Joint Submission by Access Now and the Border Violence Monitoring Network to the United Nations (UN) Special Rapporteur on the Human Rights of Migrants for Report to the UN General Assembly on the Externalization of Migration and the Impact on the Human Rights of Migrants

10 June 2025

Access Now As an ECOSOC accredited organization, Access Now routinely engages with the United Nations (UN) in support of our mission to extend and defend digital rights of people and communities at risk As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

The Border Violence Monitoring Network (BVMN) is a network of 14 organisations documenting human rights violations, particularly pushbacks and collective expulsions at EU external borders, particularly in the Western Balkans, Poland, Greece, Cyprus and Turkey. The collection of data is done, depending on the location, by a consortium of independent field experts who are part of or cooperate with humanitarian support groups united through the Border Violence Monitoring Network, or researchers collecting data through secondary sources. Since 2021, the Border Violence Monitoring Network has been conducting research and investigations on the role of border technologies in the occurrence and financing of border violence and in particular collective expulsions.

Introduction

Access Now and BVMN welcome the opportunity to provide input to the UN Special Rapporteur on the Human Rights of Migrants (UN Special Rapporteur) to inform the UN Special Rapporteur's upcoming report "Externalization of Migration and the Impact on the Human Rights of Migrants" to be presented to the UN General Assembly during its 80th session.[1] This submission is divided into three main sections.

[1] United Nations Office of the High Commissioner for Human Rights, UN Special Procedures. Call for inputs: Externalization of Migration and the Impact on the Human Rights of Migrants, (2025), Available at: https://www.ohchr.org/en/calls-for-input/2025/call-inputs-externalization-migration-and-impact-human-rights-migrants

First, the role of technology in externalizing border control. Second, the role of biometric infrastructure in externalisation practices. And finally, the fundamental rights implications of border technologies.

The submission mainly draws on the experience from European and U.S. border control. It is important to note that while this submission draws upon specific case studies and concrete examples, these are non-exhaustive, and do not represent the lived experiences of all persons at risk. More information is required to take into full account the intersecting forms of oppression of those who are directly impacted.

I) The role of technology in externalizing border control: European border management

1. Externalisation has been one of the key strategies in EU border management and has expanded significantly in the past ten years. As a first major effort to externalize EU border control, following the 2015 so-called "refugee crisis", the EU signed the so-called EU-Turkey Deal, criminalizing the crossing of the Aegean sea in search of safety.[2] This deal resulted in individuals getting "stuck" on the Greek Aegean islands, unable to return to Turkey or move to the EU-main land, many of them now detained in prison-like detention centres.[3] In parallel the EU poured billions of euros into Turkey [4] and border patrolling programmes.[5]

Funding for Border Surveillance as an instrument of EU border externalisation

2. Supporting border technologies has been one of the primary strategies of EU border externalization. The Western Balkans are a key location of EU border externalisation, where the prospects of EU and Schengen Accession are closely tied to the procurement of border surveillance equipment and training programs.[6] Border surveillance and biometric technologies at non-EU borders are often funded by EU pre-accession funding (IPA), with the goal of preventing individuals from reaching EU borders in the first place.[7]

    a. On October 25th 2022, the European Commission adopted a new assistance package to 'strengthen border management' in the Western Balkans.[8] The package, worth 350 million euros, is intended to go towards migration management systems such as surveillance and detention centres as well as returns. This also includes the expansion of the European Border and Coast Guard Operations in non-EU countries in the Western Balkans. [9]

---

[2] Access Now. Surveilling Europe's edges: when digitalisation means dehumanisation (2025). Available at: https://www.accessnow.org/digital-surveillance-european-borders-part-1/

[3] Medecins Sans Frontières (2021) "Constructing Crisis At Europes Borders" available at: https://www.msf.ch/sites/default/files/2021-06/20210610_rep_greece_hotspot.pdf

[4] European Commission. EU Support to Refugees in Türkyie. Available at: https://enlargement.ec.europa.eu/enlargement-policy/turkiye/eu-support-refugees-turkiye_en

[5] Barely a month earlier, the EU had forced North Macedonia to shut its border with Greece, thereby trapping more than 35,000 people beyond its borders. For more information see: https://www.theguardian.com/world/2016/mar/09/balkans-refugee-route-closed-say-european-leaders

[6] BVMN Surveillance Technologies at European Borders. Assessments by the Border Violence Monitoring Network. (2024) https://borderviolence.eu/uploads/document/file/438/Ex.-Summary-draft.pdf

[7] Kosta, E. (2017). Integrated border management in the EU: The Albanian experience.

[8] European Commission. (2022.) The EU increases support for border and migration management in the Western Balkans. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6276

[9] Frontex (2021) Frontex and Slovenian Presidency host high-level meetings with Western Balkan partners. Available at: https://frontex.europa.eu/media-centre/news/news-release/frontex-and-slovenian-presidency-host-high-level-meeting-with-western-balkan-partners-tLLEDP

b. According to research by PICUM, 75 % of the European Union's Border Management and Visa Instrument (BMVI) Fund was spent on Technology and Border Infrastructures between 2021 and 2024. This includes a significant amount to be redistributed to third countries to support the management of "irregular flows", including via technologies, training and the deployment of immigration liaison officers.[10] This is only the tip of the iceberg as significant funding for border surveillance is also distributed via the AMIF[11], ISF[12] and IPA funds.

3. Beyond the deployment of advanced surveillance technologies and training, new border policies aligned with the EU Integrated Border Management Strategy[13], are also most often a prerequisite for the advancement on the paths towards EU or Schengen Accession for Western Balkan States. However, in some countries, such as Albania and Bosnia, despite the EU-funded advances in border surveillance, EU accession remains a distant dream.[14]

Purpose and Functioning of Border technologies

4. Border surveillance technologies deployed by the EU outside of EU borders, primarily serve the purpose of detecting and monitoring movements, and allow for the efficient detection and classification of movement into "legal" or "illegal" contrary to the individual right to seek asylum. Research by the Border Violence Monitoring Network (BVMN) conducted in seven countries along the so called "Balkan Route", as well as testimonies from people on the move in the BVMN Database, confirmed that the deployment of so-called situational awareness technologies often helps facilitate the apprehension and subsequent pushback of people on the move.[15]

5. Some documented cases include the indiscriminate use of situational awareness technologies such as drones, radar and advanced cameras systems to facilitate the deterrence and illegal pushbacks of individuals including women, elderly, and minors.[16]

6. While reports of illegal pushbacks and inhuman and degrading treatment are widespread and systematic, the surveillance technologies placed along the border are rarely used to monitor or

[10] PICUM (2024) Beyond walls and fences: EU funding used for a complex and digitalised border surveillance systeM available at: https://picum.org/wp-content/uploads/2024/07/Beyond-walls-and-fences_EU-funding-used-for-a-complex-and-digitalised-border-surveillance-system.pdf

[11] Asylum and Migration Fund

[12] Internal Security Fund

[13] The EU Integrated Border Management Strategy was adopted in 2006 and aimed at an "integrated and global response" to the challenges posed by the phenomenon of irregular immigration through the common external border.

[14] In 2014, Albania began adopting an Integrated Border Management Strategy, a vital precondition for Albania accession to the EU. development of the IBM in Albania has, in large part, been funded by the EU. Since then Frontex has largely expanded its influence in Albania, with an operational mandate at its key border locations, yet EU Accession talks are still under way.

[15] Between 2014 and 2020, Pre-accession funding and support from the EXBS, German Federal Police, IOM, UNHCR, and the EU enabled Albania to acquire 70 border patrol vehicles - almost an entire fleet. Additionally, the Albanian State Police were able to purchase a number of advanced surveillance technologies for the surveillance of its southern Green Border with Greece, including thermal cameras, long-range night vision cameras and binoculars as well as comprehensive border surveillance systems. Additionally, in 2018 under the project "For strengthening the capacities of the Border Police to fight illegal migration" Albania received 6,000,000 euros from the European Commission. This went towards the purchase of "navigational vehicles of different capacities for surveillance, border surveillance systems (TVV Vans), mobile devices for border surveillance (thermal cameras, day and night binoculars) as well as devices for border checks at BCPs.

[16] Border Violence Monitoring Network (2022) They started beating us for almost five minutes everywhere in our body. We were screaming, 'please sir, please sir' but they didn't care about what we were saying Available at: "https://borderviolence.eu/testimony/june-11-2022-0500-palli-greece-to-uyuklutatarturkey"

investigate human rights violations. Interviews with border authorities across the Balkans reveal the perception that donated border surveillance equipment are solely deployed for monitoring irregular crossings and cross-border crime. Technologies appear not to be used for rescue even if some public documents explicitly mandate such a use, and the selective use of technology exposes people on the move to forms of border harm, such as abandonment and non-rescue. For example, when people on the move were stranded off islets in the Evros river between Greece and Turkey, authorities have repeatedly claimed being unable to locate people despite the use of technical means.[17]

II) The role of biometric infrastructure in externalisation practices

7. The digital infrastructure used to monitor and manage migration flows — as from Latin America to the United States' southern border — relies heavily on the collection and processing of personal data, particularly biometrics. While the use of digital technologies in border control is not new, the scale and scope of data collection — especially the autonomous processing and cross-border exchange of migrants' personal data — has grown significantly in recent years. Biometric data, such as fingerprints and facial scans, are now routinely collected at multiple border entry points, and increasingly often even before the arrival at a border point.[18]

8. Particularly concerning is the transfer and processing of this data by authorities of other countries, often without migrants' knowledge or consent. These exchanges are facilitated through both binding and non-binding international agreements, such as a the non-binding Memorandum of Cooperation (MOCs) signed by the United States[19] with countries including Mexico, Guatemala, Honduras, and El Salvador. Their implementation includes technical support and training to deploy the data processing technology. Most of these agreements are introduced for national security — to "suppress criminal activities and threats to domestic security"[20] — despite having no public evidence supporting this claim.[21]

    i. Some of these agreements, such as the MOC between the United States and El Salvador, permit the transfer of biometric data not only of individuals who have crossed borders, but also of those merely suspected of planning to migrate.[22] This practice undermines the presumption of innocence and subjects individuals to surveillance and profiling before any action is taken. Such widespread and opaque tracking — enabled by insufficient transparency, oversight, and legal

[17] BVMN (2024) Surveillance Technologies at European Borders: Assessment on Evros. Available at: https://borderviolence.eu/uploads/document/file/437/Border-surveillance-in-Evros.pdf BVMN (2024). See also:
[18] Angela Alarcon and Franco Giandana Gigena, *"Smart borders" and the making of a humanitarian crisis* (13 March 2024) available at: https://www.accessnow.org/smart-borders-and-the-making-of-a-humanitarian-crisis/
[19] Franco Giandana Gigena, *Alerta migrante: tus datos biométricos pueden estar siendo intercambiados con EEUU,* Access Now, (17 March 2023), available at: https://www.accessnow.org/acuerdos-datos-biometricos-migrantes/
[20] Memorandum of Understanding between the Department of Homeland Security of the United States of America and the Civilian National Police of the Republic of El Salvador concerning the process and exchange of information on Salvadorian nationals repatriated to El Salavador. Available at: https://immigrationlitigation.org/wp-content/uploads/2022/10/IARC-ICE.pdf#page=6
[21] Access Now (2023) Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data. Available at: https://www.accessnow.org/press-release/statement-terminate-agreements-biometric-data-migrants/
[22] Ibid.

safeguards — poses serious risks to migrants' safety, dignity, and fundamental rights.

b. Lack of transparency and regulation with regard to data sharing is a key concern, especially considering that in many of the involved countries, weak or non-existent data protection frameworks fail to provide effective accountability or recourse. As a result, migrants are treated less as rights-holding individuals and more as data points in an expansive, transnational surveillance system. This unchecked use of data and biometrics not only reinforces harmful power imbalances but also jeopardizes the very possibility of safe and dignified migration, sometimes even with support from international or intergovernmental agencies with an alleged human rights or humanitarian mandate.[23]

c. The sharing of life-threatening information concerning people on the move occurs despite the evident corruption by the enforcement authorities processing those data

    i. El Salvador has been under a state of exception that has been extended for more than a year, enabling mass arbitrary detentions and human rights violations.[24] It has also allowed Salvadorean authorities to submit false gang affiliation, abusive INTERPOL Red Notices,[25] and other inaccurate information that has later been used [26]by U.S. authorities to deny asylum and for police harassment. The detention of individuals with no legal basis or without a formal accusation constitutes a disproportionate use of the force, and such an authoritarian state should not be trusted for data transferring.

9. The BVMN, through its member organisations, routinely collects testimonies of people forcibly pushed back across EUropean borders, and of the violence they experience during the process. Of the 1824 pushback testimonies uploaded in the BVMN database, 281 testimonies recount incidents in which the fingerprints and facial images of people were forcibly taken prior to being pushed back. Of the 281 testimonies, 265 expressed their intention to apply for asylum prior to being pushed back without access to the asylum procedure.

    a. In a testimony from the 28th of February 2023 a respondent describes being pushed back from Republika Srbska (BiH) to Serbia. *"They were taken to a small police station that was close to the bridge. The respondents described it as a small white building. In this building they were taken to a room that they described as an interrogation room equipped with cameras. (..)The respondents were hesitant to give their fingerprints but they were told that they have to do this. One of the respondent's details how they violently forced his hand onto the machine which scans the fingerprints. The uniformed men also took pictures of the boys' faces and eyes. (...). At no point was there a translator present or any*

[23] Jacob Goldberg and Hamshika Krishnamoorthy, *IOM's digital tool aims to speed up migrant removals, but at what cost?* (18 May 2025) available at: https://www.thenewhumanitarian.org/investigations/2025/05/19/iom-rcms-digital-tool-aims-speed-migrant-removals-what-cost; See also Ángela Alarcón, Franco Giandana Gigena, and Giulio Coppi, *"Smart borders" and the making of the humanitarian crisis*, Access Now (14 March 2024), available at: https://www.accessnow.org/smart-borders-and-the-making-of-a-humanitarian-crisis/
[24] Grant W. (2023) Mass arrests bring calm but at what price? Available at: https://www.bbc.com/news/world-latin-america-65596471
[25] Access Now Rights groups call for investigation: U.S. relies on unreliable information in immigration screening and adjudications. Available at: https://www.accessnow.org/press-release/a-call-for-investigation-u-s-reliance-on-unreliable-information/
[26] Ibid.

effort made to contact one, as per the respondents. They were then forced into the back of the van, driven over the border for two hours and left to their own devices by the roadside in Serbia." [27]

10. The collection of biometric data prior to being pushed back raises serious questions regarding the principle of purpose limitation and the protection of personal data. The process of collecting fingerprints and facial images serves the purpose of identification of the person within the asylum procedure, however in the case of pushbacks individuals are prevented from accessing the asylum procedure and any other administrative procedure questioning the purpose of the collection of personal data in the first place. The collection of their biometric data is not accompanied by the safeguards foreseen in the GDPR—namely, the provision of information regarding what data is being collected, for what purpose, who will have access to it, and where and for how long it will be stored, raising serious data protection concerns. [28]

11. In the EU, biometric data on people on the move is typically stored in EURODAC,the EU-wide information system which processes the fingerprints of asylum seekers and certain categories of 'irregular migrants' upon their entry to any EU Member State. The database was made operational in 2003, initially created for "the effective implementation of the Dublin mechanism,"[29] which designates the EU Member State responsible for processing the asylum application of a third-country national or stateless applicant. EURODAC is only accessible to EU member states and key EU agencies. However in recent years the EU has made significant efforts to expand the creation of EURODAC-like databases outside of the EU that can become interoperable with key EU databases and facilitate data sharing.

12. This effort is driven by the European border and coast guard agency Frontex, and involves financial and technical assistance to the development of relevant IT systems as well as support in the effort to expand biometric data collection to non-EU countries . Through bilateral agreements with Western Balkan Countries including Serbia, Albania and North Macedonia, both Europol and Frontex are expanding their access to biometric data, under the pretext of the fight against migrant smuggling. [30]

13. As a result Frontex has access to a broad range of data pertaining to migration and asylum processes in the Western Balkans, which, without adequate safeguards, potentially bypasses legal limitations on the exchange of personal data and poses significant risks to the fundamental rights of people on the move. Frontex is bound under Regulation 2018/1725 [31] which governs the

[27] Border Violence Monitoring Network (2023) "Denied any medical assistance after falling from a bridge." Available at: https://borderviolence.eu/testimony/27925-2
[28] Privacy International & Border Violence Monitoring Network (2023) Decoding BalkanDac. Available at: (https://borderviolence.eu/app/uploads/Balkandac-report-2.pdf
[29] Vavoula, Niovi. (2020). Transforming Eurodac from 2016 to the New Pact. ECRE. Available at: https://ecre.org/wp-content/uploads/2021/01/ECRE-Working-Paper-Transforming-Eurodac-from-2016-to-the-New-Pact-January-2021.pdf
[30] Privacy International & Border Violence Monitoring Network (2023) Decoding BalkanDac. Available at: (https://borderviolence.eu/app/uploads/Balkandac-report-2.pdf
[31] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725

protection and sharing of personal data by EU agencies and institutions. According to the regulation, any sharing of data with third countries must be preceded by an 'adequacy decision' from the Commission which confirms that the national legislation sufficiently safeguards data protection rights (Art 47). In the absence of such a decision, data can still be exchanged pursuant to other safeguards (Art 48) such as a legally enforceable instrument or standard data protection clauses among others. In the research for this submission adequacy agreements between the Commission and Western Balkan accession states could be found.

14. The expansion of data sharing between EU and non-EU countries both through the development of increasingly interoperable databases as well as the expansion of the powers of EUROPOL and Frontex under the pretext of the fight against smuggling, creates serious concerns with regard to the fundamental rights of people on the move. In particular, EUROPOLs power to share personal data with third countries puts individuals at risk who may fear political persecution at home.[32] In the context where advanced biometric technology, for example facial recognition, is used for biometric matching, the risk of misidentification and false accusations are particularly high given the proven inaccuracy of the technology on racialized communities. [33]

The role of technologies in exacerbating violations of non-refoulement and collective expulsions and illegitimate returns

15. Situational awareness technologies play a role not only in detecting people on the move, but also in apprehending them, and eventually in facilitating the illegal pushback and collective expulsion of individuals seeking asylum in Europe. Cooperation with non-EU countries, including through the export of surveillance technologies, is essential in facilitating this process.

    a. The cooperation between the EU, Cypriot and Lebanese authorities for maritime patrols is a key example of the connection between technology, illegal pushback and the externalisation of migration control.[34] In May 2024, the EU, Cyprus and Lebanon announced a €1 billion aid deal of which €200 million were meant for bolstering Lebanese border and migration management. The deal allowed Cypriot authorities to patrol international waters and use maritime surveillance equipment to identify key locations of intervention. Reports by people on the move and human rights organisations such as Human Rights Watch, confirm that helicopters, drones and shore-based cameras were used to detect boats that were subsequently pushed back to Lebanon. In related research, Human Rights Watch also exposed that those pushed back to Lebanon were subsequently pushed back to Syria during the brutal Assad rule, violating non-refoulement.[35]

[32] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:32022R0991&from=EN
[33] Protect Not Surveil (2025) "Stopping the unfettered expansion of Europols Digital Surveillance Powers against Migrants: A position paper on the European Commission's proposal for a Regulation to enhance Europol's support in 'preventing and fighting migrant smuggling' available at: https://protectnotsurveil.eu/uploads/ProtectNotSurveil-Europol_Paper.pdf
[34] Border Violence Monitoring Network (2024) Surveillance Technologies at European Borders : An assessment of Cyprus. Available at: https://borderviolence.eu/uploads/document/file/440/BVMN-Border-Technologies-Cyprus.pdf
[35] Human Rights Watch (2024) Lebanon/Cyprus: Refugees Pulled Back, Expelled, Then Forced Back to Syria. Available at: https://www.hrw.org/news/2024/09/04/lebanon/cyprus-refugees-pulled-back-expelled-then-forced-back-syria

16. Beyond illegal pushbacks, even official return processes are also impacted by the use of technologies for border externalisation.

    a. The Readmission Case Management System, or RCMS, an EU funded and IOM implemented project, was developed to enable real-time coordination and data exchange between EU and non-EU border authorities.[36] However, it may have been used to deport migrants who had legal permission to stay in the EU, as well as asylum seekers who only agreed to be sent home to avoid detention. The lack of oversight and possible abuse of this tool, raises serious concern with regard to possible violations of the principle of non-refoulement.

    b. Starting in 2017, IOM oversaw the development of separate RCMS platforms for Bangladesh, Pakistan, and Sri Lanka. Border authorities in these countries can use RCMS to correspond in real time with their European counterparts, exchange migrants' personal and biometric data, set up interviews, and issue travel documents after they have been ordered to leave the EU. According to the information publicly available, there is no oversight on how the tool is used and by whom, making it impossible to monitor possible violations of international law. While IOM can only support so-called "voluntary return", Human Rights Watch and other human rights organisations have argued that the "prospect of indefinite abusive detention" in countries of return such as Libya, seriously question the voluntariness of returns. Between 2017 and 2019 IOM was accused of facilitating the removal of tens of thousands of migrants.[37]

Concluding Remarks

While technologies have the potential to be used to prevent and investigate human rights violations at borders including enforced **disappearances** and illegal pushbacks, this function is rarely fulfilled. Instead situational awareness and biometric identification technologies play a key role in border enforcement, in facilitating illegal pushback, deportations and fundamental rights violations. With increasing efforts to externalize border control, technologies are often a central element in agreements with third-countries, facilitated through the operational deployment of supranational agencies. Given the detrimental impact on human and privacy rights the deployment of technology for border control merits special attention and oversight.

Recommendations

1. Develop clear guidelines on the provision and usage of new technologies, based on best practices of documentation and with extensive consultation of CSOs and asylum seekers and migrants self-documenting enforced disappearances
2. Refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of

[36] Goldberg J. (2025) & Krishnamoorthy H. (2025) IOM's digital tool aims to speed up migrant removals, but at what cost? Available at: https://www.thenewhumanitarian.org/investigations/2025/05/19/iom-rcms-digital-tool-aims-speed-migrant-removals-what-cost
[37] Human Rights Watch (2019). No Escape from Hell EU Policies Contribute to Abuse of Migrants in Libya. Available at: https://www.hrw.org/report/2019/01/21/no-escape-hell/eu-policies-contribute-abuse-migrants-libya

human rights, especially of those who are in vulnerable situations (per UN General Assembly resolution A/RES/78/265);

3. Ensure access to remedies for human rights violations and abuses arising from biometric identification and recognition technologies (per UN Human Rights Council resolution A/HRC/RES/58/23)
4. Enforce transparency and fundamental rights compliance obligations for non-state actors including international organisations and private companies involved in the funding, development or implementation of border surveillance and biometric technologies.

Access Now (https://www.accessnow.org) defends and extends the digital rights of individuals and communities around the world. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact: **un@accessnow.org***

The Border Violence Monitoring Network (https://borderviolence.eu/) is an in independent network of NGOs that monitors human rights violations at and within European borders and advocates to stop violence against people on the move. Our testimonies and reports serve as a basis for the Network's multi-jurisdictional advocacy efforts to denounce border violence and pursue accountability of those responsible for it.

For more information please contact UNAdvocacy@borderviolence.eu