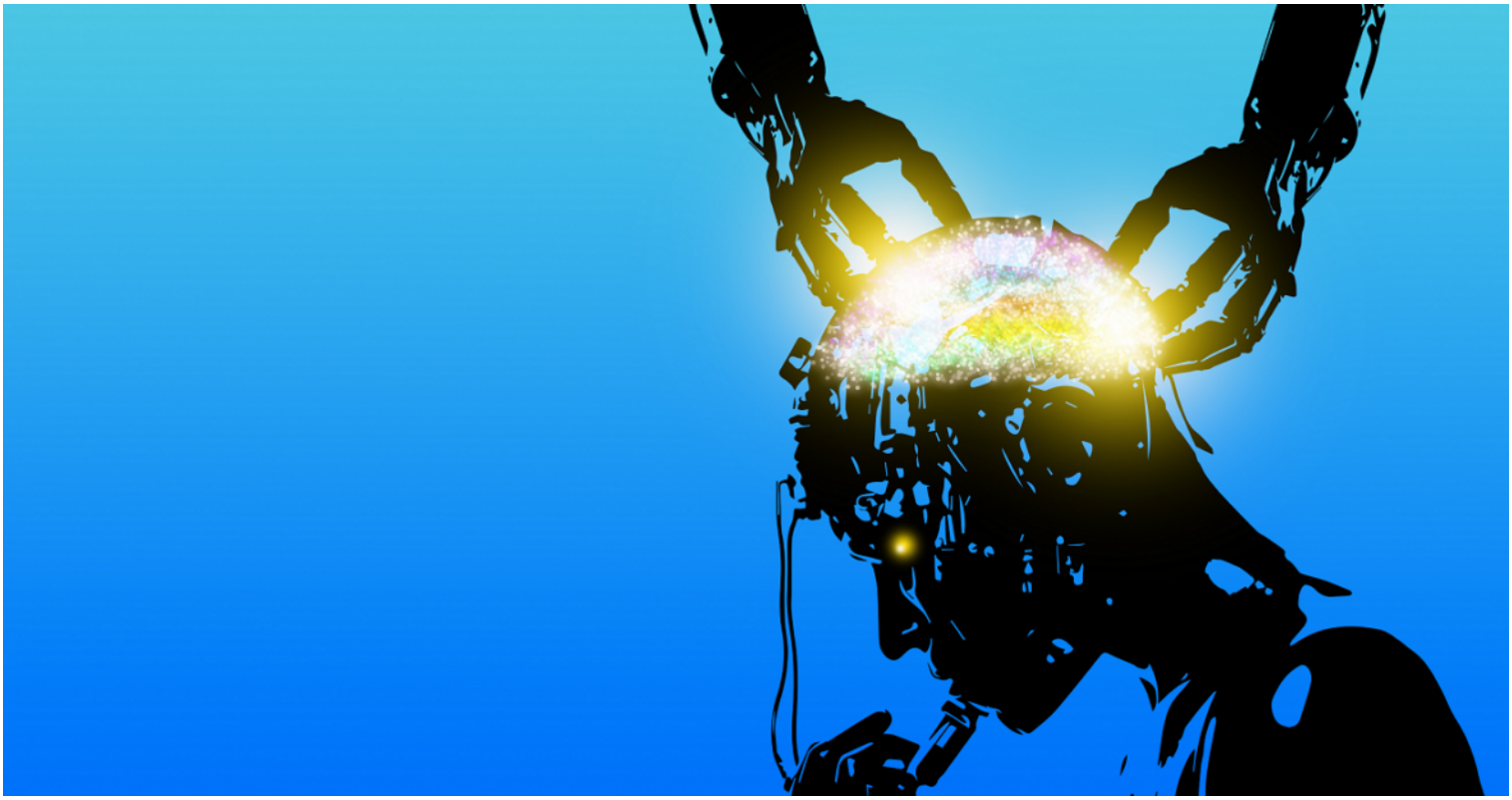
HUMANITARIAN LAW & POLICY

Deploying OSINT in armed conflict settings: law, ethics, and the need for a new theory of harm

December 5, 2023, Analysis / Cybersecurity and data protection in humanitarian action / Human Costs of Cyber / IHL / New Technologies / Technology in Humanitarian Action

16 mins read

Ed Millett
Legal researcher and OSINT analyst



The deployment of open-source intelligence, or OSINT – information gathered from publicly available data sources and used for intelligence purposes – is having a dramatic impact on armed conflict in the 21st century, rebalancing information asymmetries between states and other actors while supporting accountability efforts. There is, however, a downside to these developments, with OSINT creating and enabling the risk of harm to civilians' rights, lives, and safety in ways that are not yet fully understood.

In this post, part of a new series on Cybersecurity and data protection in humanitarian action, legal researcher and OSINT analyst Ed Millett considers how far international humanitarian law (IHL) and international human rights law (IHRL) currently regulate the use of OSINT techniques by state and non-state actors in armed conflict settings, suggesting that our limited understanding of emergent harms is hampering effective regulation.

Open-source information and its subcategory, open-source intelligence (OSINT) – information gathered from publicly available data sources and used for aiding policymaking and decision-making in a military or political context – is becoming a major feature of armed conflict in the 21st century.*[1]* Its use in Ukraine, for example, is well documented: private-sector satellite companies providing geospatial data to Ukrainian artillery units,*[2]* civil society organizations using geolocated footage and social-media posts to map civilian casualties,*[3]* and international organizations using drones to monitor ceasefire compliance.*[4]*

The opportunities presented by such technology for a range of users are widely reported, particularly where OSINT operations run the full gamut of the "information cycle" – acquiring, exploiting, retaining and reproducing data – and where they gather publicly available information from diverse sources, including social-media and messaging platforms, geospatial data, mapping software, and database services such as global trade data.*[5]* Open-source information can, for example, help to foster accountability and support justice efforts by uncovering human rights abuses and atrocity crimes,*[6]* or refine state military targeting to embed better IHL compliance.*[7]*

However, the misuse of OSINT, in its acquisition, retention and publication, can also facilitate real-world harms, negatively impacting on individual human rights such as privacy, data protection and fair-trial rights. For example, in the Netherlands, an unregulated online manhunt for a suspected criminal fugitive took place on social media following the publishing ("doxing") of their personal information, leading to accusations that such activity risked circumventing legal safeguards on police investigative procedures.*[8]* In Ukraine, drone footage from the Donbas region published online by the OSCE risked inadvertently alerting Russian authorities to the existence of an undocumented crossing in a ceasefire line, allegedly resulting in curtailment of civilian access to schools, workplaces and health services.*[9]* Finally, Nathaniel Raymond has illustrated how the location of demobilized child soldiers in an armed conflict setting could easily be learned by non-state armed groups through the piecing together of public reporting and statistics by a range of humanitarian agencies (known as the "Mosaic Effect").*[10]*

In light of these threats, this post investigates the legal frameworks governing the incorporation of OSINT into operations and investigations carried out in armed conflict settings by states and civilian non-state actors (NSAs). It considers applicable IHL before investigating how far international human rights law (IHRL) can fill gaps in the legal framework. Finally, it considers the patchwork of non-legal standards that largely regulate the use of OSINT by NSAs, highlighting how limited understanding of potential harms is hampering the development of both legal and non-legal restraints.

IHL: providing some limited restraint?

OSINT activities during armed conflict now form part of the wider ecosystem of state digital capabilities. Previously, such capabilities were often conceived narrowly in terms of cyber operations to *disable, disrupt or destroy* computer systems, or to *exploit* such systems by exfiltrating information. Increasingly, OSINT activities, aimed at *accessing, analysing and publishing* digital information should also be seen as a crucial part of state capabilities in this area, along with other digital measures (for example, the deployment of civilian hackers, internet shutdowns). The potential impact of such activities is significant, for example where belligerents are able to leverage affected populations' personal data to target civilians, with disinformation or violence.*[11]*

Nevertheless, informational privacy during armed conflict remains something of a lacuna in IHL frameworks.*[12]* The emerging view in customary IHL is that the *medical data* of persons who are not or are no longer participating in hostilities – e.g. civilians and combatants who are *hors de combat* – falls within scope of the obligation on conflict parties to "respect and protect" medical services and infrastructure.*[13]* This obligation is now widely considered to protect the *confidentiality, integrity and availability* of medical data, limiting the whole range of digital activities that could be leveraged against medical data, even where patients and infrastructure are unaffected.

The legal framework protecting general, *non-medical* personal data is more conceptually problematic. One key area of ongoing dispute relates to the types of digital activities falling under the protection of IHL's general protections in *Article 52* of Additional Protocol I (API), and thereby rendering IHL targeting rules – the principles of distinction, proportionality, and precautions – applicable. The application of Article 52's protections is contingent upon the object satisfying the definition of "civilian object" and the activity in question satisfying the definition of "attack" set out in *Article 49 API*, which requires "acts of violence".

There is ongoing academic debate as to whether "content-level data" – e.g. non-medical data held on a computing system – can be considered a "civilian object" for these purposes.*[14]* Most pertinently for OSINT activities, there is *also* significant uncertainty as to what *activities* against such data would fall to be considered "attacks". Schmitt has suggested that operations aimed at affecting the *integrity or availability* of data held on a computing system would qualify as an "attack", whereas operations that leave content-level data intact and only target *confidentiality* would not.*[15]* However, it follows from this that the full OSINT "operations cycle" of data collection, processing, exploitation and (re)production could be effectively conducted to gather, analyse and republish personal information without affecting data-integrity, thereby falling outside IHL's protection entirely. This would represent a lacuna in the current interpretation of IHL with respect to attacks on civilian objects.

What role for IHRL?

Given these gaps in the legal framework applicable to conflict actors making use of OSINT, legal norms emanating from IHRL can provide support, for example with regards to privacy and data protection rights. Progressive interpretations of IHL already point in this direction: the *ICRC's updated Commentary on the Second Geneva Convention* provides an example of IHRL's emerging role, noting that personal health data held by hospital ships "must be afforded a reasonable level of security" in accordance with "international privacy and data protection standards."*[16]* However, there remain several significant issues with using IHRL standards and jurisprudence to regulate the use of OSINT during armed conflict.

First, the question of whether OSINT activities *actually infringe* upon privacy and data protection rights, thereby entailing IHRL protections, remains conceptually complex. IHRL jurisprudence endorses a concept of "privacy in public", but suggests that publicly available information *can* be freely observed and collected without falling within the ambit of privacy rights, provided this is not done *systematically* in order to create "structured data" i.e. some types of OSINT activity simply do not fall within scope of the right to privacy.*[17]* However, in an era when vast amounts of sensitive and valuable personal information can be gathered from open social media platforms, the distinctions between what is private and what is not are becoming murkier; older principles of "privacy in public" now insufficiently capture the realities of the online environment. State practice – drawn from OSINT's deployment

domestically for law enforcement purposes – suggests a "reasonable expectation of privacy" standard for online activity, but there remains a lack of clarity over *what* publicly available information falls within scope of that expectation. For example, information posted in a private group on a social-media platform, or the "social graph" of a person's online friend network *could* be considered protected by privacy rights – placing limits on state acquisition and exploitation.*[18]*

Second, there remains significant theoretical debate about using IHRL standards to supplement the IHL framework, particularly where norm conflicts arise. With respect to data protection and privacy, direct conflicts could, for example, occur in relation to IHL's rules authorising surveillance and censorship of POW correspondence, which would likely fall within the ambit of privacy rights. That said, for the most part IHL is silent on issues of privacy and communications, partly due to the speed of technological advancement in this area, suggesting that in reality norm conflicts may *not* be a significant barrier to relying on IHRL to gap-fill the IHL regime.*[19]*

Third, the extra-territorial application of IHRL continues to stoke debate: the European Court of Human Rights has expressed the view that IHRL obligations continue to apply to acts which "produce effects" extra-territorially, with the exception of kinetic uses of force in the active phase of hostilities.*[20]* This would suggest that IHRL obligations *could* continue to apply to non-kinetic OSINT operations where they "produce effects", although this is likely to be contested by states and the linkage between OSINT and the effect would be hard to establish in practice.

Fourth, privacy and data protection rights – including under instruments such as the EU's General Data Protection Regulation (GDPR) – are invariably limitable and/or derogable rights. Regional courts have at times imposed strict necessity tests on states' ability to limit and derogate from these obligations,*[21]* while states have developed sophisticated judicial oversight measures for surveillance activity, permitting lawful interference with these rights where necessary and proportionate.

Taken together, these issues may significantly limit the ability of IHRL to limit the impact of OSINT activities during armed conflict on privacy, data protection and other rights.

Regulating non-state actors?

When it comes to NSAs, legal restraints weaken considerably. A great variety of civilian NSAs – international humanitarian organizations, civil society groups, individual actors – already conduct open source investigations in armed conflict settings. Where their activity has no nexus to the conflict, IHL does not formally bind them, except insofar as individuals continue to be bound by criminalized rules of IHL, or where domestic laws implementing rules of IHL are applicable.

The applicability of IHRL to NSA activities is piecemeal and contested. Formally, civil society organizations cannot be said to be bound by IHRL.*[22]* International organizations (IOs) usually do not consider themselves bound by IHRL obligations, while privileges and immunities could mean that IOs do not apply legal obligations concerning data protection, such as GDPR.*[23]*

Accordingly, a patchwork of data protection regimes, self-regulatory standards and non-binding protocols has emerged. Multiple IOs have data protection regimes, although they often do not address the question of the applicability of IHRL.*[24]* For media organizations, the IMPRESS Standards Code for Journalists, for example, sketches out a "reasonable expectation of privacy" standard for online activity.*[25]* The Berkeley Protocol, a leading soft-law framework for open source investigations aimed at civil society users, calls on investigators to respect the right to privacy, but primarily on the limited basis that breaches may result in evidence being excluded from criminal proceedings.*[26]*

Ultimately, imposing onerous legal obligations on NSAs may not be the solution, given the risk of a chilling effect on the many positive uses of open source investigatory techniques and activities. Nevertheless, the absence of applicable legal frameworks delegates regulation to non-binding ethical doctrines and voluntary commitments, resulting in a fragmented approach between users based on a limited understanding of potential harms. Accordingly, it is becoming clear that civilian NSAs are in need of stronger, more harmonized codes of practice for open source investigatory activities that take into account the particularities of the online environment, in particular thorny conceptual issues concerning online privacy.*[27]* However, the fact that different users have vastly different purposes for information-collection and are increasingly integrating open source information with other data-sources pose challenges to codifying current practices.

Conclusion

This post has spotlighted some of the potential harms emanating from unprincipled, unregulated uses of open source investigatory techniques in armed conflict settings, considering applicable legal regimes for different users – and their current limits. There are also other potential sources of harm from the use of OSINT in these settings – from problems with obtaining informed consent for digital interventions from conflict-affected communities, to growing civilian involvement in digital activities during armed conflict. Broadly, our understanding of how IHL and IHRL frameworks regulate this area needs to develop further, and at a more fundamental level we are still lacking sufficient understanding of the harms that can emerge from the use of digital technologies like OSINT. Accordingly, developing a more holistic theory of digital harms and norms – one that is sensitive to the impact of technologies such as OSINT and the particular conceptual challenges of the digital environment – is a necessary precursor to establishing more robust legal and ethical principles and practices to protect digital rights in armed conflict settings.*[28]*

[1] 'Open source intelligence' is usually considered to be a subcategory of 'open source information': information that is being collected, exploited and disseminated for intelligence or law-enforcement purposes. Non-state actors who use open source information, such as civil society organizations and international organizations, understandably prefer to use terminology such as 'open source investigations' in the context of their analysis. For further

discussion of definitions, see Human Rights Center, UC Berkeley School of Law and the Office of the High Commissioner for Human Rights, *Berkeley Protocol on Digital Open Source Investigations* (2020) para. 19 ff.

[2] Mike Cerre, Dan Sagalyn, 'Private companies track the war in Ukraine in real time' *PBS Newshour* (2022).

[3] Bellingcat Investigation Team, 'Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine', *Bellingcat* (2022).

[4] Cono Giardullo, A. Walter Dorn, Danielle Stodilka, 'Technological Innovation in the OSCE: The Special Monitoring Mission in Ukraine' in IFSH (ed.) *OSCE Yearbook 2019* (2020) p. 120.

[5] Heather Williams, Ilana Blum, 'Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise', *RAND Corporation* (2018) p. 13; Isabelle Böhm, Samuel Lolagar, 'Open source intelligence: Introduction, legal and ethical considerations' *International Cybersecurity Law Review* 2 (2021) pp. 320-1.

[6] John Thornhill, 'Ordinary Ukrainians wage war with digital tools and drones', *Financial Times* (2022); Lindsay Freeman, 'Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court', in Sam Dubberley, Alexa Koenig, Daragh Murray (eds.) *Digital Witness* (2019) pp. 68-86.

[7] Asaf Lubin, 'The Rights to privacy and data protection under international humanitarian law and human rights law' in Robert Kolb, Gloria Gaggioli, Pavle Kilibarda (eds.), *Research Handbook on Human Rights and Humanitarian Law* (2022) p. 487.

[8] Leonore Ten Hulsen, 'Open Sourcing From The Internet – The Protection Of Privacy In Civilian Criminal Investigations Using OSINT (Open-Source Intelligence)' (2020) 12 *Amsterdam Law Forum* Vol.1 p. 28.

[9] Author's interview with former member of OSCE Special Monitoring Mission to Ukraine (from 2015-2019), 30 July 2022

[10] The full case study is described here: Nathaniel Raymond, 'Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data', in Linnet Taylor, Luciano Floridi, Bart van der Sloot (eds.) *Group Privacy: new challenges of data technologies* (2017) p. 95.

[11] Joelle Rizk, Sean Cordey, 'What we don't understand about digital risks in armed conflict and what to do about it', *ICRC Humanitarian Law and Policy* (2023).

[12] Lubin, supra p. 477

[13] Michael Schmitt (ed.), *Tallinn Manual 2.0* (2017) Rule 132; ICRC, *Customary IHL Database*, Rules 25, 28, 29; Robin Geiß, Henning Lahmann, 'Protection of Data in Armed Conflict', 97 *International Law Studies* 556 (2021) p. 564.

[14] Geiß/Lahmann, supra p. 565-7

[15] Michael Schmitt, 'The Notion of "Objects" During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision', 48 *Israel Law Review* 81, (2015) pp. 95,101.

[16] ICRC, *Commentary on the Second Geneva Convention* (2017) §2403.

[17] Lilian Edwards, Lachlan Urquhart, 'Privacy in public spaces: what expectations of privacy do we have in social media intelligence?' *International Journal of Law and Information Technology* 24 (2016) p. 307; *von Hannover v Germany* [2005] 40 EHRR 1; *Rotaru v Romania* [2000] 8 EHRC 449 §43; *Segerstedt-Wiberg v Sweden* [2007] 44 EHRR 2 §72;

[18] UK Home Office, 'Covert Surveillance and Property Interference: Revised Code of Practice August 2018' (2018) §§3.10-17; Edwards, Urquhart, *supra* p. 294.

[19] Lubin *supra*, p. 482

[20] Georgia v. Russia (II) [GC], Merits, App.No.38263/08 [2021] §133; Mary Ellen O'Connell, 'Data Privacy Rights: The Same in War and Peace' in Russell Buchan, Asaf Lubin (eds.) *The Rights to Privacy and Data Protection in Times of Armed Conflict* (2022) p. 23.

[21] Regarding GDPR, see *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, CJEU Case C-73/07 [2008] §56; *Szabo and Vissy v Hungary* App.No.37138/14 [2016] §73.

[22] Noam Schimmel, 'The IHRL Responsibilities of NGOs', *Oxford Human Rights Hub* (2015).

[23] Lubin *supra* p. 255; Christopher Kuner, 'International Organisations and the EU General Data Protection Regulation', *International Organisations Law Review* 16 (2019) p. 162; Massimo Marelli, 'The law and practice of international organizations' interactions with personal data protection domestic

regulation: At the crossroads between the international and domestic legal orders', *Computer Law and Security Review* 50 (2023) pp. 12-14.

[24] Asaf Lubin, 'Data Protection as an International Legal Obligation for International Organisations: The ICRC as a Case Study' in Russell Buchan, Asaf Lubin (eds.), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (2022) p.250; Christopher Kuner, 'International Organisations and the EU General Data Protection Regulation', *International Organisations Law Review* 16 (2019) p. 163.

[25] IMPRESS, 'Standards Code' Art.7 Guidance.

[26] Berkeley Protocol on Digital Open Source Investigations, para. 62.

[27] Vidhya Ramalingam, Raquel Vazquez Llorente, 'Symposium on Fairness, Equality, and Diversity in Open Source Investigations: "Fair Game"? Rethinking Ethics and Harm in the Age of Digital Investigations', *Opinio Juris* (2023)

[28] Kristin Sandvik, Nathaniel Raymond, 'Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response', *Genocide Studies and Prevention* Vol.11 Iss.1 (2017) p. 16.

See also:

- Joelle Rizk, Sean Cordey, *What we don't understand about digital risks in armed conflict and what to do about it*, July 27, 2023
- Fiona Terry, Fabien Dany, *Harnessing the power of Artificial Intelligence to uncover patterns of violence*, May 25, 2023
- Kubo Mačák, Tilman Rodenhäuser, *Towards common understandings: the application of established IHL principles to cyber operations*, March 7, 2023

Tags: armed conflict, digital technology, ethics, IHL, IHRL, law, osint, protection of civilian population, protection of civilians, technology

You may also be interested in:

Reducing harm in military security operations

14 mins read

Analysis / Cybersecurity and data protection in humanitarian action / Human Costs of Cyber / IHL / New Technologies / Technology in Humanitarian Action

Stephen Kilpatrick, Philippe Cholous, LT COL Susan Mwanga & Elizabeth Rushing

Responsibility for maintaining law and order generally falls to civil authorities such as the police ...

The complex neutrality of commercial space actors in armed conflict

12 mins read

Analysis / Cybersecurity and data protection in humanitarian action / Human Costs of Cyber / IHL / New Technologies / Technology in Humanitarian Action Guoyu Wang

During an international armed conflict, commercial space actors under the jurisdiction or control of a ...