www.ijonest.net

Identity and War: The Role of Biometrics in the Russia-Ukraine Crisis

Mikhail I. Gofman
California State University, Fullerton, United States

Maria Villa
California State University, Fullerton, United States

To cite this article:

Gofman, M. I. & Villa, M. (2023). Identity and war: The role of biometrics in the Russia-Ukraine crisis. *International Journal on Engineering, Science, and Technology (IJonEST), 5*(1), 89-111. https://doi.org/10.46328/ijonest.143

International Journal on Engineering, Science, and Technology

2023, Vol. 5, No. 1, 89-111 https://doi.org/10.46328/ijonest.143

Identity and War: The Role of Biometrics in the Russia-Ukraine Crisis

Mikhail I. Gofman, Maria Villa

Article Info

Article History

Received:
18 September 2022
Accepted:
23 December 2022

Keywords

Biometrics
Security
Cybersecurity
Ukraine
Russia
War
Military

Abstract

On February 24, 2022, Russia launched a full-scale invasion of Ukraine. While many experts have examined the conflict from geopolitical, economic, and humanitarian angles, few have formally studied biometric technologies' role in the conflict. Our analytical survey helps fill this gap. On one hand, the faces and fingerprints of refugees are being used to protect the national security of asylum countries in what has become the worst refugee crisis since WWII. Biometric passports simplify travel for Ukrainian refugees to countries in the European Union through a visa-free traveling regime. Meanwhile, the United Nations (UN) uses fingerprinting to distribute cash aid to eligible Ukrainian refugees securely. Biometrics may also become a potent weapon for fighting the war-exacerbated human trafficking crisis in Ukraine. On the other hand, refugees applying for Canadian, UK, and other visas were subject to long waiting times to fulfill the biometric registration requirement of the visa application. Biometrics were also forcefully collected from Ukrainians deported to Russia from Russian-occupied territories in Ukraine. Meanwhile, Russia uses public face recognition to identify, arrest, and prosecute anti-war activists. From the refugee crisis to the battlefield to information warfare, our work analyzes reports of how the use of biometric technologies has impacted the ongoing conflict. We also present potential solutions to problems stemming from the use of biometrics during the ongoing conflict. Our examination of the conflict through a lens of biometrics applications can help researchers and analysts deepen their comprehension of the ongoing war as well as other and future conflicts. The information presented here is current as of the time of the writing. The reader interested in the subject presented here is highly encouraged to follow the latest reports and analyses from the sources tracking the conflict.

Introduction

On February 24, 2022, Russian Federation launched a full-scale invasion of Ukraine [4]. The move was a major escalation in the Russia-Ukraine conflict that began in 2014 with the Russian annexation of Ukrainian peninsula of Crimea and skirmishes in the Donbas region of Ukraine [66]. While many experts have examined the Russia-Ukraine conflict from geopolitical, economic, and humanitarian angles, no work has formally studied the significant ways in which biometric technologies are shaping the ongoing conflict. Our work fills this gap.

Biometrics is a fast-growing field of science and technology that focuses on identifying people based on physical and behavioral characteristics such as face, voice, fingerprints, and DNA. Modern biometric technology can quickly and automatically identify and verify people. This ability has led to the widespread use of biometrics in military, investigative, and civilian applications, which include the ongoing Russia-Ukraine war.

On one hand, biometrics has seen uses that can be classified as positive. Fingerprinting and face recognition systems are helping to secure entrances into asylum countries accepting Ukrainian refugees during what has become the worst refugee crisis in Europe since World War II. The United Nations High Commissioner for Refugees (UNHCR) uses biometrics to verify the identities of Ukrainian war victims who are eligible for the UN's humanitarian cash assistance program. Ukrainian refugees possessing a biometric passport can travel to Schengen countries without a visa.

On the other hand, the use of biometrics in the current conflict has also been highly controversial. For example, multiple media sources reported that Ukrainian refugees were experiencing excessively long waiting times to schedule biometric registration appointments required for obtaining visas for entering asylum countries. Russia has been collecting biometrics of forcefully deported Ukrainian citizens from occupied areas and used face recognition in public places to identify those who voice opposition to the ongoing war. The Ukrainian army has used online face search engines to gather personal information of captured and killed Russian soldiers to notify the soldiers' families in an attempt to turn the tide of Russian public opinion against the war.

In this paper, we present and analyze the roles of biometrics in the conflict. Our methodology introduces and analyzes the documented incidents of biometrics being used for refugee and immigration processes, repression of dissidents in Russia, and for military, intelligence, or information warfare purposes. For each of these areas we also discuss how the use of biometrics is impacting the area of conflict as revealed by the documented incidents and how the role of biometrics is likely to evolve in the area. Where appropriate, we also provide potential solutions stemming from the use of biometrics. We conclude by using the information we learned from the analysis of reports to project how the role of biometrics may evolve with the conflict.

Our work is structured as follows: Section 2 focuses on the roles and impacts of biometrics in the refugee crisis resulting from the conflict. Section 3 describes the use of biometrics in the forced deportation of Ukrainians. Section 4 discusses how Russia has used biometrics to arrest and prosecute Russian citizens who have publicly opposed the war. Section 5 discusses how biometrics are being used for military, intelligence, and information war applications. Section 6 discusses how biometric technologies can help fight human trafficking in Ukraine that is exacerbated by the conflict. Finally, Section 7 concludes with an analysis of topics discussed.

Biometrics and the Refugee Crisis

The Russia-Ukraine conflict spurred the largest refugee crisis in Europe since World War II. An estimated 11.3 million Ukrainians have left their homes as of the time of this writing [44]. The use of biometrics had both positive and negative impacts on the refugee crisis. Ukrainian refugees in possession of biometric passports are now authorized to travel visa-free to the countries in the Schengen Zone and stay for 90 days (Shengen Zone consists of 26 European countries with a mutual visa-free travel regime; Ukraine is not in the Schengen Zone) [53]. This is an example of the potential for biometrics to help speed up the immigration process for refugees while safeguarding the asylum countries from undesirable entrants. The biometric passports store the holder's biometrics on a secure chip (often face and/or fingerprints) which allows the border control agencies of asylum countries to quickly match the biometrics of the passport holders against the biometrics stored on the chip, thus mitigating the problems associated with fake identity documents.

At the same time, the use of biometrics had multiple documented negative impacts. As refugees attempt to procure visa for entering the asylum countries, such as Canada and UK, they are required to register their biometrics with the country's immigration office. The immigration offices, however, were reportedly slow to register biometrics of asylum seekers. Furthermore, refugees arriving in the asylum countries may also be required to register their biometrics with country's social benefit system to receive social benefits. Refugees have reported the registration process to be long, tedious, and frustrating.

In this section, we discuss and analyze the reports to help understand the contrasting impacts of biometric registration requirements and biometric passports on the ongoing refugee crisis. We also identify emerging problems, discuss potential solutions proposed by others, and, where appropriate, present our own recommendations.

Visa Issues

Ukrainians fleeing the war zone are reportedly subject to the long and tedious process of obtaining entrance visas to the asylum country. One factor increasing the length of the process is the requirement that refugees register their biometrics with the asylum country's immigration office. The cause of delays is largely attributed to the immigration offices being overwhelmed by the sudden influx of refugees, offices being located geographically far away from refugee locations, and issues related to the inefficient operation of offices [8]. Multiple instances of such issues have been documented in Canada and the United Kingdom.

The number of refugees affected by the biometric registration-related bottlenecks may be significantly larger than documented considering the scale of the refugee crisis. According to United Nations High Commissioner for Refugees (UNHCR), nearly 5 million Ukrainian refugees have been registered across Europe [45] as of June 2022. An estimated 6,500 refugees have arrived in the United States, with around 100,000 expected to arrive in the future [71]. Canada received over 100,000 temporary visa status applications [27]. To cope with the influx, countries such as the US, Canada, and UK have introduced various measures, as described below.

Canada The Canadian VISA process requires refugees to register fingerprints and a face photograph [28]. In response to the crisis, Canada has been prioritizing biometric registration requests from Ukrainian refugees. It has also opened the Canadian Biometric Operations Centre (CBOC) in Warsaw, Poland, where thousands of Ukrainian refugees are trying to obtain asylum in Canada. The goal is to have the facility process between 1,500 and 3,000 biometrics per day. In addition, mobile biometric testing kits have been distributed to the Canadian immigration offices in Vienna, Austria and Bucharest, Romania [11].

As an additional coping measure Canada has implemented a “risk-based approach” that waives biometric registration for individuals of ages 17 and younger, individuals 61 and older, and applicants who have been approved for a Canadian VISA in the last 10 years. The registration fee is also waived for refugees eligible for the Canada-Ukraine Authorization for Emergency Travel (CUAET) program that allows refugees to stay in Canada for up to two years.

As of the time of this writing, the reports of refugee complaints persist. Among the cited complaints are the lack of instructions and customer service regarding the registration biometrics process [57].

United Kingdom Ukrainian refugees fleeing to the United Kingdom (UK) were initially faced with issues stemming from the biometric registration requirement. For example, refugees fleeing to Scotland, where biometric scans are required for obtaining a visa, have complained of the difficulty of scheduling biometrics registration appointments [16]. The instructions, the refugees claimed, were vague and difficult to follow.

Similarly, the Northern Ireland government requires Ukrainian refugees to register fingerprints and face biometrics to obtain the Biometric Residence Permit (BRP). The BRP allows refugees to extend by two years their six-month stay granted by the presentation of the Permission to Travel to the UK letter granted by the UK government [67]. According to the government website, the BRP process takes eight weeks.

To help address these problems, in March 2022 the UK has decided to waive the pre-arrival biometric registration requirements for Ukrainian refugees and to perform the registration at the biometric registration office in Britain. The change was recommended by the UK’s security and intelligence services [36]. As of the time of the writing, we have not discovered any reports of how the scheme is impacting the refugees in practice.

United States The US Government has launched the Uniting for Ukraine program that allows Ukrainian citizens and their families to come and stay in the US for up to two years [70]. The United States also requires Ukrainian refugees to undergo rigorous health and personal background checks, pass strict biometric and biographic screenings, and obtain vaccinations and public health prerequisites [3]. Biometric screening plays an essential role in the process [25]. As of the time of this writing, we have not discovered substantial reports regarding the impacts of biometrics on the refugees seeking asylum in the US.

Discussion Throughout the years, biometrics have become an indispensable means of identity verification in immigration and border security. This is because biometrics are more difficult fake compared to, for example, forging traditional paper ID documents. Furthermore, biometric screening allows countries to identify and prevent the entry of internationally known criminals and other undesirable individuals (e.g., known terrorists).

Although getting rid of the biometric requirement could theoretically speed up the asylum-seeking process for the refugees, the detrimental effects on the national security of asylum countries would generally be unacceptable (especially during times of war). Similar conclusions have been reached by the UK government that initially refused to relax the biometric security requirements for Ukrainian refugees seeking to obtain the UK visa [18]. They cited the history of Russian government-sponsored violence in UK among reasons for the security concern.

Viability of the Selective Biometric Registration Exemptions The solution of exempting children and the elderly from the biometrics registration, as proposed by the Canadian government, brings up multiple concerns. First is the question of whether such exemptions will significantly reduce the bottlenecks in the asylum-seeking process. This is because child refugees are typically accompanied by their parents who are not exempt from having to register their biometrics. Indeed, some Canadian politicians and immigration critics have expressed this concern [33]. Similarly, those over the age of 61 may be accompanied by their non-exempt caretakers on whom they rely.

Second, the decision to grant such age-based exemptions may come at the price of national security to the asylum-granting countries. Indeed, as history shows, children and the elderly can partake in criminal and terrorist activities or be exploited by such groups [6, 19, 30, 60], and eliminating the biometric screening for these groups can allow undesirable individuals to enter the country under the guise of asylum seeking.

We believe that the root cause of the problem of the asylum process bottlenecks during this crisis is not the biometric technology or even the biometric requirement–it is how the biometric registration processes are designed and implemented. As seen from reports, some refugees must travel long distances to have biometric data collected and wait long times for appointments. These problems seem to stem from the difficulty of biometric registration offices to cope with the sudden large influx of refugees. To avoid such issues, asylum countries should continuously invest in, monitor, and optimize the operation of their biometric registration offices. Such due diligence will help develop capabilities to dynamically cope with the ongoing and future crisis.

For example, reserves of human, monetary, and technical resources can be maintained and deployed in cases of sudden surges of refugees. To ensure the availability of trained workers in times of crisis, governments can incentivize employees working in non-biometrics registration related positions of immigration offices to receive voluntary training in biometric registration processes and agree to be called upon in cases such as the current Russia-Ukraine crisis. Incentive programs can also be created to recruit and train biometrics registration reserve members from the general public.

Allocation of budget reserves can be achieved through the standard processes of strategic budget planning. Additional steps can be taken to improve operating cost-efficiency of immigration offices and funnel the savings into reserve budgets. For example, the UK Home Office –the ministerial office in the UK responsible for homeland security, law and order, and immigration– published a case study documenting a set of practices that have cut the department’s cloud computing costs by 40% [24]. The study noted that the Immigration Technology division, for example, used the auto scaling feature in their product to dynamically scale the use of computing resources depending on the demand–an IT practice that may potentially prove useful for immigration offices for maintaining a scalable biometric registration service whose computational needs can be scaled up or down depending on demands.

Similarly, immigration offices should consider the cost-benefit analysis of investing in automation technologies to help reduce the operating costs (e.g., efficient appointment scheduling systems, technical support, automated biometric enrollments, etc.). Finally, the governments of asylum countries can consider dynamically creating pop-up biometric registration sites as needed using mobile biometric technologies. We analyze such attempts by the Canadian government next.

Mobile Kits and Pop-Up Biometric Sites Solutions such as Canada's decision to deliver mobile biometrics kits to its immigration offices can be a step in the right direction. They are an attempt address one of the underlying causes of the asylum process bottlenecks–the struggle of the immigration offices to scale to the large demand. Additional biometrics kits can help offices enroll biometrics of more people and do so faster. The availability of kits can also help create additional pop-up sites in different locations in Europe. Increased locations of biometric sites can help reduce the travel burdens for refugees.

Although the use of mobile biometric technologies for addressing problems of scale can become a promising solution, its implementation can be non-trivial in practice. For example, in addition to providing mobile biometric kits, the government must also address the indirect challenges of making sure that there are sufficiently trained professionals to operate the kits, that the mobile sites are strategically placed at points to maximize their accessibility to the refugees, and that the operational aspects such as a functional system for scheduling and fulfilling appointments and clear instructions to the refugees are in place.

Furthermore, rapidly deployed pop-up biometric collection sites must address the physical and cybersecurity considerations to prevent confiscation or leakage of biometric data. For example, for a site in Ukraine, it is likely that both the Russian military as well as state-sponsored Russian spies and hackers would be interested in the capture of the biometric data of refugees. Captured data can be used for surveillance, blackmail, or strategic targeting of critics of the Russian regime, something the Russian government has been notorious for in the past. A strategy to help minimize such risks is to host such Ukrainian-based sites in areas of the country less affected by the conflict and to ensure that all data communications from the sites are done securely through properly encrypted and authenticated channels. Furthermore, kill switch systems and processes can be implemented to quickly destroy any onsite data or prevent access to systems storing biometric data. The kills witch measures can be triggered in case of a sudden invasion, infiltration of the site, and other emergencies.

Post-Arrival Biometric Checks UK's approach of requiring refugees to register their biometrics post-arrival is an interesting approach for easing the burdens of long waiting times and travel distances. With this approach, the refugees with a passport can simply travel to UK to get out of danger in Ukraine or to finally leave the country they were transiting through (e.g., Poland) on their way to the asylum country. In addition, this can drastically reduce the need of the asylum country's government to commit resources to implementing viable biometric registration processes in offices located outside of their borders as discussed in Sections 2.1 and 2.1. Instead, such resources can be channeled to optimizing and expanding the capacity of biometric registration offices inside of the asylum country to help register the biometrics of the arriving refugees.

The shift in the UK's biometric registration policy also may have security implications for both the refugees and the UK. On one hand, registering refugee biometrics in the asylum country can help increase the physical and cybersecurity controls designed to protect the biometric data. This is because the asylum country can exercise greater control over the operating environment than in offices located outside of its borders. For example, it is unlikely that the biometric office located in the asylum country will be physically raided by Russian invaders as it can be in Ukraine, and all network communications take place across the internet infrastructure operated by the asylum country.

On the other hand, it is possible that the post-arrival biometric registration approach can also introduce additional national security concerns for the asylum country. Spies, criminals, and other undesirable individuals can now enter the country more easily and without a priori registration of their biometrics. It is critical for the asylum country to implement controls that would ensure that all arrivals quickly register their biometrics; before a potential undesirable entrant is able to prosecute their plans against the asylum country.

Controls could include the asylum country not granting new arrivals the freedom of movement around the country until they have registered their biometrics. However, such approaches could result in having to keep the new arrivals in refugee camps or similar settings until their biometrics are registered. This can result in additional stress and trauma to the refugees and require commitment of resources from the asylum country to maintain such places. An alternative approach is policies that require strict tracking of those new arrivals until their biometrics are registered. Overall, more research and is needed that would allow for a solution that would protect the asylum country from the undesirable entrants with minimized negative impact on the refugees.

Biometric Passports

According to the reports, Ukrainian biometric passports have helped streamline the travel process for refugees fleeing to the countries in EU/Schengen Region. Biometric passports are government-issued legal travel documents equipped with a microchip storing the holder's biometric information in the standardized digital format. As of 2022, standard biometric passports provide for the storage of face, fingerprints, and iris [26] biometrics. The biometrics on the chip can be read using the contactless reader system and be matched against biometrics of the passport holder acquired during the screening process.

In 2015, the Ukrainian government started issuing biometric passports [76]. All citizens reaching the age of 14 must receive a biometric passport containing fingerprints. Citizens objecting to biometric passports on religious grounds may request a non-biometric passport [74]. The fingerprints are not included in passports for children under 12. Upon reaching the age of 12, the child may receive a passport with the consent of the parent [46].

In 2017 the European Union (EU) authorized a 90-day visa-free stay/traveling in all EU countries for Ukrainians who possess a biometric passport [5]. After the Russian invasion of Ukraine these rules were extended to also allow admission of Ukrainian refugees without biometric passports on the humanitarian grounds. Under the new rules, refugees may stay in EU for up to three years without applying for asylum [77, 9, 68, 55].

Discussion Offering a visa-free 90-day travel/stay in the EU for Ukrainians with a biometric passport can help alleviate stress for Ukrainian refugees looking to flee to EU. Although admission on humanitarian grounds is an available option, the process is more straightforward with a biometric passport. In addition, biometric passports can be an efficient tool in helping secure the asylum countries as they are difficult to forge compared to traditional passports. The standardized nature and identity verification power of biometric passports can be useful for other purposes where refugee identification is important–for example, getting access to social benefits in the asylum country or seeking humanitarian aid from world organizations such as the UN.

Biometrics in Social Benefits and Humanitarian Aid

Biometrics also continue to impact refugees once they arrive in the asylum country. Some countries, such as the United Kingdom, require refugees to register their biometrics to obtain social benefits. The United Nations High Commissioner for Refugees (UNHCR) has also recently successfully used biometrics to distribute cash assistance to Ukrainian refugees and those Ukrainians who chose to stay in Ukraine.

Social Benefits Once the refugees arrive at the asylum country, they are often eligible either for special refugee help programs or receive social benefits similar to those of the country’s citizens. The United Kingdom (UK) has a Universal Credit program, which is currently helping Ukrainian refugees by covering their living costs [54]. Obtaining the Universal Credit benefits requires refugees to obtain a Biometric Residence Permit (BRP) upon arrival [39]. BRP is also required for Ukrainian refugees to find employment in the UK.

According to refugees, scheduling biometric scans to obtain BRP was difficult and confusing. Such cases were cited by refugees seeking asylum in the Coventry region [40]. There are also reports of refugee frustration stemming from the office staff not showing up to the BRP appointments.

UNHCR Cash Assistance Biometrics also plays important roles in the UNHCR’s Multipurpose Cash (MPC) program designed to help the affected Ukrainians by lending them cash money [22]. Refugees can spend the money as needed.

The refugees who applied for the program receive a text message. They then then present the message at the cash assistance enrollment center where the message is verified by the staff. Second, a fingerprint scan is used to create a proof of enrollment. A refugee then receives a PIN number that can be used to collect cash at ATMs. As of the time of the writing, the program is already operating in parts of Ukraine, Poland, Slovakia, and Moldova. The UN is also experimenting with the use of iris biometric to help make the biometric enrollment process contactless [10].

Discussion The recurring theme of the difficulty of scheduling biometric appointments seems to affect not only the refugees seeking to obtain asylum visas, but also the refugees who have arrived in the asylum country and are seeking to obtain social benefits. The previously discussed measures of having backup staff and resources to handle large influxes of refugees can be applied here as well.

The seemingly successful cash distribution program run by UNHCR is an example of how biometric technologies can help protect the integrity of the humanitarian aid distribution process. However, as discussed previously, biometric enrollment sites, such as those operating in parts of Ukraine, must take measures to protect the physical and cybersecurity of biometric data from sudden seizures and misuse. This is because refugee biometric data can be of use to Russian state actors as means of tracking down persons of interest, future blackmail, and other purposes. For example, the UN must protect its biometric enrollment systems from Russian state actors looking to steal biometric data or to disable to impede the aid distribution (possibly as an indirect retaliatory response against Ukraine or against UN member states supporting measures unfavorable to Russia).

Finally, the UN’s experimentation with iris biometrics in the MPC program can be helpful as well. At the same time we believe that the final system should support both iris and fingerprint biometrics to help address issues of biometric universality – where individuals lacking a specific biometric are unable to use the system.

The benefits of contactless enrollment and verification as well as identification accuracy provided by the iris biometric have well-documented benefits [29]. The use of iris biometrics would also allow refugees who are unable to use fingerprints (e.g., as in cases of hand injuries from explosions or burns) to easily enroll in the system with iris biometrics. Similarly, those unable to enroll with iris biometrics, could use their fingerprint. Overall, support for multiple biometrics can help accommodate a wider population of individuals.

Biometrics and the Forcefully Deported Ukrainians

Russia has been collecting unspecified types of biometrics of Ukrainian citizens who were forcefully resettled from the occupied Ukrainian territories to Russia. According to reports, the Ukrainian citizens have been taken from their homes to the filtration camps located in the occupied areas where their biometrics were scanned, and their Ukrainian passports were confiscated [61]. After being processed through filtration camps, the deportees were reportedly taken to Russia where they were pressured to settle.

Although we found no verifiable information on how Russia uses biometrics of the forcefully deported (or what type of biometrics are collected), we see many possibilities. First, according to the reports, one of the purposes of the filtration camps is to identify pro-Ukrainian individuals [50] who are then imprisoned. The collected biometrics can be used to identify such known individuals targeted by the Russian government. This can be done, for example, by matching the person’s face against the online photographs featured in social network sites, news media, etc. Also, of concern here is the potential use of biometric passports held by the forcefully deported as tools for identifying pro-Ukrainian activists.

Second, biometrics can be used for surveillance and tracking the forcefully resettled Ukrainians. The resettled can be tracked in the Russian territory with the public face recognition surveillance system deployed in Russia in 2020 [34, 41]. In 2022, the Russian Ministry of Emergency Situations also proposed the deployment of face recognition-based surveillance at the Russian borders and in Russian-held territories in Ukraine such as Crimea [43]. The data collected by surveillance systems can then be used to arrest or further persecute the resettled for actions deemed unacceptable by the Russian government. The actions can include anti-war protests, communicating with individuals located in other countries, and social network posts.

It should also be noted that tracking of deportees can potentially continue even if they leave Russia. Biometric data can be used to, for example, identify deportee faces in social media posts, news broadcasts, or even in hacked video streams from public and private cameras abroad. In addition, Russian lawmakers have adopted a bill that, if passed, would require banks to share the biometrics of their customers with the government services [31]. This could potentially include sharing the biometrics of the forcefully resettled Ukrainian citizens using the services of Russian banks, which would give the government even more biometric data useful for surveillance and tracking.
Third, the biometric data can be used in construction of deepfakes; fake photographs and videos of the individual generated using Deep Learning artificial intelligence algorithms [49]. These deepfakes can then be strategically used to blackmail the deportees or be utilized for propaganda purposes. Indeed, deepfakes of the Ukrainian President Volodymyr Zelensky and the Russian President Vladimir Putin have been circulated throughout the conflict as means of waging information warfare [1].

Biometrics in Wartime Russia

Russia has one of the largest public face recognition camera networks in the world. As of 2020, a network of around 189,000 cameras was deployed on the streets, busses, and other public places with thousands of cameras in Moscow being connected to the "Safe City" face recognition system. According to Educationaltechs [51, 15], the system can identify individuals even if up to 40% of their face is covered. During the COVID-19 pandemic, the system was allegedly used to successfully identify individuals on streets of Russia who were violating COVID-19 safety regulations [23].

During the ongoing conflict, Russia used the face recognition network to identify, harass, and arrest individuals who have publicly opposed the war. According to the reports, Russian police used face recognition to identify and arrest 67 anti-war activists and journalists in St. Petersburg on June 12, 2022, which marks the national Russia Day holiday [64]. The face recognition system has allegedly identified the protesters in the crowd of people.
In addition, on July 25, 2022, Moscow police used the face recognition system to identify and arrest the leader of the Russian Union of Right Forces party Leonid Gozman. Gozman, was a persistent critic of Russia's war in Ukraine and was arrested on charges of not promptly reporting his dual citizenship in Israel. However, Gozman and his supporters believe that the real reason for his arrest was Gozman's criticism of the current Russian regime and its war [65]. According to the U.S. Department of State [56], many more Russian dissidents have been arrested since the start of the crisis. It has also been reported that some activists (e.g., Arina Yaroslavtseva) have been fingerprinted at the police station after arrest.

The activists are often arrested or fined for violating Russia’s laws concerning the spreading “fakes” and discrediting the Russian army [78]. According to the Russian government officials and government-run media, the laws are designed to help ensure national security. Under such circumstances, the public face recognition system widely deployed in Russia before February 24, 2022, has seemingly become a powerful tool for enforcing such laws.

Prior to deployment of the public face recognition system, Russian citizens [52] have long expressed concerns over Russia’s use of their public face recognition to crack down on protesters. The arrests of anti-war activists in Russia appear to validate such concerns.

Although little can be done from the outside to control Russia’s use or abuse of biometric surveillance systems during the war, sanctions, and curbs on exporting biometric technologies to Russia may help limit the exacerbation of the problem. In addition, it is reasonable to conjecture that (although we found no official documentation) Russian activists are already using face coverings and similar techniques that activists around the world [14] use to prevent their faces from being recognized. More advanced face recognition technologies, however, can robustly recognize occluded faces (e.g., [17]). The reported 40% accuracy of the Russian system in recognizing partially occluded faces, if accurate, is more evidence that traditional occlusion techniques for evading face recognition may gradually become less effective.

Biometrics in Military and Intelligence Gathering

The military and intelligence applications of biometrics in the conflict was thus far characterized by the often-controversial use of online face search engines. Face search engines have been used on the battlefield for identifying combatants by matching their face photographs to their photos on the web. The roles of these services will likely continue to evolve as the conflict progresses. For example, the Ukrainian army used the service provided by the US-based company ClearView AI to identify the faces of captured and killed Russian soldiers. The Wired magazine has documented the use of the Russian FindClone face search service by the journalists from the Bellingcat company and by the French Tactical Systems defense company [58] to identify the faces of Russian soldiers.

Online sleuths and those participating in open source intelligence gathering can also use face search services to gather strategic and tactical information that can influence the progression of the conflict. For a face search engine can be used to identify or confirm the individual in the photograph to be a strategic target such a general or a high-ranking government official visiting a known location in the photograph. The information can then be passed to the military to direct the actions on the battlefield. Indeed, since the conflict started, Ukraine has successfully leveraged their intelligence to identify and eliminate multiple Russian generals. It would not be unreasonable to conjecture that such search engine services could be or have been used in the operation.

Although the reports of Russia’s use of face matching services for military applications is not well documented, Russia has the technology for doing so and it is reasonable to assume that it uses them. To help limit Russia’s access to face search engines, some companies, such as US company ClearView AI [47] and a similar Polish company service PimEyes [42], fearing the misuse of the technology by the Russian side have banned the use of their services by the Russian customers [42]. However, such moves are unlikely to bar the Russian military from using the face search technology. Existence of the Russian service FindClone confirms that Russians already possess advanced face search technology and may have developed even more powerful and robust face matching engines that it keeps classified.

In addition, the FindFace face matching service provided by another Russian company NtechLab uses an advanced face matching algorithm based on the artificial neural networks that has won multiple international face matching competitions including the University of Washington’s 2015 NTechLab MegaFace Benchmark challenge [38]. Between 2016 and 2018, FindFace offered the functionality to match the subject’s face to the faces in the photographs uploaded to the VK social network.

In this section, we begin with brief discussions on how the ClearView AI, PimEyes, and FindClone technologies have thus far been featured in the conflict. We then discuss and analyze the potential impacts their use can have on the conflict. Finally, we briefly mention some of the newer technologies, such as the mobile DNA analysis forensic system that was donated to Ukraine by the French government.

ClearView AI

The ClearView AI, a system originally designed for use by law enforcement, was offered to Ukraine’s Ministry of Defense after the company’s Chief Executive saw the Russian information sources claiming that the captured Russian soldiers in Ukrainian custody were merely actors [20]. The Ukrainian army used the ClearView AI face search engine to match photographs of the killed and captured Russian soldiers against the faces on the web and thus establish their real identity [20].

As of the time of this writing, more than 8,600 reported cadavers and captured Russian soldiers have been identified by Ukraine using ClearView AI. The faces of Russian subjects were matched to the photos on the web such as those appearing in Instagram and the Russian VKontakte social network [73]. From the social network accounts, the subjects’ family relations were identified and notified with (sometimes graphical) photographs of the subject–a tactic meant to stir anti-war sentiment in Russia.

Ukraine has also used ClearView AI at the military checkpoints to investigate if an individual claiming to be Ukrainian is possibly a Russian infiltrator or a saboteur [48].

PimEyes, FindClone, and Other Platforms

Although ClearView AI face search has thus far seen the most widely documented use throughout the conflict, there are similar technologies such as the PimEyes face search engine created by the Polish company and the Russian FindClone service. We briefly discuss the presence of these services during the conflict.

PimEyes [2] uses an artificial intelligence-based facial recognition system to search for images of the subject's face on the web. According to the company's terms of service, the subscribers may only use the service to search for their own images as, for example, means of identifying illegal use of images featuring the subject's face.

Since the start of the conflict, the company behind PimEyes has been receiving subscription requests from users based in Russia. The company has restricted their services to all users based in Russia due to concerns of the service being used for purposes of continued aggression in Ukraine. Although the decision may bar users based in Russia from using the service, the service is in theory still usable by the Russian operatives or partners outside of Russia. Due to the restricted access to services like Clearview AI and PimEyes, Russians may turn to Russian face search services such as FindClone.

Furthermore, although the Russian FindFace service no longer provides the web search feature, it is not unreasonable to suppose that the Russian operatives are using the technology in military and intelligence applications in the conflict to identify strategic targets such as Ukrainian government officials, generals, etc. The use of the technology may be covert or not yet publicly documented. Similar scenarios are likely for the FindClone technology.

It should also be noted that FindClone is also being used by users outside of Russia and by groups known to not be pro-Russia. For example, the Netherlands based investigative journalism company Bellingcat used FindClone throughout the conflict to identify the bodies of dead Russian soldiers [12]. Furthermore, the Tactical Systems French military defense company has used FindClone in their Open Source intelligence gathering operations [62, 59].

PimEyes [37] is an online face engine that uses an artificial intelligence-based facial recognition system to search for pictures of the given faces on the internet. It performs a reverse engine search using face recognition search technologies.
People subscribe to this service and the service is designed to only let subscribers search for their own images online. Anyone, except for Russians, can get a subscription to PimEyes.

The role of face search services in the conflict have been complex and controversial. First, there is an issue of agents with agendas attempting to strategically poison the search results of the face search engine by, for example, disseminating real or fake photos of individuals on fake social media accounts. Second, there are issues of malicious and unethical use of these face search engines by the belligerents and the general public in ways that can influence the conflict. Third, there are issues related to the risks of false positives–a scenario where a face of a subject is incorrectly matched to a face of another. Fourth, there are issues related to whether the capability to identify faces of the belligerents is effective in meeting the intended military and information warfare goals. We analyze such issues in this section.

Strategically Misleading the Face Search Engines Any search technology has the inherent risks of leading the user to the sources of misinformation and disinformation. Indeed, poisoning of search results is a common tactic in information warfare [7]. Such concerns do not exclude the use of face search engines in the current conflict. A party with an agenda can try to strategically poison the search results of the face search engine by posting fake photos of individuals, posting real photos on fake social media accounts, or using other similar tactics to achieve military, political, or propaganda goals. This is especially concerning considering the historical use of sophisticated online disinformation techniques by Russia.

In the era of fake social media accounts and doctored and synthetically generated images, an actor cognizant of the role of face search engines in the war can attempt to frame an individual such as the prisoner of war (POW) by attempting to strategically mislead the face search engines used by the captors. For example, an actor wishing for a conviction of a POW can create a fake social accounts and internet posts with photos (real or fake) featuring the POW's face in hopes of the face being matched by an engine. The nature of the photos can be interpreted as evidence of criminal activities as perceived by the captors. Fake accounts and posts can even be created proactively in hopes that an individual will eventually fall prisoner to the enemy. Such a tactic would be useful because the aforementioned approach of creating an account after the prisoner's capture may seem suspicious to the investigators examining the account's creation date. Similarly, fake online posts can be created to help clear real current and potential future war criminals from being convicted.

Although the issues of fake social media accounts and online posts are a broad problem transcending the face search engines, uncritical reliance on face search engines can increase the power of such disinformation techniques by directing the investigators to disinformation sources. This is especially problematic during wartime when and where the investigators may lack the time or resources to perform careful checking and may see the search engine as a simple and efficient solution for quickly gathering evidence.

Misusing the Search Engine Services All face search engines have an acceptable use policy–a contract between the user and the search engine company that defines the terms of how users may use the service. Violation of the terms by the user can be seen as grounds of banning the user from using the service. Although both ClearView AI and PimEyes have rules in their acceptable use policies to prevent problems such as violation of privacy and other forms of criminal use, users involved in the conflict can choose to violate those terms to achieve their goals. Next, we discuss issues related to misuse of face search engines.

First, one of the potential benefits of services such as ClearView AI and PimEyes is that they can help ensure accountability for war crimes by helping discover incriminating or vindicating evidence. However, actors wishing to frustrate the work of investigators can attempt to misuse the opt-out privacy features provided by services such as ClearView AI and PimEyes that allow people to exclude their faces from the search as means of privacy protection. For example, a concerned (present or future) war criminal can attempt to exclude their own face from searches to prevent the use of the face search engine to uncover the evidence of crimes. Such attempts can even be made by a third parties such as intelligence agencies who can exclude the faces of the agents, army soldiers, and other related operatives.

Second, belligerents can attempt to illegally obtain information that the search engine company has on an individual of importance in the conflict (e.g., soldiers, generals, political officials, etc.). The warring sides can achieve this by misusing the feature provided by, for example, ClearView AI service that allows a person to see the personal information that the company has about them on file. A person can only find out their own information and a headshot photo and a photo of the government ID is required. Actors operating on behalf of the belligerents can attempt to impersonate other individuals they wished removed by presenting headshot photos of the subject to be removed along with a stolen or forged government ID of the individual [13].

Third, parties who are barred from using a search engine service, can try to circumvent the restriction. For example, although the PimEyes service is reportedly not available to Russians due to the aggression, there is a concern that this tool might be used to find, capture, and kill people by Russian separatists in Ukraine, and other countries sympathetic to Russia. Furthermore, such parties can attempt to use the services by connecting through systems located in other countries where the use of the service is permitted.

The Issue of False Positives In addition to the issues associated with the deliberate deception or misuse of the face search engines, there are also concerns over the inherent propensity of the face matching algorithms used in the search to generate false positives–when a face of an individual is wrongly matched against the face of another. During the ongoing conflict, the consequences can include falsely accusing an individual of war crimes, treason, and other crimes that often carry severe penalties. Even more dangerous are the scenarios where misidentification can influence operations on the battlefield. For example, the Ukrainian side has been known for strategically taking out Russian generals and commanders. If a face search engine is used in the targeting process and incorrectly identifies another individual as a high-value target, it can result in military operations costing needless lives and destruction without achieving the military objectives.

War Strategy, Tactics, and Information Warfare It is possible that the use of services such as ClearView AI face search to identify the faces of perpetrators in the photos can help ensure accountability for war crimes. Furthermore, verification of faces of soldiers, politicians, and other key figures in photographs can be used as a tool to verify and counter misinformation and disinformation that have been frequently disseminated throughout this conflict. In addition, soldiers and civilians going missing is a common occurrence during the current conflict, and services such as ClearView AI can help scan the photos posted on, for example, media websites to identify the missing. Moreover, as previously discussed, Russia was forcefully relocating Ukrainians from the occupied areas to Russia. This includes children, which according to the UN may potentially qualify as genocide [69]. Face search engines can be used by family and investigators to find the forcefully relocated people including children, by searching for the faces of the missing in the photos posted by the deportees and those published in media.

The impacts of Ukraine's use of face search engines to identify fallen Russian soldiers and prisoners and to contact their families continues to be a subject of debate. Ukrainian experts believe that using such tactics would help erode Russia's public support for the war. Some military technology analysts, however, have cautioned that the Ukrainian tactics may backfire and cause anger from the same Russians they had hoped to persuade. Stephanie Hare, a surveillance researcher in London, for example, stated that the strategy of contacting the parents of the fallen Russian soldiers is dangerous and “classic psychological warfare” [21].

Impacts of Biometric Technologies other than Face Recognition

The Crisis and Support Centre of the Ministry for Europe and Foreign Affairs has donated a mobile DNA biometrics lab vehicle named mobil’DNA manufactured by the French company Deveryware. The lab was designed to conduct forensic investigations for identifying the dead victims of terrorism and natural disasters [32, 35]. The lab is shown in Figure 1.

Such technologies can play key roles in helping identify missing persons in Ukraine as disaster zones are created by the onslaught of Russian attacks on

Fig.1. mobil’DNA mobile DNA biometrics lab manufactured by the French company mobil’DNA lab was donated to Ukraine by Crisis and Support Centre of the Ministry for Europe and Foreign Affairs. Image copyrighted by Deveryware (image source [35]).cities, towns, and villages. Indeed, such capabilities to identify the bodies of missing persons may help find some of the over 9,000 persons who according to Stripes and Stars magazine have been reported missing since the invasion began in February 24, 2022 [72]. DNA identification can provide strong evidence linking the perished victims to war crimes. The connection can in turn be used for prosecuting crimes, designing future sanctions, and making tactical and strategic decisions on the battlefield.

In addition, DNA testing biometrics can help to fight human trafficking in Ukraine that has accompanied the ongoing crisis. We discuss this next.

Biometrics Against Human Trafficking

Biometric technologies can prove to be a promising weapon for combating the human trafficking practices that often accompany military conflicts such as the crisis in Ukraine. The United States Department of Justice defines human trafficking as “human trafficking, also known as trafficking in persons or modern-day slavery, is a crime that involves compelling or coercing a person to provide labor or services, or to engage in commercial sex acts” [75].

The war in Ukraine has raised concerns over trafficking physically, socially, mentally, or economically vulnerable individuals, especially women and children, who have lost their homes, employment, and support networks. Human trafficking was historically a serious problem in Ukraine before the crisis and the conflict can exacerbate it. The power of biometrics in identifying and verifying the identity of victims trafficked across Ukraine’s borders can prove to be a valuable weapon in combating trafficking practices during the ongoing conflict and beyond. The biometric technology is already available, and its deployment within Ukraine’s borders can prove to be a much-needed intervention.

Biometrics can detect the use of forged identities created by traffickers for victims being transported across the

Ukrainian borders (e.g., to Poland, Romania, and Belarus) and thus help rescue them. In addition, the robustness of biometric systems in establishing the identity of victims can also discourage perpetrators by complicating the identity forgery schemes that were traditionally based on forging the paper documents.

Emergent biometric technologies such as kinship tests can help to further fight the trafficking of children. For example, traffickers posing as parents carry children across borders. The new DNA biometric technologies can quickly and accurately verify whether the DNA samples taken from the parents and the child show a genetic parent-child link. We believe that future use of such technologies during the current Ukraine conflict and the years following the conflict's conclusion can form yet another important impediment to human trafficking. The privacy concerns associated with the DNA collection can be addressed by disposal of the DNA samples and any collected data once the kinship has been verified. Ukraine can also consider seeking help from the International Commission on Missing Persons (ICMP), which provides technical assistance to governments including identification of individuals based on DNA for the purpose of finding missing persons [63].

Conclusions

From influencing the lives of refugees to distribution of humanitarian aid, to affecting the outcomes of military, intelligence, and information warfare operations, the role of biometric technologies in the ongoing conflict is significant, complex, and at times controversial. The power of biometrics to seamlessly establish and verify the identity of a person can help secure the immigration process as asylum countries face a sudden influx of refugees; it can also help to ensure that humanitarian aid is dispensed to only those legally qualified. It also has a strong potential to identify and rescue victims of human trafficking which has been problematic in Ukraine historically and can be significantly exacerbated by the ongoing war.

Conversely, the power of biometric identification and verification is not absolute. Even the best-performing biometric technologies can either fail to identify/verify individuals or falsely match an individual to an identity that does not belong to them. Such mistakes can have significant impacts not just on the individual, who can for example can be accused of crimes they did not commit but can also affect the geopolitical situation in unpredictable and dangerous ways. The use of multiple biometrics and the growing accuracy and robustness of biometric technologies will likely help reduce these concerns. However, there are challenges facing countries like Ukraine in adapting state-of-the-art multimodal biometric systems. The government of Ukraine, for example, may conclude that investment in improving the biometric infrastructure is not the top priority of a nation fighting what they perceive to be a war for existence while dealing with serious economic crisis. The key solution is to educate the leadership of Ukraine's government and military leadership on the costs and benefits of biometric technologies and consider including biometric technologies in the aid packages sent to Ukraine.

Another recurring theme concerns long delays facing Ukrainian refugees at overwhelmed immigration offices to register biometrics required to receive asylum. However, the problem seems to be linked more to the operational aspects of immigration offices and not the biometric technology itself. Countries like Canada that have struggled with the problem of delays are working to address these problems by using mobile biometric technologies to create more biometric registration sites. We believe that proper adjustments and allocation of additional resources will help address these problems.

Another concern is the use of biometrics to track victims of war, especially the vulnerable Ukrainian citizens forcefully deported to Russia and critics of the war fleeing Russia out of fear of persecution. The evidence suggests that Russia is highly capable of conducting biometrics-based surveillance operations. This is evidenced by the public face recognition system currently deployed in Russia and the presence of Russian face search engines such as FindClone.

Similarly, while Ukrainian tacticians believe that Ukraine's use of face recognition search engines to identify faces slain and captured Russian soldiers and notifying the solders' families can help turn the Russian public opinion against the war, some surveillance experts believe the tactic can have an opposite effect. Although the true impacts of such tactics may become clearer as the conflict evolves, it is possible for the impacts to be mixed. Some families may turn to opposing the war after seeing the death or capture of a family member, and some may react with anger and resentment that can translate into hardened support for the war. Analysis of such tactics can prove a ripe area of study for psychologists and sociologists. The results they deliver may lead to better understanding of yet another impact of how biometrics affects this and future conflicts.

As the conflict continues, the role of biometric technologies will likely evolve with it. We expect novel applications of biometrics in border security, military, and humanitarian applications. These new roles taken on by biometrics will likely help solve existing problems but also face challenges and controversies as we have seen in current uses of biometrics. Regardless of how the Russia-Ukraine conflict progresses, the uses of biometrics by both sides have underscored that biometrics possess a critical capability during times of war–the power to establish and verify a person's identity. It helps answer critical questions such as "who are you?", "are you friend or enemy?", "is anyone looking for you?", and "who are your relatives?". This power can become an important determining factor that can decide the conflict's outcome and its aftermath.

Therefore, it is important for the research community to continue monitoring and analyzing the use of biometrics throughout conflict. The insights of such work can help deepen the understanding the nature of modern warfare.

References

[1] Deutsche Welle (www.dw.com). Fact check: The deepfakes in the Disinformation War between Russia and Ukraine: DW: 18.03.2022. url: https:// www.dw.com/en/fact-check-the-deepfakes-in-the-disinformationwar-between-russia-and-ukraine/a-61166433.

[2] About Pimeyes. url: https://pimeyes.com/en/about.

[3] Jasmine Aguilera. Ukrainian refugees in U.S. face long term challenges. Apr. 2022. url: https://time.com/6170334/ukrainian-refugeesbiden-program/.

[4] Polina Nikolskaya Andrew Osborn. Russia's Putin authorises 'special military operation' against Ukraine. Feb. 2022. url: https://www.reuters. com/world/europe/russias-putin-authorises-military-

operationsdonbass-domestic-media-2022-02-24/.

[5] Besart. EU approves visa-free travel for Ukrainians. Dec. 2018. url: https://www.schengenvisainfo.com/news/eu-approves-visa-free-travelukrainians/.

[6] Mia Bloom and Kristian Kastner Warpinski. Children in violent movements: From child soldiers to terrorist groups. Mar. 2021. url: https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-602.

[7] Daniel Bush and Alex Saheer. Bing’s top search results contain an alarming amount of disinformation. Dec. 2019. url: https://cyber.fsi. stanford.edu/io/news/bing-search-disinformation.

[8] Tyler Choi. Biometrics cause ’bottleneck’ for Ukrainians fleeing to Canada, ease France arrivals: Biometric update. Mar. 2022. url: https://www. biometricupdate.com/202203/biometrics-cause-bottleneck-forukrainians-fleeing-to-canada-ease-france-arrivals.

[9] Tyler Choi. Biometrics cause ’bottleneck’ for Ukrainians fleeing to Canada, ease France arrivals: Biometric update. Mar. 2022. url: https://www. biometricupdate.com/202203/biometrics-cause-bottleneck-forukrainians-fleeing-to-canada-ease-france-arrivals.

[10] Tyler Choi. Biometrics secure UNHCR direct cash payments to Ukrainian refugees: Biometric Update. Apr. 2022. url: https://www.biometricupdate. com/202204/biometrics-secure-unhcr-direct-cash-payments-toukrainian-refugees.

[11] Tyler Choi. Mobile biometric kits deployed to Europe for Ukrainian refugee registration by Canada: Biometric Update. Mar. 2022. url: https://www. biometricupdate.com/202203/mobile-biometric-kits-deployedto-europe-for-ukrainian-refugee-registration-by-canada.

[12] James Clayton. How facial recognition is identifying the dead in Ukraine.Apr. 2022. url: https://www.bbc.com/news/technology-61055319.

[13] Clear View Privacy policy. url: https://www.clearview.ai/privacypolicy.

[14] Cover your face: Facial recognition, legal protection, disease prevention mash-up. July 2020. url: https://whatsyourtech.ca/2020/07/22/ cover-your-face-facial-recognition-legal-protection-diseaseprevention-mash-up/.

[15] Robyn Dixon. Russia’s surveillance state still doesn’t match China. but Putin is racing to catch up. Apr. 2021. url: https://www.washingtonpost. com/world/europe/russia-facial-recognition-surveillancenavalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac_ story.html.

[16] Lynn Duke. Family who opened up their home to Ukrainian refugees touched by welcome boxes. June 2022. url: https://www.dailyrecord.co.uk/ news/local-news/perthshire-family-who-opened-up-27211032.

[17] Mustafa Ekrem Erakın, U˘gur Demir, and Hazım Kemal Ekenel. “On Recognizing Occluded Faces in the Wild”. In: 2021 International Conference of the Biometrics Special Interest Group (BIOSIG). 2021, pp. 1–5. doi:10.1109/BIOSIG52210.2021.9548293.

[18] Cristina Gallardo. UK expands visa scheme for Ukrainian refugees amid criticism. Mar. 2022. url: https://www.politico.eu/article/ukexpands-scope-of-visa-scheme-for-ukrainian-refugees/.

[19] Generation ISIS: When children are taught to be terrorists. Oct. 2017. url: https://www.nbcnews.com/storyline/isis-uncovered/generationisis-when-children-are-taught-be-

terrorists-n812201.

[20] Drew Harwell. Ukraine is scanning faces of Dead Russians, then contacting the Mothers. Apr. 2022. url: https://www.washingtonpost.com/ technology/2022/04/15/ukraine-facial-recognition-warfare/.

[21] Drew Harwell. Ukraine is scanning faces of Dead Russians, then contacting the Mothers. 15AD. url: https://www.msn.com/en-us/news/world/ ukraine-is-scanning-faces-of-dead-russians-then-contactingthe-mothers/ar-AAWfxx8.

[22] How cash assistance is helping refugees from Ukraine. url: https://www. unrefugees.org/news/how-cash-assistance-is-helping-refugeesfrom-ukraine/.

[23] How Russia is using facial recognition to police its coronavirus lockdown. Apr. 2020. url: https://abcnews.go.com/International/russiafacial-recognition-police-coronavirus-lockdown/story?id= 70299736.

[24] How the Home Office’s Immigration Technology Department reduced its cloud costs by 40 Percent. Dec. 2019. url: https://www.gov.uk/ government/case-studies/how-the-home-offices-immigrationtechnology-department-reduced-its-cloud-costs-by-40.

[25] Jacqueline Howard. Ukrainians seeking shelter in US must have TB screenings and certain vaccinations. May 2022. url: https://edition.cnn. com/2022/05/19/health/ukraine-vaccines-tuberculosis-screening/ index.html.

[26] ICAO Doc 9303 Machine Readable Travel Documents. url: https://www. icao.int/publications/pages/publication.aspx?docnum=9303.

[27] Refugees Immigration and Citizenship Canada. Government of Canada. June 2022. url: https://www.canada.ca/en/immigration-refugeescitizenship/services/immigrate-canada/ukraine-measures/keyfigures.html.

[28] Refugees Immigration and Citizenship Canada. Government of Canada. Apr. 2022. url: https://www.canada.ca/en/immigration-refugeescitizenship/services/immigrate-canada/ukraine-measures/biometrics.html.

[29] Iris scanning understanding biometric iris recognition technology. url: https://www.biometric-security-devices.com/iris-scanning. html.

[30] Zolan Kanno-youngs. Ice meant to capture drug lords. did it snare duped seniors? June 2021. url: https://www.nytimes.com/2021/06/06/us/ politics/older-americans-drug-trafficking.html.

[31] Ayang Macdonald. Russian pols OK Bill to make banks share client biometrics with government: Biometric Update. July 2022. url: https:// www.biometricupdate.com/202207/russian-pols-ok-bill-to-makebanks-share-client-biometrics-with-government.

[32] Ayang Macdonald. Ukraine gets mobile DNA biometrics lab from France toId war dead: Biometric update. July 2022. url: https://www.biometricupdate. com/202207/ukraine-gets-mobile-dna-biometrics-lab-fromfrance-to-id-war-dead.

[33] Ayang Macdonald. Ukrainian refugee crisis spotlights biometric data collection process challenges: Biometric Update. Apr. 2022. url: https://www.biometricupdate.com/202204/ukrainian-refugee-crisisspotlights-biometric-data-collection-process-challenges.

[34] Amy Mackinnon. Russia’s surveillance state struggles to wean itself off the West. May 2021. url: https://foreignpolicy.com/2021/05/24/russia-surveillance-technology-western-companies-

facialrecognition/.

[35] Magali. France provides Ukraine with a mobil’DNA. July 2022. url: https://deveryware.com/france-provides-ukraine-with-a-mobildna/?lang=en.

[36] Alessandro Mascellino. UK scraps pre-arrival biometric checks for Ukrainian refugees: Biometric Update. Mar. 2022. url: https://www.biometricupdate. com/202203/uk-scraps-pre-arrival-biometric-checks-forukrainian-refugees.

[37] 2022 May 31. Pimeyes: Biometric update. June 2022. url: https://www. biometricupdate.com/companies/pimeyes.

[38] Stephen Mayhew. Russian startup Tops UW Facial Recognition Challenge: Biometric update. Dec. 2015. url: https://www.biometricupdate.com/201512/russian-startup-tops-uw-facial-recognition-challenge.

[39] Stephanie Miskin. Refugees say expats make coventry ’like a little Ukraine’. June 2022. url: https://www.bbc.com/news/uk-england-coventrywarwickshire-61706132.

[40] Stephanie Miskin. Refugees say expats make coventry ’like a little Ukraine’. June 2022. url: https://www.bbc.co.uk/news/uk-england-coventrywarwickshire-61706132?at_medium=RSS%5C&amp;at%5C_campaign= KARANGA.

[41] Moscow silently expands surveillance of citizens. Oct. 2021. url: https://www.hrw.org/news/2020/03/25/moscow-silently-expandssurveillance-citizens.

[42] Jim Nash. Face-scrapers say they won’t help Russia in Ukraine, but ...: Biometric update. June 2022. url: https://www.biometricupdate.com/202204/face-scrapers-say-they-wont-help-russia-in-ukrainebut.

[43] Jim Nash. Russia tries to revive twice-bumped biometric surveillance net, put it near Ukraine: Biometric update. June 2022. url: https://www. biometricupdate.com/202206/russia-tries-to-revive-twicebumped-biometric-surveillance-net-put-it-near-ukraine.

[44] Operational Data Portal. url: https://data.unhcr.org/en/situations/ ukraine.

[45] Passport Services in Ukraine - issue a biometric foreign passport. Jan.2020. url: https://businessvisit.com.ua/en/internationalpassport/.

[46] Person and Jeffrey Dastin Paresh Dave. Exclusive: Ukraine has started using Clearview Ai’s facial recognition during war. Mar. 2022. url: https://www.reuters.com/technology/exclusive-ukraine-has-startedusing-clearview-ais-facial-recognition-during-war-2022-0313/.

[47] Person and Jeffrey Dastin Paresh Dave. Exclusive: Ukraine has started using Clearview Ai’s facial recognition during war. Mar. 2022. url: https://www.reuters.com/technology/exclusive-ukraine-has-startedusing-clearview-ais-facial-recognition-during-war-2022-0313/.

[48] Nataniel Ruiz, Sarah Adel Bargal, and Stan Sclaroff. Disrupting deepfakes: Adversarial attacks against conditional image translation networks and facial manipulation systems. Apr. 2020. url: https://doi.org/10.48550/ arxiv.2003.01279.

[49] Russia distributes its passports among forcibly deported Ukrainians ... url: https://euromaidanpress.com/2022/04/12/russia-distributesits-passports-among-forcibly-deported-ukrainians-ombudswoman/.

[50] Russia is using facial recognition technology to fight against coronavirus. url: https://www.educationaltechs.com/2020/05/russia-isusing-facial-recognition.html.

[52] Russia’s use of facial recognition challenged in court. Jan. 2020. url:

https://www.bbc.com/news/technology-51324841.

[53] Schengen area - visa information for Schengen countries. June 2022. url: https://www.schengenvisainfo.com/schengen-visa-countrieslist/.

[54] Government Digital Service. Universal credit. Nov. 2014. url: https:// www.gov.uk/universal-credit.

[55] Sh.januzi. About 30,000 Ukrainian refugees have arrived in France until Last Sunday. Mar. 2022. url: https://www.schengenvisainfo.com/ news/about-30000-ukrainian-refugees-have-arrived-in-franceuntil-last-sunday/.

[56] ShareAmerica. Putin's latest crackdown on dissent and information. July 2022. url: https://share.america.gov/putins-latest-crackdownon-dissent-and-information/.

[57] Amy Simon. Belmont, ont. resident describes visa delays in bringing family home from Ukraine - london. June 2022. url: https://globalnews.ca/ news/8885789/belmont-ont-resident-ukrainian-family-visadelays/.

[58] Tom Simonite. Online sleuths are using face recognition to ID Russian soldiers. Mar. 2022. url: https://www.wired.com/story/facialrecognition-identify-russian-soldiers/.

[59] Tom Simonite. Online sleuths are using face recognition to ID Russian soldiers. Mar. 2022. url: https://www.wired.com/story/facialrecognition-identify-russian-soldiers/.

[60] Smugglers sentenced; elderly pair get 5 years each in heroin case. Feb. 1957. url: https://www.nytimes.com/1957/02/09/archives/smugglerssentenced-elderly-pair-get-5-years-each-in-heroin-case.html.

[61] The Foreign Desk Staff and The Foreign Desk Staff. Ukraine probes deportation of kids to Russia as possible genocide. url: https://justthenews. com/world/foreign-desk/ukraine-probes-deportation-childrenrussia-possible-genocide.

[62] OSINT Tactical. 1/15 OSINT: Open Source Intelligence Investigation &amp; the use of facial recognition. trigger to the investigation: Russian propaganda military video posted on telegram by what seems to be a Chechen Muslim fighter. #ukraine #islamicfighters #chechen #osint #telegram #facialrec pic.twitter.com/ualpolsqo3. Mar. 2022. url: https://twitter. com/OSINT%5C_Tactical/status/1498694266754899978.

[63] Technical assistance. Oct. 2022. url: https://www.icmp.int/what-wedo/technical-assistance/.

[64] Current Time. Dozens arrested in Moscow via facial-recognition system on Russia Day. June 2022. url: https://www.rferl.org/a/moscowpolice-detain-dozens-using-facial-recognition-system/31896070. html.

[65] Anton Troianovskinew York Times. In Putin's Russia, arrests spreading widely and quickly. July 2022. url: https://buffalonews.com/inputins-russia-arrests-spreading-widely-and-quickly/article_ 45e7ca89-0e8d-5eda-aaa8-e67e7c2a0cba.html.

[66] Ukraine crisis. url: https://www.britannica.com/topic/Ukrainecrisis.

[67] Ukraine schemes: Visas and Biometrics. June 2022. url: https://www. nidirect.gov.uk/articles/ukraine-schemes-visas-and-biometrics# toc-1.

[68] Ukrainian family finds war relief in prince George. url: https://www. princegeorgecitizen.com/local-news/ukrainian-family-findswar-relief-in-prince-george-5463442.

[69] United Nations Office on Genocide Prevention and the responsibility to protect. url: https://www.un.org/en/genocideprevention/genocide.shtml.

[70] Uniting for Ukraine. url: https://www.dhs.gov/ukraine.

[71] Uniting for ukraine: How many refugees and U.S. sponsors are there? url: https://www.msn.com/en-us/news/world/uniting-for-ukrainehow-many-refugees-and-us-sponsors-are-there/ar-AAY9eZB.

[72] Paulina Villegas and Reis Thebault. Hundreds of civilians missing, taken or simply gone: The untold toll of the Ukraine war. June 2022. url: https://www.stripes.com/theaters/europe/2022-06-19/ukraine-warcivilians-missing-gone-6394492.html.

[73] VK. url: https://vk.com.

[74] Adam Vrankulj. Ukranian president signs biometric e-passport law: Biometric update. Nov. 2012. url: https://www.biometricupdate.com/201211/ukraine-president-signs-biometric-e-passport-law.

[75] What is human trafficking? Oct. 2020. url: https://www.justice.gov/ humantrafficking/what-is-human-trafficking.

[76] What is the biometric passport in Ukraine - Jur Klee. url: https:// jurklee.ua/en/blog/chto-takoe-biometricheskij-pasport/.

[77] Which European countries are opening their doors to Ukrainians? Mar. url: https://www.euronews.com/travel/2022/03/01/whichcountries-have-relaxed-entry-and-visa-requirements-forukrainian-nationals.

[78] Приняты поправки об&nbsp;ответственности за фейки о работе госорганов РФ за рубежом. Государственная Дума. Mar. 2022. url: http://duma.gov.ru/news/53773/

Author Information

Mikhail I. Gofman

https://orcid.org/0000-0002-7340-647X

California State University

Fullerton

United States

Contact e-mail: *mgofman@fullerton.edu*

Maria Villa

https://orcid.org/0000-0001-5610-4667

California State University

Fullerton

United States