CyberUA

Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine

COUNCIL OF EUROPE 75 1949 - 2024 CONSEIL DE L'EUROPE

CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine

Version 11 June 2024

Project title / number:	CyberUA project on strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine
Project area:	Ukraine
Duration:	24 months (1 February 2024 – 31 January 2026, with possible extension)
Budget:	EURO 3.5 million (currently secured: 2 million EUR)
Funding:	Action Plan for Ukraine / voluntary contributions
Implementation:	Cybercrime Division of the Council of Europe

BACKGROUND AND JUSTIFICATION

The Russian aggression against Ukraine underlines once more the need for capacities to secure electronic evidence for use in criminal proceedings not only in relation to cybercrime or other cyberattacks but also in relation to any offence, including war crimes / gross human rights violations (GHRV). There is much "[…] e*vidence of serious violations of human rights and international humanitarian law by the Russian Federation, including attacks against civilian targets; indiscriminate use of artillery, missiles and bombs, including cluster bombs; attacks on humanitarian corridors intended to allow civilians to escape from besieged towns and cities; and hostage-taking*"[1], and Ukrainian investigators, detectives and prosecutors are currently working on tens of thousands of investigations into war crimes and gross human rights violations (GHRV) committed by Russian armed forces and affiliated actors during the aggression.

Much of this evidence needed for the criminal investigation and prosecution of such offences is evidence in electronic or digital form on computer systems (electronic evidence) or based on open-source intelligence (OSINT). In order to permit the use of such e-evidence and OSINT in criminal proceedings a number of requirements must be met (including rules on evidence and admissibility, chain of custody or cross-border access to and international sharing of data).[2]

Ukraine is a Party of the Budapest Convention on Cybercrime since 2006. This treaty is relevant in the context of the Russian aggression and related war crimes and GHRV because:

- the procedural powers and international cooperation provisions of that treaty are applicable to e-evidence of any criminal offence, including e-evidence of war crimes and GHRV;[3]

[1] *Consequences of the Russian Federation's aggression against Ukraine*, Parliamentary Assembly of the Council of Europe, adopted on 15 March 2022. See also the report of the Independent International Commission of Inquiry on Ukraine of 16 March 2023.

[2] See also the decision of the European Court of Human Rights regarding the Case of Ukraine and the Netherlands v. Russia (January 2023), including on questions of admissibility of evidence provided by organisations such as Bellingcat.

[3] A Guidance Note to this effect is expected to be adopted by the Cybercrime Convention Committee (T-CY) in

- most of the e-evidence of war crimes and GHRV is likely to be shared with other Parties to the Budapest Convention which thus provides a legal basis for such cooperation;
- cyberattacks, including against state, critical infrastructure and civilian targets, are criminalized under the Budapest Convention[4] and Parties are able to cooperate with each other in the investigation and prosecution of such offences.[5]

The Council of Europe, under the CyberEast joint project of the European Union and the Council of Europe (2019-2023), has been assisting Ukrainian authorities and partners throughout 2022 regarding the admissibility and collection of electronic evidence from various sources, including OSINT, as well as specialised training. While the status and use of electronic evidence in criminal proceedings is an accepted practice in the criminal justice system of Ukraine, important challenges remain regarding:

- the admissibility of evidence originating from sources and information not readily verifiable through domestic investigative procedures;
- procedural powers to collect electronic evidence not yet available in the domestic law of Ukraine (such as the preservation and production orders under the Budapest Convention on Cybercrime);
- the availability and application of standard operating procedures for OSINT and e-evidence;
- capacities of criminal justice authorities to handle such evidence for use in criminal proceedings by domestic and international courts;
- channels, competencies and capacities for effective cooperation with competent authorities of other Parties to the Convention on Cybercrime in matters related the investigation and sharing of electronic evidence related to war crimes and GHRV.

Additionally, increased awareness and practical skills are needed for identifying and qualifying serious cyberattacks against civilian targets and critical infrastructure in Ukraine not only as cybercrime offences but also as elements of war crimes and GHRV, and possibly as crimes of aggression.

Given the scope, relevance and urgency of the matter, the present project is to address the specific challenge of the legal framework, rules and capacities for the use of electronic evidence and OSINT in criminal proceedings related to war crimes and GHRV in Ukraine.

The project contributes to the Action Plan for Ukraine for 2023-2026 of the Council of Europe that was agreed in December 2023. Relevant actions foreseen in that plan include:

- *"provide support for strengthening and further alignment of legal frameworks and practical tools for the purpose of investigation, prosecution and international co-operation on cybercrime and electronic evidence, particularly in view of the implementation of the Second Additional Protocol to the Budapest Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence;*
- *provide support for the full implementation of procedural powers under the Budapest Convention on Cybercrime to facilitate the investigation and collection of electronic evidence in cases of gross violations of human rights, including war crimes;*
- *strengthen European co-operation in the field of forensic science and further harmonisation of the legal framework and practical tools for conducting forensic examinations in order to investigate and prosecute economic crimes and cybercrime, taking into account their cross-border and transnational nature".*

June 2023.

[4] See also T-CY Guidance Note on critical infrastructure attacks.

[5] The dual criminality requirement is considered to be met between Parties for the offences of articles 2 to 11 of the Convention.

APPROACH

The Council of Europe has been supporting Ukraine in matters related to cybercrime and electronic evidence under the current CyberEast project and previous capacity building projects since 2011. Ukraine is a party to the Budapest Convention on Cybercrime and in November 2022 also signed the Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence.[6] The Council of Europe is thus well-placed to implement this project in cooperation with Ukrainian partners.

The overall objective (Impact) of the project is to improve the handling of electronic evidence for use in criminal proceedings related to war crimes and GHRV in the context of the Russian aggression against Ukraine. This process of change will be made possible through the achievement of the specific project objective (Intermediate Outcome) of strengthening the criminal justice capacities of Ukrainian law enforcement, prosecutors and judiciary on handling electronic evidence in criminal cases of war crimes and gross human rights violations.

The project objective (Intermediate Outcome) is to be achieved through four Immediate Outcomes, focusing on an improved regulatory framework for the use of e-evidence in criminal proceedings, stronger legal framework and skills for tackling cyberattacks against civilian targets and infrastructure, improved capacities for the collection and handling of e-evidence, and increased domestic and international cooperation on e-evidence.

The Outcomes of this project will also have an impact on capacities of Ukraine to make use of electronic evidence beyond war crimes and GHRV but with respect to any crime.

This project will complement the regional CyberEast+ joint project of the European Union and the Council of Europe, as well as other projects and initiatives in support of Ukraine. It may also feed into the Register of Damages that is to document damages caused by the Russian aggression against Ukraine.[7] The project will seek further coordination with other initiatives working on matters related to electronic evidence and OSINT of war crimes/GHRV. The Council of Europe participates in the Ukraine Accountability Dialogue Group.[8] The project may also be relevant for the Joint Investigation Team (JIT) set up by EUROJUST on core international crimes in Ukraine, and of the International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA).

The project will be managed by the Cybercrime Division of the Council of Europe in Strasbourg and Bucharest with core team based at the Council of Europe Office in Kyiv. This arrangement will help ensure synergies with other initiatives supporting Ukraine's efforts to investigate and prosecute and ensure accountability for war crimes and GHRV as well as consistency with the capacity building approach of the Council of Europe on cybercrime and electronic evidence.

[6] Ukraine is a State Party to the Budapest Convention and its First Additional Protocol since 2007, and has signed the Second Additional Protocol to the Convention on Cybercrime in November 2022.

[7] Following the 4th Summit of Heads of States and Governments of the Council of Europe in Reykjavik in May 2023, the Partial and Enlarged Agreement of the Council of Europe is being established.

[8] Workstreams 1 – Assistance to Ukraine and 2 – Action by Regional and International Organisations, and if possible Workstream 3 – National investigations.

PROJECT IMPACT, EXPECTED OUTCOMES AND ACTIVITIES

Project Impact	To improve the handling of electronic evidence for use in criminal proceedings related to war crimes and gross human rights violations in the context of the Russian aggression against Ukraine.
Intermediate Outcome	To strengthen the criminal justice capacities of Ukrainian law enforcement, prosecutors and judiciary for the handling electronic evidence in criminal cases of war crimes and gross human rights violations.
Immediate Outcome 1	Improved regulatory framework for the use of electronic evidence and OSINT related to war crimes and GHRV in criminal proceedings.
Output 1.1	Internal guidelines and operating procedures available regarding the handling of electronic evidence, ensuring the chain of custody and use in criminal proceedings.
Output 1.2	Draft legislative amendments available in view of full implementation of the procedural powers as well as articles 26 and 32 of the Budapest Convention and of the provisions of its Second Protocol.
Immediate Outcome 2	Stronger capacities to apply domestic criminal law in response to cyberattacks as part of crime of aggression directed against state, civilian targets and critical infrastructure.
Output 2.1	Increased awareness and skills for applying domestic laws and international standards in the context of cyberattacks and cybercrime against civilian targets and critical infrastructure.
Immediate Outcome 3	Improved capacities for the collection and handling of electronic evidence for use in criminal proceedings.
Output 3.1	Improved capacities of criminal justice authorities in the handling of e-evidence in criminal proceedings.
Output 3.2	Improved capacities and skills of private sector and civil society organisations regarding the handling of electronic evidence.
Immediate Outcome 4	Increased cooperation on e-evidence for use in criminal proceedings related to war crimes and GHRV.
Output 4.1	Enhanced domestic cooperation between criminal justice authorities and other authorities, partners and initiatives in matters related to e-evidence.
Output 4.2	Enhanced international cooperation between criminal justice authorities of Ukraine with international partners in matters regarding e-evidence.

CONTACT

Alexander SEGER
Head of Cybercrime Division
Alexander.Seger@coe.int
Council of Europe

Giorgi JOKHADZE
Project Manager
Giorgi.Jokhadze@coe.int
Council of Europe