XCEPT

CROSS-BORDER CONFLICT
EVIDENCE / POLICY / TRENDS

Policy brief

March 2025

Using technology to improve investigations of sexual and gender-based crimes in cross-border conflicts

Valerie Oosterveld

Executive summary

Courts and investigative bodies – both international and domestic – are increasingly turning to technology to document sexual and gender-based crimes (SGBC) in armed conflicts around the world. This policy brief, based on a longer research paper, explores case studies to examine how actors are using technology through survivor-forward, trauma-informed, and gender sensitive methods. It presents the risks posed by using technology in handling SGBC in specific contexts, highlighting where improvements are needed. Case studies explore the investigation of SGBC in the Russian invasion of Ukraine and areas in northern Iraq and Syria occupied by the Islamic State of Iraq and the Levant (ISIL). A third case study examines the long-term management of SGBC evidence and information stemming from the interlinked Sierra Leone/Liberia conflicts of the 1990s.

Together, the research finds that international and domestic justice actors are employing survivor consent and data protection measures; training staff in the use of technology; and deploying emerging technologies in SGBC cases. However, major gaps remain. To ensure more effective use of this technology, efforts are needed to: create a standardized

international framework for the use of technology in SGBC investigations; develop new technological applications to improve SGBC survivor interviews, open-source information gathering, and the utilization of artificial intelligence (AI) in SGBC analysis; and to develop a universal preservation system for SGBC evidence and information over the long term.

Key findings

Using technology in investigating and documenting conflict-related SGBC brings opportunities, but also risks, as illustrated by this project's three case-studies: Ukraine, Northern Iraq/Syria, and Sierra Leone/Liberia.

Some progress has already been made in anticipating and responding to risks. This includes in the areas of:

- **Data protection:** to mitigate the risks to survivors that their identity or experiences will be publicly revealed through hacking or poor data handling, international and domestic courts and investigative bodies have adopted rigorous data protection frameworks.

- **Better protocols around informed consent:** to ensure that SGBC survivors understand the use to which their information will be put, these bodies have also improved their informed consent protocols, especially with respect to third-party sharing.

- **Improved training:** courts and investigative bodies have also improved the technological training of SGBC investigative and documentation staff in survivor-centred and trauma-informed interview and evidence collection methods.

- **Leveraging emerging technology:** these bodies have also leveraged the use of emerging technologies to better analyse SGBC information, including to spot patterns and link ground-level perpetrators to others in the chain of command.

However, more efforts must be undertaken to improve the use of technology in this way. This policy brief recommends that actors:

- **Establish a standard framework:** the international community should create a standardized framework for the use of technology in SGBC investigations that incorporates best practices from investigators, documenters, and database managers. This would help to ensure a common international approach to how SGBC evidence is collected, stored, and used in judicial proceedings, including to preserve the narrative integrity of that evidence.

- **Develop new, fit-for purpose tools:** private technology companies should work with investigators and documenters to develop new technological applications that will improve SGBC survivor interviews, assist in the capture of SGBC-related social media posts, identify indicators of SGBC using AI in a safe and confidential manner, and avoid fragmenting survivor accounts within database management systems.

- **Create a universal information preservation system:** such a system should be developed to allow responsible actors to ensure the safety of evidence and testimonies regarding SGBC cases over the long-term.

Context

In May 2023, the Prosecutor of the International Criminal Court (ICC) explained that in order to pursue justice more effectively, new technology must be harnessed, calling the use of technology a "requirement rather than a luxury" in the current global context.[1] Clearly, technological tools are essential to the effective investigation and documentation of serious international crimes, including SGBC. Digital tools are increasingly used to collect, organise, and interpret evidence. This includes recording survivor statements, using digital photos, videos, audio files, scanned text, satellite or drone imagery, electronic maps, 3-D imaging, and voice or facial recognition programs. Databases help to manage this information, and AI is being used to identify patterns of abuse, connect perpetrators to command structures, and corroborate data. However, there is relatively little attention paid in scholarly and practitioner-oriented literature as to when and how such technology should be used in conflict-related SGBC cases, apart from a growing focus on the use of open-source digital materials in SGBC investigations.[2]

Methodology

This project involved 43 semi-structured interviews conducted between November 2022–October 2024.[3] Interviews were conducted with investigators at international criminal courts and tribunals; staff of international and civil society organizations working to document international crimes; archivists; and information technology specialists working for international investigative bodies. Interviewees were selected for their experience in SGBC investigation or documentation and/or information technology management of SGBC data. The interviews and qualitative analysis considered different contexts:

1   International Criminal Court (2023), 'ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform OTPLink', *International Criminal Court Statement,* (24 May). Available at: https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink.

2   E.g. Koenig, A., Ghaly, A., & Lieban Levine, S. (2024), 'Merging Responsibilities: Ethical Considerations for Securing Consent in Open-Source Investigations of Conflict-Related Sexual Violence', *Journal of International Criminal Justice,* 22(2), pp. 263–280. Available at: https://dx.doi.org/10.2139/ssrn.4895271; and Koenig, A., & Egan, U. (2021), 'Power and Privilege: Investigating Sexual Violence with Digital Open-Source Information', *Journal of International Criminal Justice,* 19(1), 55–84. Available at: http://dx.doi.org/10.1093/jicj/mqab014.

3   These interviews were initially funded by the University of Birmingham's Institute for Global Innovation and Institute for Advanced Studies as a pilot project, resulting in 13 interviews. The project was subsequently expanded through funding by XCEPT – Cross-border Conflicts: Evidence, Policy, Trends, resulting in a further 30 interviews.

SGBC investigations related to the invasion of Ukraine by Russia, crimes committed by ISIL in Northern Iraq/Syria, and the interlinked Sierra Leone/Liberia conflicts.

Case study 1: investigating SGBC in Ukraine

Context

Various forms of SGBC against Ukrainian civilians and prisoners of war (POWs) have been documented since the beginning of Russia's aggression in 2014. Since Russia's full-scale invasion in 2022, SGBC has skyrocketed in its gravity, frequency, territorial scope, and victim spectrum. According to the UN Independent International Commission of Inquiry on Ukraine, victims range from children to the elderly, including men and women.[4] Civilian women are the predominant victims during occupation, while in detention, both civilians and POWs, the majority of which are male, are victims.[5] Russian military and occupation authorities perpetrate SGBC against Ukrainians – which may constitute crimes against humanity or war crimes of torture, rape, enforced sterilisation, sexual slavery, and other forms of sexual violence – "with brutality, and in combination with other grave violations".[6] This includes inhuman treatment, unlawful detention, enslavement, unlawful killings, and summary executions, which may also demonstrate genocidal intent.

Ukraine's use of technology in SGBC response

Ukraine's responses to SGBC in these cases, especially since the full-scale invasion by Russia, consists of two core elements:

- **Criminal justice:** this embodies the efforts of the state, Ukrainian human rights nongovernmental organizations (NGOs), and international stakeholders to document and prosecute direct perpetrators and their commanders for SGBC. In 2022, the War Crimes Department of Ukraine's

Office of the Prosecutor General established a unit on conflict-related sexual violence (CRSV). As of November 2024, Ukraine had 326 CRSV cases, of which 117 concerned men.

- **Reparations and survivor support:** this involves reparations for medical and psychological support, vocational training, and other measures to help SGBC survivors and their families heal and feel empowered to move forward. In 2024, Ukraine implemented a pilot urgent interim reparations scheme for CRSV survivors. As of November 2024, 552 survivors (313 men, 228 women, 9 girls, 2 boys) applied for reparations. Of these, 325 survivors (168 men, 155 women, 1 girl, 1 boy) received urgent interim reparations.

State and civil society stakeholders engaged in both responses employ technology to varying extents. This is impacted by the type of response (i.e., whether it is criminal proceedings or a reparations process) and the state of response (i.e., with or without survivors' engagement). Across both tracks, the role of technology was analysed in interviews and included:

- **Server security:** server security is foundational to ensuring the integrity of collected data and, crucially, survivors' private information (and therefore personal security). Prosecution and reparation teams have adopted different strategies. Those who keep servers with SGBC information within Ukraine point to Ukraine's expertise with repelling cyber-attacks. Those who use international servers did so due to the cyber security reputation of a chosen jurisdiction and emphasised that only a limited number of professionals have access to the server-stored information, through a multi-step authentication process.

- **Engagement with survivors:** in prosecution and reparation processes involving technology, survivors emphasised that they require clear and respectful explanations of how the information they provided will be digitally stored and used, and the security protocols that will be applied. They also indicated that they preferred communication from trusted interlocutors, especially fellow survivors further along in their recovery from

---

4   Independent International Commission of Inquiry on Ukraine (2023), *Conference room paper,* (29 August, A/HRC/52/CRP.4), para. 567; para 599. Available at: https://www.ohchr.org/en/documents/reports/ahrc52crp4-conference-room-paper-independent-international-commission-inquiry.

5   Ibid., para. 575.

6   Ibid., para. 567.

trauma, civil society lawyers, paralegal professionals, and psychologists.[7]

- **Open-source investigations:** both criminal justice and reparations investigations analyse non-confidential open-source public data (such as social media posts) for evidence of conflict-related SGBC. In Ukraine, the main tech-related concern for both is identifying AI-created and other artificially generated images, specifically designed and planted in the public domain as a form of disinformation to compromise investigations.

Challenges and responses

Technological training

Many criminal justice professionals involved in SGBC investigations in Ukraine lack proper training in the use of new technologies that have been introduced. This had led investigators to make operational mistakes while conducting interviews and/or working with evidence, resulting in the production of inadmissible records, or in some cases, even loss of testimonies and evidence. While technology can enhance efficiency in investigative processes, it must be used correctly to ensure a survivor-centered approach.

Nature of SGBC:

Criminal justice professionals and civil society representatives stated that the particular features of conflict-related SGBC, namely that it is usually perpetrated indoors, can make technologies like satellite or drone imagery less useful for investigations (except to place a perpetrator in the area around the time of the SGBC). However, facial and voice recognition programs are useful in identifying alleged perpetrators when a comparative analysis of oral or photo samples is possible.

Transcription software:

SGBC survivors in Ukraine are not always ready to communicate with more than one investigator in the room and many decline consent to any type of recording beyond written notes. This can hamper a more traditional two-person documentation approach (with one person asking questions and another recording the exchange), which often cannot be used. As a result, investigators highlighted

the need for the development of accessible software that accurately transcribes oral questions and answers, or that can turn written notes into typewritten transcripts. Such technology would allow the interviewer to keep their attention on the interviewee and would improve the efficiency and accuracy of the recorded testimonies.

Information preservation:

The international community has not yet developed a coherent or long-term approach to the storage of investigative materials—including SGBC evidence with survivor identities—once the responsible authority has concluded its mandate. Therefore, investigators are calling for the development of technological solutions for reliable long-term preservation and protection of SGBC evidence and testimonies, following a standard universal practice.

Policy recommendations

Recommendations for the Government of Ukraine:

- Regularly review and assess the security of servers handling SGBC information, including the rationale for using domestic or international servers.

- Assess the reliability of private technology companies providing support for Ukraine's SGBC responses considering the changing geopolitical climate.

- Prioritise survivor communication, ensuring that at all stages of prosecution and reparation processes, survivors are informed in a respectful and understandable manner about how their information will be stored and used.

- Equip frontline staff with adequate technological support, including transcribing and translation needs, especially to persons interviewing or otherwise engaging with survivors.

Recommendations for Ukraine's international partners:

- Ensure sustained, uninterrupted, and adequate funding for Ukraine's state and civil society responses to SGBC.

---

7   Paralegal professionals and psychologists are increasingly involved in interviewing survivors and in reparations case-management.

- Jointly explore avenues for technological development that will ensure accessible software options for effective and survivor-centered interviewing and documentation in SGBC cases.

- Help to develop a universal information preservation system that will allow responsible actors to ensure the safety of evidence and testimonies regarding SGBC cases over the long-term.

Case study 2: SGBC in ISIL -controlled Iraq and Syria

Context

In June 2014, ISIL gained control of large areas in northern Iraq and eastern Syria, taking advantage of the ongoing civil war in Syria and military disintegration in Iraq. The rise of ISIL led to significant reports of SGBC. Following an attack on the Yazidi community in Sinjar in Northern Iraq in August 2014, the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ ISIL (UNITAD) documented several patterns of ISIL SGBC.[8] These crimes were particularly against women and girls, starting with the initial capture of victims and separation from their families, at detention sites, in the *sabaya* (sexual slavery) system, and in forced and child marriages. It found that such acts amounted to war crimes (particularly rape, torture, and sexual slavery), crimes against humanity (including persecution), and genocide. [9]

Overview of the use of technology in documenting ISIL SGBC against Yazidis

Local NGO's leveraging technology:

In response to ISIL's SGB crimes, particularly those against the Iraqi Yazidi community, the NGO 'Yazda' was established. A crucial part of Yazda's work involves using technology for legal advocacy, evidence documentation, and cooperation with prosecuting and judicial authorities. Yazda has gathered over 3,000 testimonies from survivors, providing invaluable information for prosecuting ISIL

crimes. This role has increased following UNITAD's closure in September 2024. Due to a lack of pre-existing organizational infrastructure and translation resources, Yazda built its own system for collecting and categorizing survivor testimonies to ensure proper documentation and efficient retrieval of information for legal proceedings.

Challenges and responses

Security of SGBC information:

As in the case of Ukraine, SGBC survivors are concerned about the security of digital information shared. UNITAD implemented stringent security protocols, which influenced the approach of investigators and organizations in the region to:

- Code the SGBC testimonies to ensure that they remain anonymous.

- Store data on cloud-based platforms when not confidential and hardware platforms for confidential data to prevent loss or unauthorized access.

- Limit who has internal access to the data – i.e. record the date, time, and purpose of accessing it, and comply with the legal chain-of-custody principle – to optimise evidence admission in potential future judicial proceedings.

- Limit external access to the data. Only share evidence via secure platforms and use two-factor authentication and other access restrictions to maintain security.

- Regularly train staff members on data protection and documentation methodologies ensuring they handle SGBC testimonies appropriately.

Some survivors are willing to participate in video interviews if given the opportunity to inspect recording equipment beforehand, which allows them to feel more in control of the process. Yazda also provides English transcriptions of these interviews, which assists law enforcement agencies receiving the information. Additionally, investigators use open-source information and satellite imagery to confirm the crime locations and identify the perpetrators named by the survivors. This technology-driven

8   UNITAD (2023), *Report on Sexual Violence Against Women and Girls Committed by ISIL in Iraq.* Available at: https://www.unitad.un.org/
     sites/www.unitad.un.org/files/scgb_report_e-report_en-.pdf.

9   Ibid., paras. 97-151.

approach helps to substantiate survivor testimonies and strengthens universal jurisdiction cases against perpetrators.

Informed consent of SGBC survivors:

One of the fundamental principles guiding Yazda's work is the emphasis on SGBC survivor consent to the interview, and to the use of technology to capture what was said. This requires building trust, including through understanding the survivors' cultural beliefs and practices, especially in adherence to the 'do-no-harm' principle. Yazda's 'Get to Know Me First' guide for non-Yazidi investigators provides practical guidance on Yazidi religion, history, language, taboos, and gender norms.[10] Further, building trust involves providing psychological support to survivors, as the documentation process can be retraumatizing. SGBC survivors are also given clear information about the purpose of the interview, how their testimonies will be used, where the data will be stored, and what measures are in place to protect their privacy. If their interview becomes relevant for a third state proceeding, they are contacted again and provided with information about the specific request and their rights and obligations in that jurisdiction.

'Locked-up' SGBC evidence:

UNITAD digitally collected and stored extensive amounts of confidential SGBC evidence during its operation from 2018-2024. When its mandate was abruptly ended in 2024, control of this database was turned over the United Nations (UN) Secretariat, as well as partially to Iraqi authorities, amidst SGBC survivor concerns about the long-term safety, security, confidentiality, and accessibility of their information, and respect for their levels of consent. There were also concerns about the potential to re-traumatise survivors, who had already provided testimonies to UNITAD, if they were required to provide these again to other entities to seek justice and accountability.[11]

Furthermore, the UN Secretary-General confirmed that the UN Secretariat could not guarantee that evidence had been preserved in accordance with international criminal law standards, including

chain-of-custody and integrity of data.[12] Thus, it was unlikely to be useable in court proceedings as evidence.[13] This case highlights the very real risks of SGBC evidence becoming 'locked up' in databases associated with international investigative mechanisms, once their mandates have ended and funding is cut.

Policy recommendations

International, governmental, civil society, and private partners all have a role to play in strengthening and developing technology to further advance SGBC investigations and documentation. This can be achieved by the following methods:

- **Develop tools to facilitate evidence gathering:** Create automated translation software in minority languages spoken in conflict zones, to facilitate the transcription and translation of SGBC survivor testimonies.

- **Create social media archiving tools:** Provide accessible yet secure (for chain-of-custody) social media archiving tools that meet evidentiary standards.

- **Design bespoke training:** Develop accessible training to SGBC documentation organisations on how to safely and securely investigate the dark web and encrypted platforms such as Telegram.

- **Support development of AI tools:** Deploy AI designed to be gender-sensitive (and not gender-biased) to improve SGBC data management. For example, AI could automate deduplication processes, increasing efficiency and reducing the workload of human analysts.

- **Ensure collaboration on the use of AI:** Ensure that legal professionals, investigators, and NGOs collaborate with tech specialists to improve methods of documentation and receive clear guidance and training on the safe and secure use of AI.

- **Develop a standardised framework:** A standardised framework for the use of technology in SGBC investigations should be developed that

---

10   Yazda (2023), *'Get to Know Me First': A Survivor-Informed Guide for Interviewing Yazidis from Sinjar.* Available at: https://www.yazda.org/publications/get-to-know-me.

11   Report of the United Nations Secretary-General, *Implementation of Resolution* 2697 (2023), (UN Doc. S/2024/20 - 15 January 2024), para 21. Available at: https://digitallibrary.un.org/record/4034240/files/S_2024_20-EN.pdf.

12   Ibid., para. 22.

13   Ibid.

incorporates best practices from interviewers and database managers. This would help to ensure a common international approach to how SGBC evidence is collected, stored, and used in judicial proceedings.

Case study 3: long-term storage of SGBC Data - the Sierra Leone and Liberia context

Context

SGBC were widespread during the armed conflicts in both Sierra Leone (1991–2002) and Liberia (1989–2003).

In Sierra Leone, Human Rights Watch estimated that between 215,000–257,000 women and girls of all ages, ethnic groups, and socio-economic classes may have been subjected to sexual violence in the conflict.[14] The Sierra Leone Truth and Reconciliation Commission (2000-2004) recorded these crimes extensively, which included cases of threatened and actual rape; sexual slavery; forced pregnancy; enforced sterilization; sexualized torture; gendered forms of enslavement (such as forced domestic labour); sexual mutilation; and forced nudity.[15] The Special Court for Sierra Leone convicted wartime leaders for numerous gender-related crimes.[16]

In Liberia, the Liberian Truth and Reconciliation Commission (2005-2009) recorded high levels of SGBC during the armed conflict. This included cases of forced nudity; sexualized torture; sexual mutilation of both men and women; and various forms of rape, sexual slavery, forced pregnancy, forced abortion, and disembowelment of reproductive body parts directed against women and girls.[17] Females

targeted for sexual violence were, on average, 15-19 years old.[18]

The archives of these commissions, including SGBC related documents, are preserved in different locations. The Sierra Leone Truth and Reconciliation Commission's documents (including those on SGBC) are archived at the Sierra Leone Peace Museum, and the Liberian Truth and Reconciliation Commission's documents are archived at the Georgia Institute of Technology in the United States.[19] The Residual Special Court for Sierra Leone manages the archive of the Special Court for Sierra Leone. These institutions have experience with the long-term management of SGBC information and evidence over the course of decades.

Lessons on the long-term management of digital SGBC evidence and information

In certain respects, the management of digital SGBC evidence and information over the long term is similar to management in the shorter term. Digital information must be subject to clear access and tracking protocols, with different levels of access for different actors and types of evidence. For example, the identity of survivors who presented SGBC evidence under protective measures must be kept confidential as long as is needed to protect them, which could be decades. Access to this evidence must only be granted to those required to know the survivors' identities, such as those who oversee victim and witness protection. Importantly, the Special Court for Sierra Leone designed the victim/witness digital statement storage process to take into account the need for different levels of confidentiality and security and their maintenance over time.

On the other hand, such long-term management presents special requirements: digital systems require constant upgrading and maintenance which can be expensive for organisations. Such systems also require ongoing training for staff, collaboration

14   Human Rights Watch (2003), *'"We'll Kill You if You Cry": Sexual Violence in the Sierra Leone Conflict',* (January). Available at: https://www.hrw.org/report/2003/01/16/well-kill-you-if-you-cry/sexual-violence-sierra-leone-conflict. No estimates are available regarding the prevalence of conflict-related sexual violence directed at men and boys.

15   Sierra Leone Truth and Reconciliation Commission (2004), *Witness to Truth: Final Report of the Sierra Leone Truth and Reconciliation Commission,* Volume 3(B), Chapter Three, Women and the Armed Conflict in Sierra Leone, paras. 203–328. Available at: https://www.sierraleonetrc.org/index.php/view-the-final-report/download-table-of-contents.

16   E.g. Special Court for Sierra Leone (2009), *Prosecutor v. Sesay, Kallon & Gbao,* SCSL-04-15-T, Trial Judgment, 2 March; SCSL-04-15-A, Appeals Judgment, 26 October.

17   Republic of Liberia Truth and Reconciliation Commission (2009), *Final Report,* (Volume 3, Appendices, Volume 1: Women and the Conflict), pp. 31, 35–41. Available at: https://www.sierraleonetrc.org/index.php/view-the-final-report/download-table-of-contents.

18   Ibid., at 29.

19   Crawford, J. (2020), 'Why Liberia's TRC Archives Stay in a US University', *JusticeInfo.Net,* 9 June. Available at: https://www.justiceinfo.net/en/44506-why-liberia-trc-archives-stay-in-us-university.html.

with other organisations using the same archiving platform, and frequent evaluations of the system so that it can be adapted to evolving technology. Evidence that presents security risks, if made public, might need to be stored on secure 'air-gapped servers' (which are not connected to the internet).

After the original time-limited mandate of the court ends, residual versions of these courts may require ongoing access to the evidence for judicial processes, witness protection, and official requests from other justice bodies for information, all of which are important in SGBC cases. There is also a related need to preserve evidence and information classified as public, for researchers and for public knowledge of the realities of the war, to guard against historical revisionism, especially regarding the use of SGBC during the conflict.

Policy recommendations

To ensure that evidence of SGBC remains secure, accessible, and useful for future accountability, the following recommendations are proposed:

- **Plan for long term storage from the start:** Planning for the long-term retention and protection of SGBC (and other) evidence and information should begin from the inception of an international court or investigative body. This must include financial planning of who will fund the storage, maintenance, security, and preservation of the digital data over decades. Ideally, the digital data should be managed over time by the organisation that originally collected the data.

- **Ensure adequate training and SGBC expertise:** Those handling the digital data over the long term should be trained in SGBC-specific security and preservation aspects of evidence and information. They should also be connected with other institutions to share best practices on handling SGBC data over the long term.

- **Promote responsible public access:** It is important for the population of the conflict-affected country, and others, to be able to access digital information or evidence classified as public over time, including to ensure awareness about, and to prevent future revisionist denials of, the gravity, breadth, or types of SGBC that took place in conflicts.

About the author

Dr. Valerie Oosterveld is the Western Research Chair in International Criminal Justice and a Professor at the Faculty of Law, University of Western Ontario, Canada.

Acknowledgements

About XCEPT

The Cross-Border Conflict Evidence, Policy and Trends (XCEPT) research programme brings together world-leading experts and local researchers to examine conflict-affected borderlands, how conflicts connect across borders, and the drivers of violent and peaceful behaviour. Funded by UK International Development, XCEPT offers actionable research to inform policies and programmes that support peace. The views expressed in this material do not necessarily reflect the UK government's official policies.

www.xcept-research.org.

Contact

Contact for XCEPT:
info@xcept-research.org.

XCEPT

CROSS-BORDER CONFLICT
EVIDENCE / POLICY / TRENDS

UK International Development

Partnership | Progress | Prosperity