8

Faces of War

Russia's Invasion of Ukraine and Military Use of Facial Recognition Technology

Agne Limante

8.1 INTRODUCTION

Shortly after Russia launched large-scale military action on Ukraine on 24 February 2022, Clearview AI (a US-based facial recognition company) announced that it had given its technology to the Ukrainian government to be used for military purposes in Russia's attack on Ukraine.[1] In mid-March 2022, it was reported that Ukraine's Ministry of Defence started using facial recognition technology (FRT).[2] In such a way, simply and effectively, without long-lasting political debate and academic or civil society discussions, FRT was brought to a new profitable market and joined a list of tools that can be employed for military purposes.

While the Russian war against Ukraine is not the first time that FRT has been used in a military setting, this conflict has brought the military use of this technology to a different level: FRT was offered openly at the outset of the war to one of the sides, being promptly accepted by the Ukrainian authorities and tested on the ground for a variety of objectives. Before 2022, there was only minimal evidence of FRT employment for military purposes. One might recall that in 2019, Bellingcat, a Netherlands-based investigative journalism group specialising in fact-checking and open-source intelligence, used FRT to help identify a Russian man who had filmed the torture and killing of a prisoner in Syria,[3] or that in 2021, Clearview AI signed a contract with the Pentagon to explore putting its technology into augmented reality glasses.[4] It has also been reported that Israel performs surveillance of Palestinians

[1] BBC, 'Ukraine offered tool to search billions of faces' (14 March 2022), *BBC News*, www.bbc.com/news/technology-60738204.

[2] Paresh Dave and Jeffrey Dastin, 'Exclusive: Ukraine has started using Clearview AI's facial recognition during war' (14 March 2022), *Reuters*, www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

[3] BBC, 'How facial recognition is identifying the dead in Ukraine' (13 April 2022), *BBC News*, www.bbc.com/news/technology-61055319.

[4] kwon0321, 'Clearview AI working on A.R. goggles for Air Force security' (3 February 2022), *Days Tech*, https://daystech.org/clearview-ai-working-on-a-r-goggles-for-air-force-security/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

using a facial recognition program.[5] However, these cases only provide evidence of incidental use or potential future application of FRT for military purposes.

This chapter discusses how FRT is employed by both sides in Russia's war against Ukraine. In particular, it examines how Ukraine engages FRT in the country's defence, testing the different possibilities this technology offers. It also acknowledges the use of FRT on the other side of the conflict, elaborating on how it is used in Russia to suppress society's potential opposition to the war. The chapter focusses on the potential and risks of using FRT in a war situation. It discusses the advantages that FRT brings to both sides of the conflict and underlines the associated concerns.

8.2 FRT IN THE BATTLEFIELD: UKRAINE

Ukraine began exploring the possibilities of FRT use in the military during the first month of the war. There was no time for elaborate learning or training, and the FRT was put directly into the battlefield, applying creative thinking and a trial-and-error approach. As a result, the Ukraine war can be seen as a field trial for FRT, where, faced with the pressing need to defend its territory and people, the country referred to collective efforts to generate ideas on innovative ways to employ modern technologies and is putting them into practice and checking what works well.

It should be admitted that the FRT developed by Clearview AI (perhaps the most famous and controversial facial recognition company) worked for the interests of Ukraine, owing to its enormous database of facial images. The company has harvested billions of photos from social media companies such as Facebook, Twitter, and Russian social media sites (Vkontakte).[6] Such a method of database creation attracted wide criticism in peacetime,[7] but proved beneficial in war, enabling access to facial images of Russian citizens, including soldiers.

[5] Elizabeth Dwoskin, 'Israel escalates surveillance of Palestinians with facial recognition program in West Bank' (8 November 2021), *Washington Post*, www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

[6] BBC, 'How facial recognition is identifying the dead'.

[7] In Europe, Clearview AI's services have been condemned by, for instance, the Swedish DPA, the French DPA, the Italian DPA, and the UK Information Commissioner's Office. See European Data Protection Board, 'Swedish DPA: Police unlawfully used facial recognition app' (12 February 2021), https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_es; Commission Nationale de l'Informatique et des Libertés, 'Facial recognition: The CNIL orders CLEARVIEW AI to stop reusing photographs available on the internet' (16 December 2021), www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet; European Data Protection Board, 'Facial recognition: Italian SA fines Clearview AI EUR 20 million' (17 March 2022), https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en; Information Commissioner's Office, 'ICO fines facial recognition database company Clearview AI Inc more than £7.5 m and orders UK data to be deleted' (23 May 2022), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

One might think that collecting facial images of military personnel, especially those of a higher rank, from social networks might be a challenge – as they are less likely to reveal their identity. But this is not entirely true. While persons who post frequently on social media can be identified more easily, facial recognition systems can also identify and verify those who do not even have social accounts. It is enough that a family member, friend, co-worker, or person also serving in the army post a picture where the person is seen. The technology can even single out a face in a crowd picture and compare it with the face in question. Face recognition can also be used where only some people from a group (e.g., a military unit) have been identified, with the rest of the group being identified through content from any of the identified members. Even if a person appears on the internet in a randomly taken picture, it might also be helpful information allowing their gradual recognition.[8]

Here, several ways in which the Ukrainian authorities employed FRT in its efforts to fight Russia are discussed. The author would like to note that the list might be not exhaustive as, at the time of writing (September 2022), the war continues, and part of the information remains undisclosed.

8.2.1 *Identification of Dead*

Being probably the first country in the world to use FRT for such a purpose, Ukraine has made the headlines by announcing that it is employing FRT to recognise fallen Russian soldiers.[9] Many discussions have arisen regarding this controversial idea, its objectives, ethical issues, and effects in case of a mismatch.

Identification of the dead is typically a task for forensic experts. Methods such as examining DNA, dental data, and physical appearance can be used to identify the deceased and have proven reliable. While in peacetime this information is usually available, in wartime experts might be faced with limited data availability, both in the case of nationals of the country in question and soldiers or civilians of the enemy state. Obtaining pre-death samples of enemy fighters' DNA or dental data is challenging, if not impossible, and in a majority of cases requires too much effort to be of value to a country at war.

In such a situation, the FRT becomes a particularly handy tool, as all is needed is to take a picture of a dead soldier and run it through the database. In the first fifty days since Russia's invasion of Ukraine, Ukrainian officials are stated to have run more than 8,600 facial recognition searches on dead or captured Russian soldiers, identifying

[8] Pictures of soldiers might be useful in many ways. Another possible use of images is geoprofiling, employed at public and private level. A background of a picture often allows the identification of the location where the picture was taken, in a war situation enabling identification of the position of the enemy. Kyiv media cites the situation where using a dating website a hacker group received a picture of a Russian soldier standing next to a military base, thus allowing the detection – and then elimination – of the enemy. *KyivPost* post on Facebook, 5 September 2022.

[9] FRT-based identification of fallen soldiers can also be performed on soldiers on any side of the conflict; however, it is more relevant with regard to enemy personnel.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

some of them.[10] Why was FRT used this way, especially towards the deceased? An unprecedented strategy was developed by Ukraine. After the bodies were identified, the Ukrainian officials (as well as civil activists) contacted the families of the deceased Russian soldiers to inform them about the death of their relative. As recognised by Ukraine's Digital Transformation Minister, this served two purposes. On the one hand, it could be perceived as a method to inform the families, providing them with information on their beloved ones and allowing them to retrieve the bodies. On the other hand, it was seen as a tool for Ukrainians to overcome Russian propaganda and denial of the human costs of the war.[11] In other words, such FRT employment worked as a political counter-offensive and was one of Ukraine's strategies in endeavours to inform Russians, who had limited access to non-state-controlled information or were simply ignorant, about the war hostilities and death of Russian soldiers.[12]

This second objective of informing Russian families about the death of their relatives fighting in Ukraine nevertheless appeared to be challenging to accomplish. Again, Ukrainians had to develop their own model to fulfil this goal, as FRT had not been used in this way before and thus there were no experiences to learn from. Theoretically, it would have been possible only to send information to the relatives that their family member had died in a field. However, in the light of constant Russian claims as to 'fakes' being spread by the Ukrainians,[13] this would not have been enough – some evidence needed to be added. From the other perspective, accompanying information about the death of a soldier with pictures of his abandoned corpse or lifeless face, which allegedly was done from the Ukrainian side in several instances, might be interpreted as psychological violence towards the family members or even psychological warfare. Instead of encouraging Russian mothers and fathers to start opposing the war, such a strategy had a risk of bringing the opposite results of anger and claim of disregard for human dignity and humiliation by the enemy.

8.2.2 *Identification and Verification of the Identity of Persons of Interest*

Another possible use of FRT in a war zone is identifying persons of interest who come within eyeshot of military personnel or public authorities and verifying their identity. Such identification and verification might be employed in different contexts and serve various needs.

[10] Drew Harwell, 'Ukraine is scanning faces of dead Russians, then contacting the mothers' (15 April 2022), *Washington Post*, www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/.

[11] Sara Sidner, 'Ukraine sends images of dead Russian soldiers to their families in Russia' (n.d.), *CNN Video* (including interviews with Ukraine officials), www.cnn.com/videos/world/2022/05/13/ukraine-face-recognition-russian-soldiers-lead-sidner-pkg-vpx.cnn.

[12] This strategy was employed at the beginning of the conflict, but it lost its initial scale within a few months.

[13] The term 'fake' (Rus. фейк) has entered the Russian language and is used on a regular basis in the politics, media, and everyday life. It has become a keyword that is used to raise doubts as to any information published by Ukraine or Western countries that conflicts with the information disseminated by Russian-controlled media.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

As public sources state, the Ukrainian government used FRT at checkpoints to help identify enemy suspects (Russian infiltrators or saboteurs, covert Russian operatives posing as Ukrainian civilians).[14] At the time of writing, however, it is impossible to obtain data on the extent and how effectively FRT was employed in checkpoints. But it can be claimed that FRT has considerable potential in this regard, especially if specific persons are sought – although systemic use of FRT at checkpoints might be complicated during wartime owing to technical and time constraints.

FRT could also be (and likely was) employed when identifying and interviewing captured soldiers. This limits the ability of captured soldiers to deny their links with the army or present false or misleading information. It also allows additional psychological pressure to be put on an enemy soldier, who is well aware he has been identified.

It might also be tempting to publish a video interview with a captured enemy soldier, aligning it with his image (alone or with family members) retrieved from social media. Similar to notification of families about killed Russian soldiers, this could be a strategy to encourage Russian society to oppose the war. In this regard, it should be taken into account that Article 13(2) of the Geneva Convention (III) prescribes that prisoners of war must be protected from insults and public curiosity, whether these take place at the same time or not. The International Committee of the Red Cross commentary (of 2020) on Article 13 of the Geneva Convention (III) underlines that the prohibition of exposing prisoners of war to 'public curiosity' also covers the disclosure of photographic and video images, recordings of interrogations in public communication channels, including the internet, as this practice could be humiliating and jeopardise the safety of the prisoners' families and of the prisoners themselves once they are released (para. 1624).[15] The Committee suggests that any materials that enable individual prisoners to be identified must normally be regarded as subjecting them to public curiosity and, therefore, may not be transmitted, published, or broadcasted (if there is a compelling public interest in revealing the identity of a prisoner – for instance, owing to their seniority or because they are wanted by justice – then the materials may exceptionally be released, but only insofar as they respect the prisoner's dignity) (para. 1627).

8.2.3 *Combating Misinformation, Denial, and Propaganda*

As noted earlier, one of the objectives of Ukrainian authorities when using the information retrieved by FRT is combating the misinformation and denial of Russian citizens regarding the human costs of war and propaganda related to the war itself.

[14] BBC, 'How facial recognition is identifying the dead'.

[15] International Committee of the Red Cross, 'Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949. Commentary of 2020, Art. 13 : Humane treatment of prisoners' (2020), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=3DEA78B5A19414AFC125858500434 4BD#:~:text=1626%E2%80%83%E2%80%83More%20compellingly,international%20tribunals%20subsequently.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

In Russia, information published by Ukraine or Western countries on dead and captured Russian soldiers, as well as war atrocities committed by Russian soldiers, is dealt with using a simple strategy: denying the information, raising doubts about its truthfulness and blaming the other side. Russian commentators often claim that the faces are not of Russian soldiers, that the situation is staged, or that actors are involved.[16]

In fact, during wartime, both sides could be falsifying information while simultaneously denying accurate information, damaging their policy. FRT, however, allows published material to be more precise and evidence-based, as faces can be linked to the name and family name, place of residence, and photos taken from social media profiles. It also simplifies cross-checking information published by the other side, and thus is a tool in an information war.

An example of using FRT to verify public information concerned the sinking of the Russian warship *Moskva* in the Black Sea south of Ukraine. When the Russian state held a ceremony for the surviving sailors and officers who had been on the ship, many people wondered if these were actual sailors from the *Moskva*. Bellingcat ran the pictures through Russian facial recognition platform FindClone using images in Russian social media, and found that most of the men were indeed Russian sailors from Sevastopol.[17]

8.2.4 *Identification of War Criminals*

Historically, photographic and other visual evidence has been used to prosecute war crimes, promote accountability, and raise public awareness of abuses.[18] FRT has a high potential to improve such usage of visual tools and to contribute to the process of bringing those responsible to justice, as well as identifying guilty soldiers who it might otherwise be complicated to single out.

Ukraine does not deny that it uses facial recognition to identify Russian soldiers suspected of war crimes or caught on camera looting Ukrainian homes and storefronts. It acknowledges that from the beginning of the conflict it has deployed this technology to identify war criminals, and will continue to do so.[19] For instance, Ukraine's Digital Transformation Minister (Mykhailo Fedorov) shared on Twitter

[16] For example, 1TV, 'Украина и Великобритания сняли антироссийский фейк, поместив туда символику нацистов. Новости. Первый канал' (3 June 2022), www.1tv.ru/news/2022-06-03/430410-ukraina_i_velikobritaniya_snyali_antirossiyskiy_feyk_pomestiv_tuda_simvoliku_natsistov.

[17] Lizzy O'Leary, 'How facial recognition tech made its way to the battlefield in Ukraine' (26 April 2022), *Slate*, https://slate.com/technology/2022/04/facial-recognition-ukraine-clearview-ai.html.

[18] Aoife Duffy, 'Bearing witness to atrocity crimes: Photography and international law' (2018) 40 *Human Rights Quarterly* 776.

[19] Ministry of Digital Transformation, Ukraine, 'Як Розпізнавання Обличчя Допоможе Знайти Всіх Воєнних Злочинців' (9 April 2022), Interview (directed by Міністерство цифрової трансформації України), www.youtube.com/watch?v=fUKQM7BXryc.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

and Instagram the name, hometown, and personal photo of a man who, according to him, was recorded shipping looted clothes from a Belarus post office to his home in Russia. The Ukrainian official added, 'Our technology will find all of them', presumably referring to FRT.[20] He also noted that 'many killers have already been identified who terrorised civilians in Bucha and Irpen. In a short time, we will establish all the information about these people.'[21] The Chief Regional Prosecutor (Ruslan Kravchenko), in an interview with a news portal, also acknowledged the use of FRT to identify the Russian soldiers suspected of criminal offences, giving an example of how a Russian soldier who murdered a civilian was identified by FRT and later confirmed by the witness.[22] There were more reported recognitions later.[23]

If FRT can successfully identify war criminals in Russia's war against Ukraine, there is a slight hope that this could (at least to some extent) deter soldiers from committing war crimes in the future. One has to admit, though, that any false matches may lead to wrongful accusations of war crimes (see Section 8.4.1). Therefore, FRT should only be seen as an investigative lead, but not as definitive evidence. The risk of a false match can be minimised by performing additional analysis on the person concerned. Such further searches can prove to be particularly fruitful where context-related information can be found (e.g., videos and photos confirming the person was fighting in Ukraine, his statements and pictures, communication with relatives, photos and articles on his previous military activity and visibility).[24]

8.3 FRT IN RUSSIA: A GOVERNMENT'S TOOL IN ITS EFFORT TO STIFLE ANTI-WAR PROTESTS

During the war against Ukraine, the FRT in Russia mainly, though not exclusively,[25] served a different purpose – to stop any anti-war protests.[26] While marches and mass

[20] Mykhailo Fedorov [@FedorovMykhailo], Post, Twitter (7 April 2022), https://twitter.com/FedorovMykhailo/status/1512101359411154953: 'After events in Bucha, I am launching the #russian-looters column. Our technology will find all of them. Shchebenkov Vadym stole more than 100 kg of clothes from UA families and sent them from Mozyr, Belarus, to his hometown of Chita. It is 7 thousand km away.'

[21] 'FEDOROV', Telegram, (9 April 2022), https://t.me/zedigital/1546.

[22] Sidner, 'Ukraine sends images of dead Russian soldiers'.

[23] For example, Oleksandr Topchij and Vitlij Saenko, 'Завдяки відео CNN встановлено особу росіянина, який розстріляв двох цивільних на Київщини' (2 September 2022), *Unian*, www.unian.ua/society/zavdyaki-video-cnn-vstanovleno-osobu-rosiyanina-yakiy-rozstrilyav-dvoh-civilnih-na-kijivshchini-novini-kiyeva-11964534.html.

[24] See 'Tactical OSINT Analyst' [@OSINT_Tactical], Post, Twitter (1 March 2022), https://twitter.com/OSINT_Tactical/status/1498694344781484037.

[25] Russia also uses FRT to survey the areas close to the border zone to identify the enemy and saboteurs, for example. *Moscow Times*, 'Russia to expand high-tech surveillance to Ukraine border areas – Kommersant' (20 June 2022), www.themoscowtimes.com/2022/06/20/russia-to-expand-high-tech-surveillance-to-ukraine-border-areas-kommersant-a78043.

[26] There is no doubt that the potential of FRT has a negative impact on freedom of assembly. Facial recognition systems integrated in street surveillance cameras significantly reduce the chances of

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

rallies against Russia's attack on Ukraine were taking place all over Europe, protests in Russia had been sporadic and small-scale. In Moscow, with a population of more than 12 million, the number of protesters never exceeded a few thousand. Large numbers of protesters were also never seen on the streets in other cities.

There are different reasons for this. On the one hand, the small number of Russians who expressly oppose Russian aggression might be interpreted to confirm overall society's support for the current government, prevailing approval of the policies being pursued, and agreement with the arguments put forward by the authorities as to the validity and necessity of the 'special operation' (the term used in Russia to refer to the attack on Ukraine). This support arguably stems from strong influence of national mass media, general mentality, and from the iconisation of Russia as a superpower and even 'true-values protector',[27] which has to be respected and abided by. On the other hand, owing to the massive arrests of protesters, those opposing the war see it as dangerous to protest.

From the very beginning of the invasion of Ukraine, Russian authorities effectively stopped any anti-war protest efforts. In addition to prohibiting protests against the Russian military attack on Ukraine and traditional street arrests, Russia employed FRT to track down and apprehend anti-war protesters. Analysis of online posts and social media reveals that Russian citizens are in no doubt that Big Brother is literally watching them, and that the FRTs used by the authorities in public spaces will prevent them from remaining unidentified and simply being part of the crowd.

According to Human Rights Watch, Russian authorities have been integrating public surveillance systems with FRT across the country and using these technologically advanced systems to identify and prosecute peaceful protesters since 2017.[28] The authorities do not deny this information and do not comment on the details of the extent of use, thus reinforcing the deterrent effect.[29] Already back in 2017, it was announced on the official website of the Mayor of Moscow that more than 3,500 cameras had been connected to the Joint Data Storage and Processing Centre, including more than 1,600 cameras in the entrances of residential

people remaining anonymous, which is often crucial during protests. Particularly in countries where freedom of assembly is restricted and where administrative or criminal liability for anti-government rallies can be imposed, the likelihood of being identified, even after a rally, encourages people to refuse to express their opinions or ideas and to take part in the democratic process (the chilling effect).

[27] See, e.g., LIFE, 'Путин: Россия никогда не откажется от любви к Родине и традиционных ценностей' (9 May 2022), https://life.ru/p/1492826.

[28] Human Rights Watch, 'Submission by Human Rights Watch on Russia to the Human Rights Committee' (15 February 2022), www.hrw.org/news/2022/02/15/submission-human-rights-watch-russia-human-rights-committee.

[29] While in Europe and many other Western countries companies offering face recognition platforms faced a lot of criticism and even fines, personal data protection seems to be much less stringent in Russia. Face recognition platforms in Russia boast wide use by private individuals. See VestiRu, 'FindFace: российская программа распознавания лиц завоевывает мир (22 February 2016), www.vesti.ru/article/1656323.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

buildings, with many closed-circuit television cameras in the city also reportedly being connected to a facial recognition system.[30] Additional cameras were placed during later years, and after the start of the war, surveillance was increased in the places where protests typically take place.[31] The collection of biometric data also continues to be strengthened. For instance, in May 2022, Russian authorities demanded that the four largest state-owned banks hand over their clients' biometrics to the government.[32] To ensure that the biometric data is collected from the practically entire adult population, the laws were amended in July 2022 to oblige banks and state agencies to enter their clients' biometric data, including facial images and voice samples, into a central biometrics database. This measure, which does not require clients' consent to share data with the government, came into force in March 2023.[33]

Human Rights Watch stated in its submission to the Human Rights Committee on Russia on 10 February 2022 that the use of FRT, including for police purposes, is not regulated by Russian law. It highlighted that such use in the context of peaceful protests contradicts the principle of legal certainty by interfering with the rights to liberty and security by using methods that are not adequately supervised or provided for by law. It also violates the rights to privacy and peaceful assembly and is used in a discriminatory manner on the basis of political opinion. Human Rights Watch suggested that the Committee urge the Russian government to end the use of facial recognition during peaceful protests and ensure that all government use of facial recognition is strictly regulated by law.[34] It is not likely that Russia intends to implement this proposal in the near future, as the FRT has proved to be a powerful tool to control protests against the country's policies.

[30] ОВД-Инфо, 'Как Власти Используют Камеры и Распознавание Лиц Против Протестующих' (17 January 2022), https://reports.ovdinfo.org/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih. The use of FRTs to stop protests in the country caught the attention of the international community in 2019, when women's rights activist Ms Popova filed a lawsuit after being detained for an unauthorised picket in 2018. Ms Popova claimed that the video used in her case file contained evidence of the use of FRT. In September 2019, Ms Popova and the politician Mr Milov filed another lawsuit alleging that the authorities use the technology to collect data on public protesters. However, Russian national courts rejected both claims, as well as all other similar claims. Human Rights Watch, 'Moscow's use of facial recognition technology challenged'(8 July 2020), www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged.

[31] After March 2022, additional surveillance cameras, presumably with facial recognition, were installed on Nevsky Avenue in St Petersburg, where some anti-war protests had been held.

[32] *Moscow Times*, 'Russian banks to share clients' biometric data with the state – Kommersant' (31 May 2022), www.themoscowtimes.com/2022/05/31/russian-banks-to-share-clients-biometric-data-with-the-state-kommersant-a77844.

[33] Federal Law of July 14, 2022 No. 325-FZ On amendments to Articles 14 and 14-1 of the Federal Law 'On Information, Information Technologies and Information Protection' and Article 5 of the Federal Law 'On Amendments to Certain Legislative Acts of the Russian Federation', Official Publication of Legal Acts, Russia. http://publication.pravo.gov.ru/Document/View/0001202207140096?index=3&rangeSize=1.

[34] Human Rights Watch, 'Submission by Human Rights Watch on Russia'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

8.4 CONCERNS ASSOCIATED WITH THE USE OF FRT IN WARTIME

While there is no doubt that the FRT brings many advantages to both sides of the conflict, it also raises a number of concerns. The main ones are the possibility of false identification, misuse of FRT, and problems associated with its continued use after the war.

8.4.1 *False Identification*

One of the significant risks linked to the use of FRT is false identification. FRT might produce inaccurate results; moreover, the input data determines the accuracy of FRT systems. This might be forgotten in wartime stress, especially considering the limited training for persons using it.

As to the recognition of dead soldiers, there is little research about FRT effectiveness in the case of deceased or distorted bodies. One recent study recognised that decomposition of a person's face could reduce the software's accuracy, though, according to researchers, overall the research results were promising.[35] Similar findings were presented in academic research on automatic face recognition for humanitarian emergencies, which concluded that automatic recognition methods based on deep learning strategies could be effectively adopted as support tools for forensic identification.[36] However, it has to be taken into account that the quality of the photos obtained in a war scenario can be substantially different from those taken under optimal conditions. Poor image quality, poor lighting, changes in faces after death, and injuries could lead to false positives or negatives.

When Ukraine started running FRT on dead Russian soldiers, it received a lot of criticism. This largely revolved around the idea that sending pictures of dead bodies to their relatives could constitute psychological violence and that any false-positive recognition of a dead soldier and subsequent notification of his family about his death would cause distress to the family. One could argue, however, that this second point might be slightly exaggerated. To cause stress, the misidentified family must first actually have a son at war in Ukraine, and second, they must have the option to try to contact him or his brothers in arms and verify the information received. Furthermore, one might expect that, at least currently, when FRT is taking its first steps as a military technology, its ability to identify fallen enemy soldiers remains

[35] David Cornett, David Bolme, Dawnie W. Steadman, Kelly A. Sauerwein, and Tiffany B. Saul, 'Effects of postmortem decomposition on face recognition' (1 September 2019), Oak Ridge National Lab, Oak Ridge, TN, United States, www.osti.gov/biblio/1559672#:%7E:text=During%20the%20early%20stages%20of,have%20little%20effect%20on%20detection.

[36] Ruggero Donida Labati, Danilo De Angelis, Barbara Bertoglio, Cristina Cattaneo, Fabio Scotti, and Vincenzo Piuri, 'Automatic face recognition for forensic identification of persons deceased in humanitarian emergencies' (2021), *2021 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, https://ieeexplore.ieee.org/document/9493678/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

considerably limited. The Ukrainian side tested the possibilities of identifying deceased soldiers and the impact of such identification on the Russian people; however, currently Ukraine focusses its war efforts on eliminating as many enemy soldiers as possible, and recognition of the dead ones is not on the priority list.

More problematic would be a mismatch by facial recognition performed in the warzone on live persons and when identifying the enemy. This could lead to the eventual prosecution (or even killing) of wrongly identified persons. Thus, FRT in no case should become a single tool to define the fate of a person, as the technical mistake could lead to fatal outcomes. Of particular importance to avoid false positives when using the FRT in a war context is to double-check a face recognition match using alternative intelligence and contextual information. While at the stage of after-war investigation of war crimes, FRT will most likely be used as a complementary source of information, double-checking its results, it is less realistic to assume such control in the fog of war.

8.4.2 *Misuse of FRT*

In an active war zone, it is difficult to guarantee only limited use of FRT or to enforce any restrictions on the use of the technology. It is a challenge to ensure that FRT is used only for the purposes it is designated or by the authorised persons.

As FRT is a new technology in a war zone with little legal regulation in place, it is tempting to experiment with it and its possibilities. This allows the almost uncontrolled proliferation of FRT uses. If the deployment of FRT on the battlefield proves effective for identifying enemy soldiers, this may lead to its incorporation into systems that use automated decision-making to direct lethal force. This possibility only increases with the development of the accuracy of the FRT. The more precise the tool actually is, the more likely it will be incorporated into autonomous weapons systems that can be turned not only on invading armies, but also on, for instance, political opponents or members of specific ethnic groups.[37]

Another issue is the possibility of the unauthorised use of FRT. One strategy to mitigate this risk is to create a clearly established system that verifies the identity and authority of any official who is utilising it. The administrator of a body using the FRT should be able to see who is conducting searches and what those searches are. Moreover, the system should be designed with the possibility to revoke entry from a distance, disabling the possibility of use in case of abuse.[38] However, legal instruments should be developed and personnel trained to implement such a control.

[37] Darian Meacham and Martin Gak, 'Face recognition AI in Ukraine: Killer robots coming closer?' (30 March 2022), *openDemocracy*, www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/.

[38] See 'At war with facial recognition: Clearview AI in Ukraine' (17 May 2022), Interview with Hoan Ton-That, CEO of Clearview AI, at kwon0321, Days Tech, https://daystech.org/at-war-with-facial-recognition-clearview-ai-in-ukraine/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

8.4.3 *Continued Use after the War*

Modern technologies share one common feature – once people learn to use them, the technologies spread, and their usage intensifies. This phenomenon has been observed in Ukraine: in September 2022, it was announced that additional cameras with facial recognition were already planned for installation in public places in the Kyiv region; with the declared goal being to counter sabotage and intelligence groups and search for saboteurs.[39]

It is likely that authorities who get comfortable with using FRT during wartime will be willing to continue its use after the war ends. It is thus difficult to anticipate that FRT introduced during a war will not endure throughout peacetime. In such a situation, the issues related to privacy, discrimination, and other concerns explored in this volume, which are less concerning in wartime, become important.

The subsequent use of information gathered during the conflict, including images of battlefield victims, raises another set of concerns. In the case of the Russia–Ukraine military conflict, the Clearview AI database is considerably enriched with pictures of deceased persons or persons who were interviewed or simply checked at a checkpoint during wartime. While the legality of harvesting pictures from social networks causes doubts, even more ethical and legal issues arise as to images taken of dead persons or persons who were not informed about the collection of their data (which would be naive to expect in a war zone). When FRTs are employed in the EU for border control and migration, the sensitive data required for facial identification is collected by public agencies, the data subject is informed, and EU law strictly regulates the process. Naturally, the use of FRT in a war zone differs materially in this regard.

8.5 CONCLUDING REMARKS: FRT – A NEW TOOL OF MILITARY TECHNOLOGY?

Any war is a tragedy for human society, but it also acts as a step in the further development of technologies. This is evident in the current Russian war against Ukraine. The conflict in Ukraine represents a coming of age for a number of advanced technologies, from drones to commercial satellites, loitering munitions, and FRT. As Lauren Kahn notes, Ukrainian steppes have been transformed into a proving ground for next-generation technologies and military innovations in this war.[40]

[39] Віолетта Карлащук, 'На Київщині встановлять понад 250 камер з розпізнаванням обличчя' (9 September 2022), *Суспільне | Новини*, https://suspilne.media/279898-na-kiivsini-vstanovlat-ponad-250-kamer-z-rozpiznavannam-oblicca/?.

[40] Lauren Kahn, 'How Ukraine is remaking war. Technological advancements are helping Kyiv succeed' (29 August 2022), *Foreign Affairs*, www.foreignaffairs.com/ukraine/how-ukraine-remaking-war?utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20220907.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010

From the perspective of FRT companies, the contribution of FRT to the Ukrainian war effort, in terms of proving ground and use, yields valuable data and – at the same time – visibility and even an advertisement for FRT companies. It is also difficult to argue against the fact that offering FRT technology to Ukraine during the war was a wise choice because it created a chance for the technology to prove its worth. Likely, companies whose products are being deployed in this conflict (both in Ukraine and in Russia) in a short time will become defence contractors offering their FRT as military technology.

In such a way, the broad and effective deployment of modern tools in Ukraine in its efforts to stop Russia's military invasion is bringing emerging technologies into the mainstream of the military. In an era where technology reigns, it comes as no surprise that artificial intelligence is being employed for military purposes. FRT is advancing and spreading, and it might safely be projected that FRT will be a well-established military – and propaganda – tool in a decade or two. While one can argue that bringing FRT to war is dangerous and should be avoided because of the associated risks, it would be naive to believe that this will not happen. What can be done, though, is to develop international standards on the accepted use of FRT for military purposes – work that awaits the international community in the near future.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 19 Nov 2026 at 12:08:31, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009321211.010