Report

G | M | F

IDEAS LEADERSHIP HOPE

Advanced Technologies in the War in Ukraine

Risks for Democracy and Human Rights

Anna Mysyshyn
ReThink.CEE Fellowship

October 2024

Table of Contents

Summary

Ukraine's use of advanced technologies has been invaluable in defending itself against Russia's invasion, but these also present significant risks to democracy and human rights in the country.

Satellite-based remote-sensing technology helps document war crimes and provide real-time battlefield intelligence. It has exposed atrocities and tracked armed groups, and it will be vital for reconstruction. Companies have provided satellite imagery essential for holding Russia accountable and assessing infrastructure damage. However, the use of satellite imagery poses risks of, for example, data manipulation, privacy violations, and misuse by governments or private entities. In Ukraine, the lack of standardized practices and updated legislation exacerbates these risks. Unauthorized access or tampering with imagery can distort facts, while broad data collection by satellites raises concerns about who controls the information. The involvement of Palantir Technologies and the use of the Delta system in Ukraine's defense also has the potential to affect democracy and human rights. Using Palantir's advanced data-mining tools raises concerns about misuse and privacy violations. The company having confidential agreements with the government underscores the need for ethical use and strict adherence to privacy laws. Using the satellite-based Delta situational awareness system enhances battlefield decision-making, but it also carries risks related to data breaches, system failures, and lack of transparency. Without proper oversight, its use could lead to over-surveillance and privacy violations.

The use of facial recognition technology, notably from Clearview AI, in the war has been transformative but also raises serious ethical concerns. While it aids in identifying Russian soldiers and missing persons, it also has potential for mass surveillance, misidentification, and privacy violations. Its unregulated use threatens fundamental rights, and Clearview AI has faced legal actions in different countries for breaching data-protection laws. These concerns are heightened by the technology's possible continued use after the war. Russia's use of AI in information warfare has intensified the conflict, with AI-generated disinformation, deepfakes, and voice cloning spreading false narratives and destabilizing Ukrainian society. Deepfake videos, such as those depicting Ukrainian leaders surrendering, are used to erode trust in media and pose significant threats to social cohesion and democracy.

As Ukraine increasingly relies on these technologies in the war, the needs to withhold sensitive information and to maintain public trust conflict. Striking a balance between national security and human rights is essential. International law allows for limited derogations from human rights during emergencies, but these must adhere to the principles of necessity and proportionality.

These crucial technologies require stringent safeguards to protect democratic values and human rights in Ukraine. Key recommendations to do so include regulating remote-sensing technologies; harmonizing the country's AI and data-protection laws with EU standards; adopting impact assessment frameworks; creating "regulatory sandboxes" for the safe development, testing, and adaptation of AI innovations; and enhancing media literacy programs to counter AI-generated disinformation. Through these measures, Ukraine can harness advanced technologies for defense and reconstruction while ensuring that wartime measures do not undermine its democratic future.

Introduction

New advanced technologies are profoundly changing modern warfare. The war in Ukraine illustrates this with the use of tools such as satellite-enabled remote sensing, situational-awareness systems and drones, facial-recognition technology, and artificial intelligence (AI). The combination of traditional and technological warfare provides new opportunities, but it also creates challenges at the intersection of ethics, law, and democracy.

Russia's full-scale invasion in February 2022 led to Ukraine undergoing defense-technological progress that helps it fight against the enemy but also carries risks for society. The government's collaboration with technology companies shows the deep integration of the defense and digital spheres. However, with technological progress comes political dilemmas such as over AI making autonomous decisions in wartime, protecting citizens from the misuse of facial-recognition tools and of surveillance by satellite technology, and the danger of information warfare.

In this context, there is an urgent need for Ukraine to rethink its legal, regulatory, and policy framework. This is essential to strike a balance between strategic benefits and ethical imperatives concerning democracy and human rights. A framework crafted in the pre-digital era is inadequate for tackling the challenges of today's technologically advanced landscape. To address this, it is critical to examine not only the impact of technologies but also to the role of specific companies and initiatives that have emerged in Ukraine during the war. A comprehensive approach is essential for developing strategies that are responsive to the complexities introduced by digital advances and effective.

This paper delves into the effects of emerging advanced technologies on human rights and democracy in the war in Ukraine, alongside examining the contributions of key companies and initiatives. It first looks at the situation before the full-scale invasion by Russia in February 2022 and then focuses on three key technologies: remote sensing, facial recognition, and AI. The paper then considers the importance for Ukraine of harmonizing its legislation with EU standards and the need to address the question of proportionality in balancing technology and human rights. It concludes with recommendations for regulatory and ethical frameworks for the advanced technologies currently used for war purposes, and for combatting AI-generated disinformation and propaganda.

The State of Play in February 2022

Ukraine began to move into a state of technological warfare in 2014 following Russia's illegal annexation of Crimea and military intervention in eastern parts of the country, relying largely on volunteers and private initiatives. Many new software appeared. Yaroslav Sherstyuk, an officer in the 55th Separate Artillery Brigade, had already digitized artillery calculations the previous year, laying the foundation for the Ukrop mobile app.[1] There was an urgent need for up-to-date maps and the volunteer group Army SOS provided offline maps on tablets, which later gave rise to the Kropyva app, an integrated artillery-management system. The system now coordinates artillery reconnaissance, command, and firing operations through sophisticated calculation software.

The many military applications that volunteers developed range from ballistic calculators to terrain-detection systems, secure communications apps, and the demobilization timer Dzhura. Some of these have expanded their functionality while others have fallen by the wayside. Certain software, such as Kropyva and GIS Arta have evolved into comprehensive troop-management systems that are now available on Android devices in various military units. These military software innovations have proven themselves to be not inferior to more expensive Western equivalents.

Some tools have come about through cooperation between volunteers and the state, such as the Delta situational-awareness system, which was initiated by volunteers who formed the civil society organization Aerorozvidka ("aerial reconnaissance" in Ukrainian) in 2015 and was later adopted by the Armed Forces of Ukraine (AFU).[2] A web-based service, Delta synthesizes information from various sources, from satellites to ground informants, to provide a comprehensive overview of the battlefield. It has proved its effectiveness in international exercises and in combat situations. By February 2023, use of system was extended to the border guard, the police, and the National Guard.[3]

The landscape of satellite surveillance was largely shaped by the interplay between evolving technological capabilities and the participation of specific companies until 2022. During Russia's annexation of Crimea in 2014 and subsequent invasion of eastern Ukraine, satellite surveillance was predominantly the domain of state-owned systems that offered limited public access to their data, due to its classified nature. However, the rapid development of the private satellite industry has begun to change this dynamic. Companies such as Maxar Technologies, Planet Labs, and Capella Space have become key players, bringing advances in satellite-imaging technology and democratizing access to high-resolution imagery.

Since 2014, the latest in satellite imagery—which, for example, can see through clouds—has played a significant role in documenting and analyzing the situation on the ground. The images obtained have provided important information on troop movements, artillery deployments, and infrastructure destruction, enabling a clearer picture of the war's dynamics.[4] Ukraine's intelligence service has used satellite imagery to make decisions at the operational and tactical levels. For example, in December 2021, images from Maxar Technologies showed the world the concentration of hundreds of Russian tanks and fighter jets near the border. So, even before the full-scale invasion, the AFU had an idea of where Russia's main forces were concentrated.

In Ukraine, satellite imagery is widely used by international organizations and independent investigative organizations. For example, Bellingcat, the investigative journalism network that uses open-source intelligence, has made extensive use of satellite imagery to document and analyze the armed conflict. This notably included the case of the downing of Malaysia Airlines Flight MH17 in July 2014, when Bellingcat found that Russia has falsified satellite imagery to pretend that a Ukrainian fighter jet was near the passenger aircraft at the time.

Such findings have demonstrated the ease with which satellite imagery can be altered to fit certain narratives and highlight the critical importance of verification by organizations to ensure the integrity of open-source intelligence. The use of satellite imagery as evidence in this case highlights the importance of such technologies in the pursuit of justice.

Remote-Sensing Technology

Since the beginning of Russia's full-scale invasion of Ukraine in 2022, remote-sensing technology has been an important tool in the war. It has played a key role in documenting war crimes and atrocities committed by Russian forces as well as in providing real-time information for situational awareness.[5] It is inextricably linked to satellites, as platforms on which remote-sensing devices are deployed and which facilitate data collection by observing large, often inaccessible areas. Satellite-based instruments include sensors designed to measure different types of physical or chemical properties. The data collected is then interpreted using various techniques, with sophisticated software often used to visualize and analyze it, allowing researchers to identify patterns, trends, and anomalies.

The use of remote sensing, in particular satellite imagery, provides invaluable information about events that may have occurred in places to which access is restricted due to war, environmental hazards, or governmental restrictions. It can produce evidence of mass graves, destroyed villages, and other signs of war crimes.[6] It can also help track the movements of armed groups, the displacement of populations, human smuggling, or the destruction of buildings or other infrastructure.

Satellite remote sensing can provide evidence of crimes such as forced migration or genocide, which can be crucial in the investigation and prosecution of criminals, complementing traditional investigative methods.

For example, Russia disputed the authenticity of photographs showing dead civilians on the streets of the city of Bucha, and it claimed that the horrific events had occurred not during the Russian occupation in the first weeks of the war but after its troops had left the area, shifting the blame to what it called "Ukrainian radicals".[7] However, careful examination of video evidence and satellite imagery refuted this. Satellite imagery from Maxar Technologies confirmed the timeline of events that several civilians were killed during the Russian occupation of Bucha.

In another case, Russia tried to blame shelling by Ukraine's forces for the death of Ukrainian prisoners of war it held in a barrack in the occupied village of Olenivka in July 2022. According to the Security Service of Ukraine, the explosion was a deliberate act of the Russian occupiers. Satellite images from Maxar Technologies of the prison camp in Olenivka, taken before and after the event, provided crucial evidence of atrocities against Ukrainian prisoners. Analyzing these images, the forensic team of the General Prosecutor's Office in Ukraine identified the unmistakable signs of an explosion.[8] While the satellite images captured were still photos rather than video footage, they strongly suggest the possible involvement of the Russian private military company Wagner in the execution of the detainees.

Importantly, all such satellite images have been carefully collected, analyzed, and preserved by national and international organizations that intend to present them as evidence of Russian war crimes. The Ukrainian case is groundbreaking because it relies heavily on satellite imagery that is likely to influence future proceedings in international and Ukrainian courts. Such extensive use of satellite data could lead to significant changes in the methodology of evidence in international courts.

Moreover, satellite remote sensing will be extremely necessary and helpful for the postwar reconstruction of Ukraine. The cost of the destruction is already estimated at $108.3 billion,[9] and the amount of indirect economic losses at $750 billion—a scale of destruction and losses unseen since the Second World War.[10] To restore the country after the war and to integrate its economy into the European space and global value chains, Ukraine needs to implement a massive recovery program. For example, the UADamage project is digitizing satellite and drone imagery to identify damage, assess losses, and plan reconstruction projects. There are also private volunteer initiatives for damage assessment that use elements of satellite imagery and machine-learning technologies.[11]

The latest Delta technology uses data from satellites. The situational-awareness system is interoperable with similar NATO systems and resembles a game in which data is collected in real time. Delta integrates inputs from providers of satellite imagery, radar data, sensors, GPS trackers, and systems such as eVorog chatbots and STOP Russian War that allow ordinary Ukrainians to report the movements of enemy vehicles and troops (although these systems are controversial in terms of data security as they are based on the Telegram platform). AI is already integrated in Delta's system. Data collected by drones using onboard sensors or data received from satellites is fed into specialized AI algorithms designed to identify and interpret key elements in the data, including recognizing different types of equipment and identifying people. The results of this AI analysis are projected onto a digital map, providing a comprehensive interactive view of a scanned area and any notable objects or subjects identified. This integrated system of drone surveillance, AI data processing, and visual map display is a sophisticated tool for real-time analysis and decision-making.

Global tech giants known for their advanced data analytics and integration capabilities are also entering the fray.

Global tech giants known for their advanced data analytics and integration capabilities are also entering the fray, signaling a shift toward more comprehensive, collaborative defense solutions. The partnership between the American company Palantir Technologies and the Ministry of Digital Transformation of Ukraine highlights the deep integration of the defense and digital realms.[12] It combines strategic defense objectives and advanced technological capabilities.

Palantir's MetaConstellation platform is of key importance for Ukraine's defense. It allows users to task satellites to capture images of specific locations in real time. Using algorithms, the system filters huge amounts of data, ensuring that only relevant images are downloaded, thereby facilitating fast and efficient decision-making on the battlefield.[13] With this technology, Ukraine can accurately track and hit enemy targets, such as command centers or ammunition depots, with unprecedented speed. The system also optimizes the target coordination cycle as processes that once took hours now take a few minutes.[14] Palantir's software, which combines signal intelligence with satellite imagery, makes the task of collating huge amounts of data and making strategic decisions in real time not only feasible but also highly effective for Ukraine.

The Ministry of Economy and Palantir have signed an agreement so that, after the war, the company's software will be used to consolidate multiple data streams to help demine Ukraine, which is now the most heavily mined country in the world, with mines threatening more than 6 million civilians and rendering large areas of agricultural

land unusable.[15] The software will help identify the areas where demining would have the most impact, with the goal of returning 80% of mined land to economic use within a decade.[16]

Possible Threats to Democracy and Human Rights

Satellite imagery from private companies such as Maxar Technologies, Planet Labs, and Capella Space is playing a key role in holding Russia accountable for its actions and aiding Ukraine's reconstruction efforts by showing the true extent of damage to the country's infrastructure. However, this technology can also pose threats to Ukraine's democracy.

Satellite imagery must meet certain standards of acceptability. This means that the images have not been tampered with and that their collection and safe storage have been carried out in accordance with established protocols set by recognized authorities such as international standards organizations, government agencies, industry consortia, or regulatory bodies. Satellite imagery can be manipulated or distorted, with governments, private companies, hackers, terrorist organizations, and other entities possessing the capability to exploit it for their agenda. This can involve altering or fabricating features within the images by using advanced image-processing software, which can be virtually undetectable to the untrained eye. Additionally, insecure data storage or transmission can result in unauthorized access, enabling the modification or misuse of the imagery before it reaches the intended users. Even genuine images can be taken out of context or interpreted in a biased way, leading to false narratives or accusations. This is currently a significant problem in Ukraine due to the lack of standardized practices and updated legislation. Furthermore, the collection of information by satellite-communication technologies is very broad and not focused only on areas of hostilities. Satellite images provide location information about civilian objects and persons, which is then processed by private and public companies and transmitted to third parties. The main question is who controls the satellites and has access to their data. If access is limited to a few influential organizations, this can lead to information imbalance and potential abuse. In the context of Ukraine, where the stakes are high in terms of accountability, reconstruction, and geopolitical stability, vigilance in addressing these concerns is paramount. Therefore, ensuring the integrity of satellite imagery involves not only technical safeguards but also regulatory oversight, transparency, and accountability measures to prevent misuse and abuse by various actors.

Given their prominence in Ukraine's wartime situation, the role of Palantir Technologies and Delta deserves close inspection, as the implications for democracy and human rights from their systems and involvement are significant. The key distinction between them is that the risks are related to the nature and operations of the company when it comes to Palantir, while those associated with Delta are related to how effectively the system is designed, managed, and secured.

Founded in 2003, Palantir brings advanced data integration and analytics technologies primarily in the fields of national security, military strategy, and law enforcement. The company has faced scrutiny for its significant government contracts, including those with the US Department of Defense, particularly due to the support of Peter Thiel, one of its founders, for Donald Trump. Concerns about Palantir's role in undermining democratic principles grew during Trump's presidency, especially given its controversial partnership with the US Immigration

and Customs Enforcement in identifying and deporting illegal immigrants as part of the administration's stringent immigration policies.

The involvement of Palantir in the war in Ukraine raises concerns about how its powerful data-mining tools could be used and whether they could be targeted at specific groups or individuals, potentially violating civil liberties. The use and reach of Palantir's technology depend heavily on the specific agreements the company has with the government and on where the concerned data is stored and processed—both of which crucially influence who has access to the data. While the general nature of these agreements is known to involve data analytics and security services, many specifics are kept confidential due to national security and proprietary reasons. Furthermore, regardless of these conditions, it is imperative that Palantir uses its powerful capabilities ethically and responsibly, ensuring that its actions are governed by stringent adherence to Ukraine's human rights and privacy laws to prevent any abuse or misuse that could harm individuals or groups. Thus, while Palantir's technology provides clear security and intelligence benefits for Ukraine, its application warrants careful consideration to safeguard democratic principles.

In contrast, the risks associated with Delta are not tied to the nature of an entity but systemic and technical, similar to what could arise in the case of any comparable platform. These risks include potential data breaches, system failures, or inefficiencies that could impact user experience or security. With regard to Delta, adhering to accountability and transparency standards is of crucial importance. In a high-stakes wartime environment, decisions based on surveillance data can have far-reaching consequences, but the processes and criteria for making these decisions can be opaque. Without clear mechanisms for oversight and public understanding of the system, it becomes difficult to ensure that it is used ethically and responsibly. Lack of transparency can lead to its abuse or misuse. Furthermore, as with other mass-surveillance technologies, there is a risk of over-surveillance that may violate privacy rights. The heightened need for security may overshadow the importance of protecting human rights and upholding democratic principles.

Facial Recognition Technology

The use of facial recognition technology (FRT) in the war in Ukraine is a groundbreaking example of the application of such technology in a warfare environment. While the technology has transformative potential, it is crucial to address its ethical implications to avoid potential human rights pitfalls.

FRT refers to biometric systems that automatically detect and record a person's face, making it possible to identify or otherwise recognize a person from these digital images. There are several ways in which this technology can be used to identify individuals. One is to use biometric data, such as measuring the distance between different points on the face, the shape of the eyes, and the width of the nose. Another way is by analyzing facial characteristics such as the shape of the chin or the position of the eyes and the mouth.

Real-time FRT is often deployed in a similar way to traditional video surveillance but differs from it in key ways. It can continuously scan, identify, and potentially track all individuals within its range in real time, unlike video surveillance, which might be limited to tracking and identifying specific individuals.[17] Moreover, the collection of biometric data through FRT introduces a new level of privacy concerns. This data is unique to each individual and can be used for purposes beyond identification, including profiling or tracking movements across different locations, making FRT far more intrusive. The biometric data that FRT gathers and stores not only can be used to identify a person based on their physical or behavioral characteristics, but also is more permanent and difficult to change than other personal information. They can be used to uniquely identify a person in different situations and over extended periods, as well as to determine characteristics such as their age, gender, and ethnicity. Individuals have no control over how their biometric data is used, stored, or shared, which raises significant ethical and legal concerns, particularly in terms of consent and data protection.

Different jurisdictions have begun to address this. For instance, in 2020, the Court of Appeal in the United Kingdom ruled that facial biometrics are "intrinsically private" and comparable to fingerprints and DNA regarding their sensitivity.[18] The EU's General Data Protection Regulation (GDPR) classifies biometric data as sensitive and requires explicit consent for its collection, processing, and use. In the United States, laws like the state of Illinois' Biometric Information Privacy Act require consent for biometric data use and provide legal recourse for mishandling, setting a precedent that other states are beginning to follow.[19] In Canada, the Office of the Privacy Commissioner has called for clear legal standards to protect such information.[20]

In the run-up to the Russian invasion, Ukraine's government and its allies extensively used open-source intelligence. This helped detect Russian military movements along the border, despite Moscow's denial of having aggressive intentions. This relied heavily on satellite imagery, some of which was purchased from private companies, as well as on videos and photos on social media platforms such as TikTok. The invasion was followed by further intelligence activities that combined biometric data and social media intelligence to identify Russian agents and victims on both sides of the war.

The government of Ukraine has used Clearview AI since March 2022 to gather evidence of war crimes, to identify Russian criminals, and at checkpoints.[21] The company has granted Ukraine free access to its software, which identifies people by images that have been previously extracted from online social networks such as Facebook, Twitter, and Vkontakte, and search engines such as Google. To identify a person, their photo must be uploaded to the company's biometric database, and the algorithm will find a match. The database contains about 30 billion images, and Clearview AI often sells this data to different authorities, mainly law-enforcement agencies.[22]

Clearview AI's technology can help to reunite refugees with their families, to identify war victims, and to show and debunk Russian propaganda about the war.[23] It has also helped to expose Russian undercover agents in Ukraine, to identify Russian soldiers involved in war crimes, and to identify dead Russian soldiers and notify their families.[24] For example, during the first months of the invasion, Ukrainian intelligence used FRT to protect refugees from provocations by subversive groups, with the technology helping to identify and neutralize 20 Russian subversive groups and detain 350 suspected saboteurs in Lviv. These saboteurs had easily integrated into the local population with the intention of sowing distrust and passing important information to Russia.[25]

FRT has also played a humanitarian role. Border guards were able to identify 50 people involved in the abduction of children from Ukraine using the technology provided by Clearview AI.[26] FRT has become an invaluable tool in the search and identification of missing persons, reuniting separated families. The use of the Clearview mobile app for face scanning at checkpoints and on patrols has become an integral step in not only ensuring security but also addressing the issue of war-related separation.

Another useful application of FRT is in the efforts to identify Russian soldiers involved in war crimes, including incidents such as the killing of civilians and looting in occupied territories. The goal is to contribute to the collection of evidence for potential prosecution in international courts such as the International Criminal Court.[27] For example, in the early stages of the invasion, widespread war crimes were committed by Russian forces, including the atrocities in Bucha. FRT, in combination with social media and open-source intelligence, identified key members of a Russian army battalion involved in the crimes committed in Bucha.

Lately, the Ministry of Internal Affairs has been pushing for the adoption of a draft law that would establish a large-scale video monitoring system across all of Ukraine, ostensibly to enhance public safety. This system would rely on biometric data, such as gathered by facial recognition, to identify individuals and store personal information for up to 15 years under the ministry's control. Cameras would continuously record in public spaces, schools, businesses, and healthcare facilities.

Possible Threats to Democracy and Human Rights

The use of FRT in wartime has implications that could threaten fundamental principles of democracy and human rights in Ukraine. UN High Commissioner for Human Rights Volker Türk has highlighted the potential negative impact of FRT and said that it could lead to "mass surveillance of our public spaces, destroying any concept of privacy".[28]

There are concerns related to Clearview AI, which is the only such system in use in Ukraine now (see below), but even if the government stopped its cooperation with the company and started using any other software, the unchecked power that FRT generally offers can be a powerful tool that violates people's rights and threatens democracy. While other companies such as FindClone, PimEyes, NEC, or Search4faces may adhere more strictly to data-protection standards than others, the general risk of abuse and potential for privacy violations is present across all platforms. For instance, the FRT developed by the Japanese company NEC is renowned for its high ranking in accuracy testing by the US National Institute of Standards and Technology,[29] but there is no guarantee its technology can completely safeguard against the misuse or breaches of personal privacy associated with FRT. The safe and ethical deployment of FRT depends heavily on the specific practices and safeguards implemented by each company. Furthermore, without rigorous oversight and standardization, switching from one technology to another might not mitigate the potential for misuse.

Moreover, if the technology continues to be used after the war ends, unchecked access to vast amounts of resulting data raises the fear that citizens' actions or statements against the government can be tracked. For example, the 15-year data-retention period for the system currently being pushed by the Ministry of Internal Affairs means it would remain in operation long after the war ends, posing serious concerns for civil liberties. This can

deter people from participating in democratic processes, expressing dissent, or participating in demonstrations against government policies. This, in effect, threatens the very foundations of a democratic society, where freedom of speech and the right to protest are sacrosanct. FRT could be used not only to spy on dissidents but also to manipulate or intimidate the population, undermining democratic practices. It could be used to target certain ethnic groups, beliefs systems, leading to discriminatory surveillance and actions that grossly violate human rights. Such discriminatory surveillance and potential actions based on it may grossly violate human rights.

These risks are compounded by the fact that it is often the companies providing FRT that control who can access and utilize the technology, making the system particularly vulnerable during times of war. It is therefore crucial for Ukraine to introduce strong regulation governing the use of FRT for military and civilian purposes, ensuring that any restrictions on civil liberties imposed during the war are lifted once the state of emergency ends.

Another critical concern is that FRT can be prone to error and bias. There have been cases where it has misidentified people, and research has shown that the technology is less accurate when it comes to identifying individuals from certain racial or ethnic groups. For example, the US National Institute of Standards and Technology found that FRT is least accurate when used on women of color.[30] Such biases can lead to discrimination and unequal treatment, further exacerbating the dangers posed by the widespread use of this technology.

Given these risks, transparency, accountability, and rigorous oversight are essential to prevent the long-term erosion of democratic values and human rights in Ukraine.

Concerns About Clearview AI

The use of Clearview AI's FRT has sparked debate and concern, particularly regarding privacy rights, accuracy, and fairness. Human rights organizations and academics in different countries have described the company's system as an extremely intrusive technology. Privacy International has said that its use "represents a significant expansion of the scope of surveillance with a very real potential for abuse".[31] The reliability of Clearview AI as an actor and its adherence to regulatory standards have been questioned, as evidenced by the significant fines it has been given over conflicts with data-protection laws.

Privacy International and other similar organizations have filed several legal complaints against Clearview AI with the regulatory authorities in Austria, France, Greece, Italy, and the United Kingdom. They claim that the company violated numerous provisions of the EU's GDPR, including regarding the processing of sensitive data, lack of transparency, and lack of lawful basis for data processing.[32] Following an investigation, in 2022, France's regulator imposed a €20 million fine on Clearview AI and ordered it to stop collecting and processing data, and to delete data already collected.[33] That same year, Italy took a similar decision, banning web scraping and ordering Clearview AI to delete all data,[34] and the Information Commissioner's Office in the United Kingdom imposed a £7.5 million penalty on the company.[35]

The biggest concern is the potential infringement of the right to data privacy by Clearview AI. By continuously processing huge amounts of data, especially images scraped from social platforms and the internet, often without

users' consent, the company violates the right to privacy, which includes the right to control whether and with whom information about a person is shared.[36] Under EU law, facial images are considered biometric data, which under the GDPR requires explicit consent for processing to ensure unique identification of individuals is protected. Thus, there is a risk that people's expectations of privacy may be negatively affected if they learn that their photos may be collected and stored. Moreover, researchers believe that Clearview AI uses photos from private accounts even if the person concerned does not wish to disclose the information.[37] Its database even contains images "that are no longer public, but were once publicly available", which allows the technology to extract even photos that were deleted. In addition, there is no official way for a person to check whether their image is in the database and to request the removal of such data from there.

When using Clearview, there is always a danger of relying entirely on the system's algorithm to replace human decision-making. Automatic decision-making creates a constant problem of misidentification. In a war context as in Ukraine, this entails the constant danger that the system could make fatal mistakes, such as confusing civilians with soldiers, the seriously wounded with the dead, or Ukrainians with Russian saboteurs. Thus, the military and other security or law-enforcement agencies using the system should clearly refrain from relying on Clearview AI as the sole source of evidence before making decisions.

Another risk is that, since Clearview AI uses images from various Russian sources—prominently VKontakte, the largest Russian social network and a major repository of Russian images—there is the potential for Russian actors to manipulate these inputs to alter search outcomes and undermine the reliability of the technology. By flooding the system with false or doctored images, Russia could thus skew search results, making the technology less accurate and trustworthy when used by Ukraine. This could lead to disinformation, misidentification, and compromised data integrity, posing significant risks for users.

Finally, the fact that Clearview AI's services have been used effectively during the war means a certain legitimization of a dangerous technology, which creates risks of its further use in peacetime Ukraine and other countries.[38]

AI in Information Warfare

Rapidly improving AI technologies enable disinformation and propaganda to be generated and spread on a massive scale and at unprecedented speed. The emergence of generative AI, deepfakes, and voice-cloning technologies has significantly changed the landscape of information warfare, affecting not only military tactics but also the broader political and social dynamics. By generating audiovisual content that is highly realistic yet entirely fabricated, they can erode trust in the media, foster discord within communities, and destabilize the fabric of society. This manipulation of digital content not only challenges the integrity of information but also poses a significant threat to social cohesion and democratic values. Today, in a war context the battle for control over information is as critical as physical combat.

Russia disseminates false narratives through a highly sophisticated and interconnected network that includes state-controlled media outlets, propagandists, troll farms, bots, and cyber-armies. This orchestrated effort is crafted to destabilize Ukraine while eroding the international community's confidence in credible sources of information about the war. Russia's extensive and strategic employment of digital, especially now AI, technologies within this context not only demonstrates their complementarity advancing strategic military objectives but also reveals a broader ambition to reshape the narrative in Ukraine and elsewhere surrounding the conflict in its favor.[39]

Russia's information warfare against Ukraine began well before the 2022 invasion. Before the advent of generative AI, it had already invested over $9 billion in propaganda since 2014, using digital platforms to spread fake media.[40] Initially, Russia spread disinformation through traditional media, but with the invasion it shifted to a hybrid strategy, using advanced technologies in the military and public spheres. These now include AI-driven tools that create deceptive and manipulative content, from deepfakes to false news, that are spread on social media. These are designed to sway public opinion and sow discord in Ukraine, potentially alter the war's course, and even influence Western decisions on providing support to Ukraine.

AI technology enables Russian propagandists more than before to craft highly targeted and persuasive content and emotionally charged narratives that are difficult to distinguish from genuine and fact-based ones. This is evident on platforms like TikTok, where seemingly harmless pages can be fronts for spreading harmful messages. For instance, a TikTok page that appears to be an ordinary account with enticing visuals and engaging content could be operated by Russian propagandists, with the content carefully curated to promote various narratives aimed at undermining Ukrainian society. The three narratives below are key examples.

- **Forced mobilization.** This features AI-generated stories that instill a sense of fear, doom, and injustice in the viewer. The protagonist, often depicted as an ordinary citizen, is shown being forced into military service. This is designed to create anxiety and resistance among the population, making it more susceptible to anti-government sentiments.

- **Corruption among members of parliament.** This involves highlighting instances of corruption—whether real, exaggerated, or entirely fabricated. The goal is to evoke a sense of injustice in the viewer and provoke the thought: "What are we fighting for?" This narrative is then unwittingly picked up by bloggers, who spread the message that "everyone steals." This erodes trust in authorities, leading the audience to question the legitimacy of their leaders and the purpose of Ukraine's struggle.

- **Bribe-taking commanders.** This depicts military leaders as corrupt and indifferent to the plight of ordinary soldiers. The content could portray commanders as enjoying privileges and power while ordinary citizens suffer. Posts under hashtags like #ukraine, #mobilization, and #corruption amplify these messages, spreading the idea that the military leadership is detached from and exploiting the people. This serves to create division and demoralize the public, further weakening societal cohesion.

The goal of such content is to intimidate and demoralize Ukrainians by spreading the false idea that the AFU are constantly losing and that therefore there is no point in fighting anymore. Similarly, in 2022, a deepfake

video showing President Volodymir Zelensky announcing Ukraine's surrender circulated widely on social media, deceiving many who were not familiar with such technology.[41] In 2023, in another deepfake video the AFU's commander-in-chief, Valery Zaluzhny, appeared to call on soldiers to turn around and march on Kyiv.[42]

The ability to generate convincing synthetic voices can be exploited to create false audio tracks of public figures. Many tools and platforms offer voice cloning and fake sound generation, expanding the landscape of synthetic voice technologies. These technologies allow users to create and modify audio outputs to mimic real voices or generate entirely new ones. Voice-cloning technology has often been used to try to provoke a coup in Ukraine. For example, in 2023, a new video message that purported to show Zaluzhny calling for a coup was circulated on the internet and shared by thousands of Ukrainians who believed it was real. The original video was altered using ElevenLabs voice-cloning technology and filled with a typical set of Kremlin tropes, such as: "complete failure on the frontline", "total corruption in Ukraine", "Zelensky's terrorist acts", and "soldiers are being sent to slaughter".[43]

Deepfakes can have a profound impact on public perceptions, particularly when they feature trusted known figures. Individuals exposed to deepfakes are prone to experiencing confusion and doubt, even after false content is debunked.[44] Despite the fact that the abovementioned fake news about Zaluzhnyi was exposed as a fabrication, it had a lingering and destabilizing effect on the public. The resulting erosion of trust in official communications and the exacerbation of societal divisions serve the objective of Russian disinformation campaigns, which aim to create uncertainty, distrust, and chaos within targeted populations. The effectiveness of deepfakes varies across different sociopolitical contexts and is particularly impactful in highly polarized environments with low levels of media trust. Ukraine is a prime example of such a setting. The war has strained public trust and heightened vulnerability to disinformation, creating fertile ground for deepfakes to achieve their intended effects. According to a 2023 study, Ukrainians' trust in local media had decreased from 57% to 29% over the previous year.[45] This increases the susceptibility of the public to deepfake disinformation campaigns, especially when the stakes are high due to the ongoing war.

The war has strained public trust and heightened vulnerability to disinformation, creating fertile ground for deepfakes to achieve their intended effects.

While Russia's AI-enabled manipulative efforts may sometimes appear clumsy or outlandish, they ultimately undermine public trust and create confusion in Ukraine about what is real and what is not. By spreading false, persuasive content, they pose a significant threat to the credibility of information, especially in wartime. This strategy of introducing uncertainty and division enables Russian propagandists to weaken Ukraine's societal resilience, making it more challenging for citizens to maintain a unified stance in the face of the war waged on their country.

Overall, the use of deepfakes in the Ukraine war illustrates the dangerous potential of this AI technologies in armed conflicts. It highlights the need for increased awareness and resilience against disinformation in populations

vulnerable to psychological manipulations aimed at destabilization, where digital deception can be as damaging as physical warfare, and the battle for truth becomes a critical component of national security.

The implications of these cases of use of generative AI and deep fakes go beyond the war in Ukraine. They exemplify a broader change in the landscape of warfare and information dissemination, where digital tools can be used as a weapon to undermine democratic institutions and violate human rights.

Harmonizing Ukrainian Legislation With EU Standards

Amid the ongoing war, a critical element of Ukraine's strategic vision involves deeper integration with the EU, underscored by it being granted membership for membership in 2023. One of the prerequisites for membership is the implementation of comprehensive legislative reforms, including in areas such as personal data protection and AI regulation. The EU's frameworks, including the GDPR and the Artificial Intelligence Act, are benchmarks for Ukraine to ensure that the deployment of new technologies during the war adheres to strict human rights standards.

To align with EU norms and values, Ukraine must revise its laws and possibly enact new ones. This legislative overhaul would not only align with its commitment to EU integration, as stated in the preamble of its constitution, but also bolster its efforts to protect human rights in the use of technology in wartime. Such reforms will enable Ukraine to adopt robust regulations that govern the ethical use of AI and safeguard personal data, ensuring that its legislative framework mirrors the high standards upheld by EU jurisdictions. This alignment is not only a constitutional and political imperative but also crucial for ensuring that technological advancements during the war are managed responsibly and ethically.

In March 2024, the European Parliament adopted the Artificial Intelligence Act as the new legal framework to significantly strengthen the regulation of the development and use of AI.[46] The act establishes rules for AI based on the level of risk they pose. It defines unacceptable-risk AI systems, such as those manipulating behavior or using extensive biometric identification, and bans them, with limited exceptions for law enforcement. High-risk AI systems, which can impact safety or fundamental rights, must undergo rigorous assessment and registration. These include AI in key societal areas such as law enforcement and public services.

In 2020, Ukraine adopted a Concept of Artificial Intelligence Development, yet it still lacks a comprehensive legal framework for AI regulation. To address this, the Expert Committee on the Development of Artificial Intelligence under the Ministry of Digital Transformation is working to establish a robust set of regulations.[47] In June 2024, it developed a White Paper on the regulation of AI, an analytical document aimed at proposing an approach to regulating such technologies.[48]

Meanwhile, Ukraine also faces the challenge of modernizing its significantly outdated data-protection legislation to align it with international standards such as the EU's GDPR. The Law on Personal Data Protection of 2018 lacks

mechanisms for addressing non-compliance with data-processing deadlines and unauthorized data collection, and it does not provide clear guidance on the rights of data subjects or the penalties for violations. Furthermore, it fails to adequately define personal data protection or to distinguish between general and sensitive data categories, leaving sensitive information such as genetic and biometric data under-protected. In addition, no supervisory authority has been established to fully oversee the use of the latest privacy technologies.

Proportionality in Balancing Technology and Human Rights

The balance between national security and transparency in the context of the use of advanced new technologies in warfare is a serious challenge. As Ukraine increasingly relies on such technologies for defense, the line between protecting sensitive information and maintaining public trust is becoming increasingly blurred. On the one hand, national security requires secrecy to protect military strategies, technological innovations, and intelligence operations from potential adversaries. This is vital for maintaining strategic advantage and ensuring the safety of citizens and military personnel. Transparency, on the other hand, is essential for democratic governance, ensuring public oversight, accountability, and ethical assessment of military actions and decisions.[49]

The use of such technologies, especially in the context of international humanitarian law, needs to be critically examined through the lens of proportionality and the strict requirements of the European Convention on Human Rights (ECHR), which Ukraine ratified in 1997. Article 15 of the ECHR allows states, under certain strict conditions, to derogate from their human rights obligations in time of war or public emergency. However, this permission is not unlimited; it requires careful adherence to the principles of necessity and proportionality, especially when it comes to the use of intrusive digital technologies, such as mass surveillance and FRT.

The principle of necessity requires that any measures restricting human rights must be strictly necessary to meet a specific, vital need, such as national security or public safety. The state must demonstrate that such measures are the only way to achieve the desired protection of the nation and its citizens.[50]

The principle of proportionality requires that any derogation from human rights be proportionate to the threat faced. This means that the measures taken must not go beyond what is necessary to address the emergency, and there must be a fair balance between the requirements of the general interest of society and the protection of fundamental human rights.[51]

The European Court of Human Rights (ECtHR) outlines two general requirements for a derogation to be considered “reasonable” under Article 15 of the ECHR:

- There must be a war or other public emergency threatening the life of the nation, in which case any derogation must be strictly required by the exigencies of the situation, and there can be no limitations on non-derogable rights (except for deaths resulting from lawful acts of war).

- The state must notify the secretary general of the Council of Europe about the derogation from obligations, including the measures taken and the reasons for them.[52]

The ECtHR and the Court of Justice of the European Union (CJEU) have consistently emphasized the need for an individual assessment of each case of derogation to prevent abuses of power and arbitrary interference with fundamental rights. This judicial approach emphasizes that human rights do not cease to exist in emergencies, and thus the relevant obligations remain imposed on the state. For example, in cases such as *Lawless v. Ireland (No. 3)*[53] and *Brannigan and McBride v. the United Kingdom*,[54] the ECtHR has justified certain emergency measures due to their specific emergency purpose, provided that they are accompanied by legal safeguards against abuse. This delicate balance reflects the ongoing tension between national security interests and the preservation of democratic principles and human rights in the face of increasingly widespread and sophisticated technological means of surveillance and warfare.

The ECtHR case of *Big Brother Watch and Others v. the United Kingdom*[55] highlighted the balance between national security and privacy rights. The court found that states have the right to collect data in the interest of national security but that there must be adequate safeguards against abuse, including clear legal frameworks, oversight mechanisms and access to remedies for individuals affected by surveillance. In the case of *Klass and Others v. Germany*, the ECtHR also held that states may have the power to carry out surveillance on grounds of national security but that such powers must be accompanied by adequate and effective safeguards against abuse, reflecting the principles of necessity and proportionality.[56]

While states may have the power to restrict and even violate certain human rights in times of war or public emergency, this power is not unlimited.

Thus, while states may have the power to restrict and even violate certain human rights in times of war or public emergency, this power is not unlimited. The principles of necessity and proportionality are critical checks to ensure that any derogation from human rights is justified, targeted, and limited to what is strictly required by the exigencies of the situation. Judicial bodies such as the ECtHR and the CJEU play a key role in overseeing these derogations, ensuring that they do not become a pretext for arbitrary or excessive restrictions on fundamental rights. The balance between ensuring national security and protecting human rights is a delicate one that requires constant monitoring and adjustment in response to new threats and technologies.

However, focusing solely on legal mechanisms and justifications can overlook broader societal impacts. Derogations, particularly those that encroach on privacy and personal freedoms, can erode public trust in government and judicial institutions if perceived as disproportionate or unjustified. Moreover, there is a real danger that these exceptions, once introduced, might become normalized within legal frameworks, shifting the baseline of accepted practices in surveillance and control. This normalization could fundamentally alter citizens' expectations of privacy and freedom, embedding a new level of acceptance for state interference.

Recommendations

Regulatory Frameworks for Remote Sensing

Remote-sensing technologies have emerged as a crucial tool in the war in Ukraine by providing essential evidence for investigating war crimes and enabling comprehensive surveillance of battlefield situations. To ensure these technologies support human rights and democracy without compromising individual freedoms, Ukraine needs to develop guidelines for ensuring that remote-sensing data is used, stored, archived, and transferred in adherence with appropriate legal, technical, and ethical standards. Additionally, there needs to be a specialized centralized agency to oversee the use, storage, and transfer of satellite data. This agency would ensure compliance with international guidelines and frameworks for the responsible use and protection of satellite data, protect data from misuse, enforce strict access controls, and implement advanced network security measures to safeguard against unauthorized surveillance while maintaining data integrity and confidentiality.

A privacy impact assessment of remote-sensing technologies can help identify potential privacy risks and develop strategies to mitigate them. This assessment should prioritize the limitation of data collection to what is strictly necessary for national security or the conduct of judicial proceedings. Additionally, it should ensure the implementation of transparent practices regarding the utilization of these technologies.

Finally, promoting ethical standards and accountability in the deployment of remote-sensing technologies is essential. Establishing clear criteria for their use in surveillance activities, mandating stringent justifications for remote-sensing surveillance, prioritizing human rights, and providing oversight mechanisms to prevent abuse are crucial steps in achieving this balance.

Legal and Ethical Regulation of AI Technologies, Including Facial Recognition

It is essential to establish robust and ethical regulations governing the deployment of AI technologies, including facial recognition, to ensure the protection of human rights and the preservation of democracy in Ukraine, during the war and after it. Drawing inspiration from the EU's Artificial Intelligence Act, Ukraine should establish regulatory "sandboxes": controlled environments that allow for the safe development, testing, and adaptation of AI innovations, including those sourced from abroad. These sandboxes would ensure that AI technologies meet local safety, compliance, and ethical standards before market introduction, while also fostering local innovation, reducing dependency on foreign technologies, and building public trust. Additionally, by providing a structured regulatory framework, Ukraine can attract foreign investment, encourage collaborative development, and position itself as a regional leader in AI.

To establish clear regulatory jurisdiction within AI sandboxes, the government should develop a comprehensive legal framework that defines the boundaries and creates specific laws or guidelines for sandbox operations, addressing AI-related issues like data privacy, cybersecurity, and ethics. A designated lead agency should oversee the sandbox, coordinating with other regulatory bodies and ensuring compliance. Detailed guidelines and protocols must be established for regulated entities. The framework should align with international

standards, incorporating cross-border cooperation where necessary. Stakeholders, including industry experts and the public, should be engaged in the process to ensure transparency and accountability. Finally, the sandbox framework should be continuously monitored and adapted to keep pace with new challenges and technological advancements.

It is critical for Ukraine to harmonize its legislation with EU laws, specifically the AI Act and the GDPR. This involves revising the Law on Personal Data Protection to clearly define personal data, distinguishing between general and sensitive categories, such as racial or ethnic origins, health status, and biometric data, which require stricter handling protocols. Amendments should also mandate explicit and informed consent for data processing, establish stringent conditions for international data transfers, and set a clear framework for addressing data breaches. Ukraine should also establish an independent authority to oversee the implementation of the data-protection legislation to ensure compliance, handle violations, and educate businesses and the public about their rights and responsibilities.

In addition to these measures, Ukraine should adopt a Human Rights, Democracy, and the Rule of Law Impact Assessment of AI Systems framework, as developed by the Council of Europe,[57] to further strengthen the ethical deployment of AI technologies. This framework would guide the evaluation of AI systems, including facial recognition and other advanced technologies, to ensure they do not undermine human rights or democratic processes. The framework would provide comprehensive guidelines for assessing and mitigating potential risks, ensuring that AI systems are deployed in a manner consistent with international human rights standards.

To effectively implement this framework, Ukraine also should develop a national AI impact-assessment protocol tailored to its specific legal and social context, making assessments mandatory for all AI system—especially those used in critical sectors like law enforcement and surveillance— before deployment. Establishing an independent oversight body with the legal authority to enforce regulations, conduct audits, and require regular reporting on AI system performance would enhance accountability and transparency. Additionally, investing in training and capacity-building programs for AI developers, operators, and regulators on the ethical implications of AI and the framework's principles is crucial to ensure these standards are effectively applied. Regulatory frameworks should improve transparency in the use of generative AI, enhance accountability for its misuse, and support research into more effective detection methods.

Collaboration between technology companies, policymakers, educators, and civil society is essential to develop strategies that balance innovation with ethical and security concerns. By setting clear ethical standards for AI development, promoting open dialogue about the responsible use of technology, and investing in research, Ukraine can harness the benefits of AI technologies while minimizing their risks to society. A collaborative approach ensures that innovation progresses in a way that respects human rights and democratic values.

Comprehensive Media Literacy Programs to Counter AI-Generated Disinformation and Propaganda

Mitigating the risks of AI-generated disinformation and propaganda, especially in wartime but also later, requires Ukraine to develop a multifaceted approach that will increase media literacy, clearly delineate the responsibilities

of AI developers and social media platforms, and strengthen the legal framework to effectively manage these challenges. The proliferation of disinformation and propaganda, particularly during the war, threatens democracy and public discourse in the country, a situation exacerbated by the involvement of AI.

First, it is crucial to bolster media-literacy education. Government and educational institutions need to develop and implement comprehensive programs that focus on nurturing critical thinking skills among citizens of all ages, enabling them to evaluate the credibility of information sources, understand the nature and impact of AI-generated disinformation and propaganda, and make informed decisions.

Strengthening the legal framework is essential. Ukraine's government should reevaluate and update its legislation to address the challenges posed by AI and social media in spreading disinformation. This may include enacting or revising laws to hold platforms accountable for the content they disseminate and compelling them to proactively combat disinformation. Regulations could also be introduced to enhance the transparency of content-creation algorithms and the sources of political and thematic advertising.

Collaboration among government bodies, the technology sector, media organizations, and civil society is also crucial for a coordinated response to disinformation. This would facilitate the exchange of best practices, the formulation of ethical AI usage guidelines, and the launch of public-awareness campaigns focused on media literacy. Support for fact-checking organizations and AI-driven disinformation research must also be increased. Providing fact-checking organizations and researchers with the necessary resources to develop advanced tools and methodologies is crucial for keeping pace with the increasingly sophisticated tactics of disinformation. As disinformation evolves, these entities need state-of-the-art technology and innovative strategies to effectively detect and combat false information. Furthermore, ensuring that researchers have greater access to social media data, as advocated by frameworks like the EU Code of Practice on Disinformation, is vital. Such access allows researchers to deeply analyze how disinformation spreads and to craft more effective countermeasures. However, the difficulty in accessing this data due to privacy concerns and platform restrictions highlights the need for Ukraine to work closely with international partners and align with global standards. Such collaboration can help navigate these challenges and improve the effectiveness of efforts to combat disinformation.

Ukraine also must take a lead role in efforts to define the roles and responsibilities of AI developers and social media platforms, exercising political will to coordinate efforts. AI developers should integrate safeguards to counter disinformation, while social media platforms must enhance content moderation and collaborate with fact-checkers. Ukraine can engage in international partnerships and contribute to global discussions on AI ethics and disinformation. By sharing its unique experiences and expertise, it can play a key role in shaping international standards and building capacity. Ultimately, it is in Ukraine's hands to decide its path, while recognizing that global collaboration will also strengthen its own efforts.

Conclusion

Russia's full-scale invasion in 2022 spurred rapid advancements in Ukraine's defense, particularly through the use of cutting-edge digital technologies. This has underscored the strategic advantages and the ethical dilemmas these innovations bring. Technologies like remote sensing, facial recognition, and AI have notably boosted Ukraine's military capabilities and operational strategy. The use of companies like Palantir and of the situational-awareness system Delta have revolutionized the precision and speed of Ukraine's military responses to the Russian invasion, drastically reducing the time needed to coordinate and execute critical operations. However, the advanced technologies involved also present profound challenges and risks for democracy and human rights. This includes threats to privacy from extensive surveillance capabilities, lack of transparency and accountability in technology use, potential for bias and discrimination in automated systems, and shifting decision-making power from humans to algorithms. There are also challenges to privacy connected to the use of facial-recognition technology. Often implemented without the explicit consent of individuals, it enables invasive surveillance and relies on potentially unlawfully acquired data. Furthermore, the lack of transparency in its operations poses additional threats to personal freedoms.

The manipulation of digital content through technologies like generative AI can undermine trust in media, fuel political discord, and destabilize democratic institutions. This erosion of trust is a critical concern that requires urgent attention from Ukraine's policymakers, technologists, and civil society.

As Ukraine continues to use new advanced technologies for its defense, it must also consider the long-term implications of their use, including after the war is over, on democratic values and human rights. A balanced approach that marries technological innovation with ethical considerations and strategic foresight is crucial. This should not only address the immediate needs of warfare but also anticipate the eventual postwar environment in which these technologies could play a positive role in rebuilding democratic institutions and fostering societal cohesion.

Ultimately, the experience of Ukraine underscores the need for an international dialogue on the governance of advanced technologies in warfare and peacebuilding. Such discussions could lead to global standards that help mitigate the risks associated with these technologies while maximizing their potential benefits for society. The war highlights how technology can be used for beneficial strategic military purposes and at the same time pose risks to human rights and democratic principles. This shows the critical need to ethically regulate the use of technological developments to ensure they fulfill legitimate and necessary defense objectives and safeguard fundamental societal values.

Endnotes

1 Taisa Melnyk, "IT Chaos at the Service of the Armed Forces of Ukraine: Hundreds of Thousands of Soldiers Use Various Software Developed by Volunteers – Is Such Decentralization Dangerous?," Forbes Ukraine, November 14, 2022.
2 Military Media Center, Ukraine Unveiled Its Own Delta Situational Awareness System, October 27, 2022.
3 Kateryna Tyshchenko, "Ukrainian Intelligence States That Russia is Preparing for Protracted War," Ukrainska Pravda, February 4, 2023.
4 NATO, NATO releases satellite imagery showing Russian combat troops inside Ukraine, November 26, 2014.
5 Patrick Kroker, "Satellite Imagery as Evidence for International Crimes," International Justice Monitor, April 21, 2015.
6 Syria Justice and Accountability Centre, Investigating Mass Graves Using Satellite Imagery, April 27, 2022.
7 Cora Engelbrecht, "Satellite images show bodies lay in Bucha for weeks, despite Russian claims," The New York Times, April 4, 2022.
8 Ukrinform, Explosion in Olenivka Caused by Thermobaric Grenade Launcher – Office of the Prosecutor General, August 7, 2023.
9 Kyiv School of Economics, The Total Amount of Documented Damages Has Reached $108.3 Billion, Minimum Recovery Needs for Destroyed Assets – $185 Billion, March 23, 2023.
10 Natalia Shapoval, Digital Instruments in Ukrainian Recovery, Kyiv School of Economics, September 2022.
11 uadamage.com project
12 Lisa Gordon, Palantir and Ministry of Digital Transformation of Ukraine Strike Reconstruction Partnership, Palantir Technologies, February 23, 2023.
13 Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab," TIME, February 8, 2024.
14 GSMinfo, It Became Known What Software the Armed Forces of Ukraine Use to Target Enemy Forces, February 6, 2023.
15 Siobhán O'Grady, "Ukraine Is Now the Most Mined Country. It Will Take Decades to Make It Safe," The Washington Post, July 22, 2023.
16 Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab."
17 Information Commissioner's Office, The Use of Live Facial Recognition Technology by Law Enforcement in Public Places, October 2019.
18 R (Bridges) v Chief Constable of South Wales Police and Others, [2019] EWHC 2341 (Administrative Court), paragraph 59.
19 Illinois General Assembly, Biometric Information Privacy Act, 740 ILCS 14, 2008.
20 Office of the Privacy Commissioner of Canada, Guidance on the Use of Biometric Information, February 2011.
21 Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition During War," Reuters, March 13, 2022.
22 Aaron McDade, "Clearview AI Scraped 30 Billion Images from Facebook and Gave Them to Cops," Business Insider, April 2023.
23 Clearview AI, Clearview AI's Mission in Ukraine, 2022.
24 Interview with Diana Khrushcheva, manager of artificial intelligence at the Ministry of Digital Transformation of Ukraine.
25 Maxym Voinov, "Facial Recognition System: Legal Aspects of Use in Ukraine and the EU," Ukrainian Helsinki Human Rights Union, October 4, 2023.
26 Ukrinform, Clearview AI Helped Identify 50 Individuals Involved in the Abduction of Children from Ukraine, April 24, 2023.
27 Interview, Khrushcheva.
28 William McCurdy, "UN High Commissioner Says Facial Recognition Could Lead to Destruction of Privacy," Biometric Update, July 13, 2023.
29 NEC Corporation, NEC's Facial Recognition Technology Ranks First in NIST Benchmark Test with Authentication Accuracy of 99.88%, February 8, 2024.
30 Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," US National Institute of Standards and Technology December 2019.
31 Privacy International, The Clearview-Ukraine Partnership: How Surveillance Companies Exploit War, March 18, 2022.
32 Ibid.
33 European Data Protection Board, French SA Fines Clearview AI EUR 20 Million, October 20, 2022.

34 European Data Protection Board, Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million, March 9, 2022.

35 Information Commissioner's Office, United Kingdom, ICO Fines Facial Recognition Database Company Clearview AI Inc More than £7.5m and Orders UK Data to Be Deleted, May 23, 2022.

36 Camilla Dul, "Facial Recognition and Privacy Concerns," Queen Mary Law Journal, Vol. 3, pp. 1-24, 2022.

37 Interview with Tetiana Avdieieva, lawyer at Digital Security Lab.

38 Interview, Avdieieva.

39 Interview with Valeriia Kovtun, head of the national media literacy project at the Ministry of Culture and Information Policy of Ukraine.

40 Radio Svoboda, "Russia has invested $9 billion in its propaganda," September 16, 2014.

41 MediaSapiens, Russia Is Preparing a Fake Video with Zelenskyy About Alleged Capitulation of Ukraine – Intelligence, March 3, 2022.

42 Olena Kapnik, "Kremlin Propaganda Launched a New Fake About Zaluzhnyi – Details," TSN, March 2, 2024.

43 Ukrinform, "Russians launch fake video about Zelensky," April 21, 2022.

44 Michael Hameleers, Toni G.L.A. van der Meer, and Tom Dobbe, "Distorting the Truth Versus Blatant Lies: The Effects of Different Degrees of Deception in Domestic and Foreign Political Deepfakes," Computers in Human Behavior, Vol. 152, March 2024.

45 Kyiv International Institute of Sociology, The Impact of Russian-Ukrainian War on Political Attitudes of Ukrainians, December 2023.

46 European Artificial Intelligence Act, European Union AI Legislation Portal, 2024.

47 Cabinet of Ministers of Ukraine, Order No. 1556-r, On the Approval of the Concept of Artificial Intelligence Development in Ukraine, Verkhovna Rada of Ukraine, December 2, 2020.

48 Ministry of Digital Transformation of Ukraine, Regulation of Artificial Intelligence in Ukraine: White Paper, June 2024.

49 Interview, Avdieieva.

50 Larry May, War Crimes and Just War, Cambridge University Press, 2007.

51 François Bugnion, "Proportionality," Guide to International Humanitarian Law, 2023.

52 European Court of Human Rights, Guide on Article 15 of the European Convention on Human Rights: Derogation in Time of Emergency, August 2023.

53 European Court of Human Rights, Lawless v. Ireland (No. 3), no. 332/57, July 1, 1961.

54 European Court of Human Rights, Brannigan and McBride v. The United Kingdom, nos. 14553/89 and 14554/89, May 25, 1993.

55 European Court of Human Rights, Big Brother Watch and Others v. The United Kingdom, nos. 58170/13, 62322/14, and 24960/15, Grand Chamber, May 25, 2021.

56 European Court of Human Rights, Klass and Others v. Germany, no. 5029/71, September 6, 1978.

57 Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, September 5, 2024.

Disclaimer

The views expressed in GMF publications and commentary are the views of the author(s) alone.

As a non-partisan and independent research institution, The German Marshall Fund of the United States is committed to research integrity and transparency.

About the Author(s)

Anna Mysyshyn is the co-founder and director of the Institute of Innovative Governance, and she leads projects in Ukraine and Eastern Partnership countries on artificial intelligence (AI), disinformation, cybersecurity, and digital rights. She has a PhD in law from Lviv National University, and an LLM in innovation, technology, and law from the University of Edinburgh, with a focus on the use of satellite images for war-crimes investigations. She has also worked for the UN and UNDP in Ukraine as well as the Parliament of Canada, and she advises various governmental institutions in Ukraine on AI governance.

About the ReThink.CEE Fellowship

As Central and Eastern Europe faces mounting challenges to its democracy, security, and prosperity, fresh intellectual and practical impulses are urgently needed in the region and in the West broadly. For this reason, GMF established the ReThink.CEE Fellowship that supports next-generation policy analysts and civic activists from this critical part of Europe. Through conducting and presenting an original piece of policy research, fellows contribute to better understanding of regional dynamics and to effective policy responses by the transatlantic community.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

Cover photo credit: Parilov | Shutterstock

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

gmfus.org