічі Науково-консультативної ради, МКС оприлюднив список з одинадцяти організацій, які брали участь у щорічній зустрічі. З них вісім були міжнародними або регіональними судово-експертними організаціями, дві – організаціями судової медицини, а одна, Європейський центр боротьби з кіберзлочинністю Європолу, спеціалізувалася на кіберзлочинності[3]. Хоча, без сумніву, існує велика потреба в судово-медичній експертизі в МКС, надмірне представництво судово-медичних наук свідчить про те, що Рада не зосереджена на просуванні або вирішенні технологічних питань. Враховуючи нагальну потребу в рекомендаціях щодо цифрових доказів, Рада повинна розглянути можливість розширення своєї консультативної ролі в галузі технологій, пропонуючи Суду експертизу та найкращі практики використання цифрових доказів. На жаль, Рада збирається лише раз на рік. Таким чином, хоча ресурси Ради можуть бути дуже корисними для надання загальних рекомендацій Суду, вона не підходить для надання консультацій з технологічних питань на терміновій або регулярній основі.

Група користувачів електронного суду МКС може бути більш підходящим ресурсом для консультування з питань, пов'язаних з автентифікацією цифрових доказів.

Проте, у відкритому доступі дуже мало інформації про діяльність Групи користувачів. Залишається незрозумілим, хто кваліфікується як «користувач» для участі в діяльності Групи користувачів[4].

МКС також має розглянути можливість вжити заходів для підвищення прозорості функцій і діяльності Науково-консультативної ради та Групи користувачів електронного суду. Мало користі від того, що щорічні звіти Ради є недоступними для громадськості. Більша прозорість дозволила б дослідникам і технологам відігравати більш активну роль у вдосконаленні роботи Суду.

З огляду на результати проведеного аналізу, МКС з метою реалізації своїх завдань в епоху стрімкої цифровізації має провести ряд заходів щодо удосконалення роботи з доказами, зокрема: (1)

[1] The Office of the Prosecutor of the International Criminal Court Establishes a Scientific Advisory Board (2014) *International Criminal Court* <http://www.icc-cpi.int/news/office-prosecutor-international-criminal-court-establishes-scientific-advisory-board> accessed 28.04.2023.

[2] The Scientific Advisory Board of the Office of the Prosecutor holds 7th annual meeting (2020) *International Criminal Court* <http://www.icc-cpi.int/news/office-prosecutor-international-criminal-court-establishes-scientific-advisory-board> accessed 28.04.2023.

[3] Там само.

[4] M Dillon and D Beresford, Electronic Courts and the Challenges in Managing Evidence. A View From Inside The International Criminal Court (2014) 6 (1) *International Journal for Court Administration* 29–36 <https://doi.org/10.18352/ijca.132> accessed 28.04.2023.

призначити Групу користувачів електронного суду для керівництва зусиллями з удосконалення алгоритмів і постійного розвитку питань автентифікації; (2) розширити технологічну консультативну роль Науково-консультативної ради; (3) створити регулярні тренінги та семінари для підвищення технічної компетентності суддів; і (4) підвищити прозорість діяльності Науково-консультативної ради та Групи користувачів електронного суду. Ці кроки значно підвищать легітимність та авторитет методів автентифікації та перевірки цифрових доказів у Суді.

Висновки. Взаємодія МКС з цифровими доказами почалася, коли він заявив про свою готовність розглянути нові форми цифрових доказів у справах Аль-Махді та Аль-Верфаллі[1]. Однак Суд недостатньо адаптувався до унікальних викликів, які цифрові докази ставлять перед автентифікацією та верифікацією, зокрема основний механізм автентифікації цифрових файлів, передбачений Протоколом електронного суду, криптографічно вразливий. Швидкий розвиток технологій, забруднене інформаційне середовище та величезні обсяги вразливих, швидкоплинних і чутливих до часу даних означають, що суперечки щодо автентичності цифрових доказів є неминучими. Нові форми цифрових доказів підвищують рівень сумнівів щодо їхньої автентичності та перевірки, порушуючи серйозні питання про те, як МКС має найкраще підходити до складних технологічних сфер і що має передбачати судовий розгляд за таких обставин.

МКС не повинен бути паралізований страхом і невпевненістю перед новими технологіями і методами цифрової автентифікації. Як мінімум, криптографічний стандарт цифрової автентифікації файлів має бути замінений на надійну програму цифрового підпису, а протокол електронного суду має систематично перевірятися на наявність інших вразливостей. Ці попередні заходи, на наш погляд, значною мірою сприятимуть тому, що МКС буде краще підготовлений до майбутніх викликів, які цифрові докази принесуть міжнародному кримінальному правосуддю. Удосконалення процесів МКС матиме зворотний ефект і допоможе інформувати інші міжнародні, регіональні та національні органи, які розглядають справи про порушення прав людини та інші питання, що перетинаються[2]. З цих причин МКС має встановити надійні процесуальні гарантії та процеси судового контролю для автентифікації цифрових доказів у сучасному швидкозмінному ландшафті міжнародного кримінального правосуддя.

REFERENCES

LIST OF LEGAL DOCUMENTS

LEGISLATION

1. Code of Judicial Ethics. International Criminal Court. Article 7(2). ICC-BD/02–01–05 [in English].

2. International Criminal Court. 2019. “Strategic Plan 2019–2021.” <https://www.icc-cpi.int/sites/default/files/itemsDocuments/20190717-icc-strategic-plan-eng.pdf> data zvernennia 24.03.2023 [in English].

3. Rules of Procedure and Evidence. International Criminal Court <https://www.icc-cpi.int/sites/default/files/RulesProcedureEvidenceEng.pdf> data zvernennia 24.03.2023 [in English].

4. Regulations of the Court. Regulation 26. International Criminal Court. ICC-BD/01–05–16 data zvernennia 24.03.2023 [in English].

[1] L Freeman, Prosecuting Atrocity Crimes with Open Source Evidence : Lessons from the International Criminal Court. In Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1 (Oxford, United Kingdom, Oxford University Press, 2020) 48–67.

[2] A Cole, Technology for Truth: The Next Generation of Evidence (2015) *International Justice Monitor* <https://www.ijmonitor.org/2015/03/technology-for-truth-the-next-generation-of-evidence/> accessed 28.04.2023.

CASES

5. *Prosecutor v. Germain Katanga.* Trial Chamber II. Judgment pursuant to article 74 of the Statute. ICC-01/04–01/07. (2014) <https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/KatangaEng.pdf> data zvernennia 24.03.2023 [in English].

6. *Prosecutor v. Thomas Lubanga Dyilo.* Trial Chamber I. Decision on the admissibility of four documents."I CC-01/04–01/06–1399. (2008) 27–32 < https://www.icc-cpi.int/node/29611> data zvernennia 24.03.2023 [in English].

7. *Prosecutor v. Jean-Paul Akayesu. I*nternational Criminal Tribunal for Rwanda (ICTR). Chamber I. Judgment. ICTR-96–4-T. (1998) <https://www.refworld.org/cases, ICTR,40278fbb4.html> data zvernennia 24.03.2023 [in English].

BIBLIOGRAPHY

ARTICLES

8. Ashouri A, Caleb B and Cherrie W, An Overview of the Use of Digital Evidence in International Criminal Courts (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115–27 <https://doi.org/10.14296/deeslr.v11i0.2130> accessed 26.04.2023 [in English].

9. Mehandru N and Koenig A, n.d. Open Source Evidence and the International Criminal Court (2019) *Harvard Human Rights Journal* <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/> accessed 24.04.2023 [in English].

10. Wex.n.d. Pobative Value. Wex Legal Information Institute (LII), Cornell Law School <https://www.law.cornell.edu/wex/probative_value> accessed 24.04.2023 [in English].

11. Koenig, Alexa, Emma Irving, Yvonne McDermott, and Daragh Murray, New Technologies and the Investigation of International Crimes: An Introduction (2021) 19 (1): 1–7 *Journal of International Criminal Justice* 14–21 <https://doi.org/10.1093/jicj/mqab040> accessed 23.04.2023[in English].

12. Krzan B, Admissibility of Evidence and International Criminal Justice (2021) 7 (1) *Revista Brasileira de Direito Processual Penal* 161 <https://doi.org/10.22197/rbdpp.v7i1.492> accessed 24.04.2023 [in English].

13. Jackson J D, and Sarah J Summer (eds.) The Common Law Tradition. In *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*. Law in Context. (Cambridge, Cambridge University Press, 2012) 30–36 <https://doi.org/10.1017/CBO9781139093606.005> accessed 24.04.2023 [in English].

14. Yvonne Ng, How to Preserve Open Source Information Effectively." In *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, 1st ed., (Oxford, United Kingdom, Oxford University Press, 2020) 143–164 [in English].

15. McDermott Y, Koenig A and Murray D, Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations (2021) 19 (1) *Journal of International Criminal Justice* 85–105 <https://doi.org/10.1093/jicj/mqab006> accessed 27.04.2023 [in English].

16. Carlson F, Internet History Is Fragile. This Archive Is Making Sure It Doesn't Disappear (2017) *PBS NewsHour* <https://www.pbs.org/newshour/show/internet-history-fragile-archive-making-sure-doesnt-disappear> accessed 27.04.2023 [in English].

17. Khatib H Al, and Dia Kayyali. Video: Opinion | YouTube Is Erasing History (2019) *The New York Times* <https://www.nytimes.com/video/opinion/100000006702129/syria-youtube-content-moderation.html> accessed 27.04.2023 [in English].

18. Moriarty K, Why Are Authentication and Authorization So Difficult? (2021) *Center for Internet Security* <https://www.cisecurity.org/blog/why-are-authentication-and-authorization-so-difficult/> accessed 27.04.2023 [in English].

19. Murrow S, Security Risks of Outdated Encryption: Is Your Data Really Secure? (2020) *Infosec Resources* <https://resources.infosecinstitute.com/topics/cryptography/security-risks-of-outdated-encryption-is-your-data-really-secure/> accessed 27.04.2023 [in English].

20. Romano A, World War 3 Memes as Therapy: Coping with War and Crisis through Memes – Vox (2020) *Vox* <https://www.vox.com/2020/1/17/21065113/world-war-3-memes-iran-2020-saleem-alhabash-interview> accessed 27.04.2023 [in English].

21. Lorenz T, Internet 'Algospeak' Is Changing Our Language in Real Time, from 'Nip Nops' to 'Le Dollar Bean (2022) *Washington Post* <https://www.washingtonpost.com/technology/2022/ 04/08/algospeak-tiktok-le-dollar-bean/> accessed 27.04.2023 [in English].

22. Cole A, Technology for Truth: The Next Generation of Evidence (2015) *International Justice Monitor* <https://www.ijmonitor.org/2015/03/technology-for-truth-the-next-generation-of-evidence/> accessed 27.04.2023 [in English].

23. Desjardins J, How Much Data Is Generated Each Day? (2019) *World Economic Forum* <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/> accessed 27.04.2023 [in English].

24. Freeman L and Llorente R V, Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age (2021) 19 (1) *Journal of International Criminal Justice* 163–88. <https://doi.org/10.1093/jicj/mqab023> accessed 28.04.2023 [in English].

25. Lovett I, and Ojewska N, Citizens' Images of Potential War Crimes in Ukraine Flood the Internet, but Might Not Hold Up in Court (2022) WSJ. Accessed April 30, 2022 < https://www.wsj.com/articles/citizens-images-of-potential-war-crimes-in-ukraine-flood-the-internet-but-might-not-hold-up-in-court-11651311001 > data zvernennia 02.03.2023 [in English].

26. Koettl Ch, Murray D, and Dubberley S, Open Source Investigation for Human Rights Reporting: A Brief History. In Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1st ed. (Oxford, United Kingdom, Oxford University Press, 2020) 12–31 [in English].

27. Czuperski M, Beals E, Itani F, Nimmo B, and Higgins E, Breaking Aleppo (2017) *Washington: Atlantic Council*. .https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-aleppo/> accessed 27.04.2023 [in English].

28. Hendrix J, Ukraine May Mark a Turning Point in Documenting War Crimes (2022) *Just Security* <https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/> accessed 28.04.2023 [in English].

29. Zarmsky S, Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law (2021) 19 (1) *Journal of International Criminal Justice* 213–25. <https://doi.org/10.1093/jicj/mqab048> accessed 28.04.2023 [in English].

30. Johnson A F and Millett L I. (eds.) Cryptographic Agility and Interoperability: Proceedings of a Workshop. In Forum on Cyber Resilience: Workshop Series (The National Academies of Sciences, Engineering, and Medicine. Washington, D.C., The National Academies Press, 2017) <https://doi.org/10.17226/24636> accessed 28.04.2023 [in English].

31. Dillon M, and Beresford D, Electronic Courts and the Challenges in Managing Evidence. A View From Inside The International Criminal Court (2014) 6 (1) *International Journal for Court Administration* 29–36 <https://doi.org/10.18352/ijca.132> accessed 28.04.2023 [in English].

32. The Office of the Prosecutor of the International Criminal Court Establishes a Scientific Advisory Board (2014) *International Criminal Court* <http://www.icc-cpi.int/news/office-prosecutor-international-criminal-court-establishes-scientific-advisory-board> accessed 28.04.2023 [in English].

33. Pohoretskyi M A, Shelomentsev V P, Kiberzlochyny: do vyznachennia poniattia [Cybercrime: to the definition of the concept] (2012*)* 8 *Visnyk prokuratury* 89–96 [in Ukrainian].

34. Pohoretskyi M A, Shelomentsev V P, Poniattia kiberprostoru yak seredovyshcha vchennia zlochynu [The Concept of Cyberspace as an Environment for the Study of Crime] (2009) 2 (2) *Informatsiina bezpeka liudyny, suspilstva, derzhavy* 77–81 [in Ukrainian].

35. Smal I A, Problemni aspekty zastosuvannia elektronnykh dokaziv u kryminalnomu sudochynstvi [Problematic aspects of the use of electronic evidence in criminal proceedings] (2021) 4 *Naukovyi zhurnal «Pravo i suspilstv»* 226–232 [in Ukrainian].

36. Cherniavskyi S S, Orlov Yu Yu, Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni [Electronic display as a source of evidence in criminal proceedings](2017) 2 *Visnyk kryminalnoho sudochynstva* 112–124 data zvernennia 02.03.2023 [in Ukrainian].

37. Stolitnii A V, Kalancha I H, Formuvannia instytutu elektronnykh dokaziv u kryminalnomu protsesi Ukrainy [Formation of the electronic evidence institute in the criminal process of Ukraine] (2019) 146 *Problemy zakonnosti* 179–191 data zvernennia 02.03.2023 [in Ukrainian].

BOOKS

38. Digital evidence and computer crime: forensic science, computers and the internet / by Eoghan Casey; with contributions from Susan W. Brenner … [et al.]. 3rd ed. London: Elsevier. 837 <https://booksite.elsevier.com/9780123742681> accessed 24.04.2023 [in English].

39. Dubberley S, Koenig A, and Murray D, Introduction: The Emergence of Digital Witnesses. In Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1st ed. (Oxford, United Kingdom: Oxford University Press, 2020) 3–11 [in English].

40. Freeman L, Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court. In Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, 1st ed. (Oxford, United Kingdom, Oxford University Press, 2020) 48–67 [in English].

41. Ethiopia's Tigray Conflict Sparks Spread of Misinformation (2020) *BBC News* <https://www.bbc.com/news/world-africa-54888234> accessed 27.04.2023 [in English].

42. Higgins E, New July 17th Satellite Imagery Confirms Russia Produced Fake MH17 Evidence (2015) *Bellingcat* <https://www.bellingcat.com/news/uk-and-europe/2015/06/12/july-17-imagery-mod-comparison/> accessed 27.04.2023 [in English].

43. *ICTY – UNICRI. 2009. ICTY Manual on Developed Practices.Turin, Italy: International Criminal Tribunal for the Former Yugoslavia (ICTY) and United Nations Interregional Crime and Justice Research Institute (UNICRI)* <https://www.icty.org/> accessed 27.04.2023 [in English].

44. Korneika O V (za red.), V*ykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh, metod. rekom* [Use of electronic (digital) evidence in criminal proceedings, method. by river] 2-he, dop. (Kyiv, Vyd-vo Nats. akad. vnutr. Sprav, 2020) 104 [in Ukrainian].

45. *The Human Rights Center at the University of California, Berkeley, School of Law. 2012. "Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court." Workshop Report.* <https://www.law.berkeley.edu/files/HRC/HRC_Beyond _Reasonable_Doubt_FINAL.pdf> accessed 23.04.2023 [in English].

46. *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh*, [Use of electronic (digital) evidence in criminal proceedings] / za zah. red. O V Korneika. Vyd. 2-he, dop. (Kyiv, Vyd-vo Nats. akad. vnutr. sprav, 2020) 104 [in Ukrainian].

47. Wang X and Hongbo Yu, *How to Break MD5 and Other Hash Functions. Advances in Cryptology – EUROCRYPT 2005: Conference. Lecture Notes in Computer Science, vol 3494* (Springer, Berlin, Heidelberg) <https://doi.org/10.1007/11426639_2> accessed 27.04.2023 [in English].

48. Yvonne Ng, How to Preserve Open Source Information Effectively." In *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, 1st ed., (Oxford, United Kingdom, Oxford University Press, 2020) 143–164 [in English].

Pohoretskyi M. A.
Doctor of Science in Law, Professor,
Vice-rector for scientific and pedagogical work,
Taras Shevchenko National University of Kyiv,
***ORCID ID:** 0000-0003-0936-0929*

Lysachenko Y. I.
Ph.D (Law), attorney
***ORCID ID:** 0000-0003-0937-2110*

***DOI:** https://doi.org/10.17721/2413-5372.2023.1-2/54-73*

ESTABLISHING THE RELIABILITY OF DIGITAL EVIDENCE BY THE INTERNATIONAL CRIMINAL COURT: SOME PROBLEMATIC ISSUES AND WAYS TO SOLVE THEM

Abstract. *The article is devoted to the study of some problematic issues of authentication of digital evidence in the course of consideration of cases by the International Criminal Court.*

The authors note that in the digital era, new technologies and the development of computing power have changed the nature of potentially relevant evidence which is assessed in international criminal law. The International Criminal Court is currently insufficiently prepared to address the issues of authentication of digital evidence, i.e., to determine the reliability of this type of evidence.

The purpose of the article is to: (1) outline the challenges and dangers of the ICC's current approach to establishing the reliability of digital evidence; (2) study scientific approaches to the authentication of digital evidence in criminal proceedings; and (3) establish the need to establish the most pragmatic approach to determining the reliability of digital evidence in the future.

The article outlines the challenges and dangers of the ICC's current approach to authentication and verification of digital evidence, examines the discussions among scholars on the issues outlined,

and identifies recommendations for improving the Court's work and its ability to verify the reliability of digital evidence.

The general approach of the ICC to the admissibility of evidence is defined, which provides for a consistent three-part test in which each of the following criteria must be met: 1) relevance: According to Articles 64(9)(a) and 69(4) of the Rome Statute, as well as the Rules of Procedure and Admission of Evidence, evidence is considered relevant if "the evidence produced makes the existence of the fact in question more or less probable". In other words, evidence may be considered relevant if it is "prima facie" ("at first glance") relevant to the case; 2) sufficiency: Evidentiary value is generally understood to mean whether the evidence is sufficiently useful to prove an important part of the trial. In essence, probative value measures the extent to which the proposed evidence may affect the determination of a fact or issue. The court must balance the probative value of the item against its prejudicial effect on the accused; 3) weighing probative value and prejudicial effect: According to Rules 69(4) and 63(2), the evidence provided must be "sufficiently relevant and probative to outweigh any prejudicial impact or effect that its admission may have". In other words, the weight given to the evidence must fully respect the rights of all parties and not be manifestly unfair to the prosecution or defense, nor prejudicial to the overall fairness of the trial.

The author concludes that the ICC should seriously consider the following recommendations: (1) appoint an eCourt User Group to lead efforts to improve algorithms and continuously develop authentication issues; (2) expand the technological advisory role of the Scientific Advisory Board; (3) establish regular trainings and seminars to enhance the technical competence of judges; and (4) increase the transparency of the Scientific Advisory Board and the eCourt User Group.

***Keywords**: International Criminal Court, evidence, proof, authentication, reliable evidence.*