From Soviet Shadows to Digital Eyes: Civilian Participation and the Transformation of State Surveillance in Ukraine Through the Lens of Foucauldian Discipline and Control

Laner Zhu *

Trinity College School, Port Hope, Canada

* Corresponding Author Email: mlaner26@tcs.on.ca

Abstract. Since gaining independence in 1991, Ukraine has undergone a profound transformation in the nature of state surveillance, shaped by its Soviet legacy, digital innovation, and intensifying conflict with Russia. The widespread adoption of smartphones, social media platforms, and open-source intelligence (OSINT) tools has enabled civilians to become direct contributors to surveillance processes, thereby reshaping traditional power relations between the state and its population. This participatory transformation has become particularly pronounced following the annexation of Crimea in 2014 and the full-scale invasion in 2022, both of which significantly intensified Ukraine's reliance on surveillance technologies under the rationale of national defence. Through smartphone-based reporting, social media activism, and grassroots war crime documentation, civilians now play a pivotal role in intelligence gathering and open-source investigations of alleged human rights violations. This study employs a qualitative methodology--combining historical analysis, case study research, and reviews of legislative and technological developments--to examine the evolution of Ukraine's surveillance apparatus. The analysis is grounded in Michel Foucault's theory of disciplinary power, and supplemented by Gilles Deleuze's concept of "societies of control" and Haggerty and Ericson's "surveillant assemblage". These theoretical lenses reveal a hybrid structure where remnants of centralized, top-down monitoring persist alongside emerging decentralized, data-driven modalities influenced by growing civilian engagement.

Keywords: Surveillance, Ukraine, War, Foucault, Digital Control.

1. Introduction

On May 23, 2022, a Ukrainian court convicted Vadim Shishimarin, a twenty-one-year-old Russian tank unit sergeant of war crimes for killing an unarmed civilian in Chupakhiva. During the trial, Shishimarin explained that he opened fire because the civilian was using a cell phone and his unit feared their location would be exposed [1]. This incident underscores a defining element of modern conflict: civilians, equipped with smartphones and networked technology, can act as both observers and agents in warfare. In Ukraine, this shift has been dramatic. Citizens now document war crimes, report troop movements, and gather battlefield intelligence through digital platforms such as Telegram, TikTok, and mobile government apps. Since the full-scale Russian invasion in 2022, Ukraine's Ministry of Digital Transformation has reported tens of thousands of daily civilian-submitted reports via tools like the Diia app and the "Stop Russian War" chatbot [2]. These actions mark a shift in the surveillance dynamic, where citizens are no longer merely observed but actively contribute to the mechanisms of state monitoring.

This phenomenon is not exclusive to Ukraine but reflects a broader global shift in surveillance culture. It is seen in post 9-11 "vigilant citizen" initiatives like the United States (U.S.) campaign "If You See Something, Say Something", and in revelations from the Snowden leaks exposing mass data collection [3]. However, what sets Ukraine apart is the intensity, scale, and stakes of this participatory surveillance during active warfare. The country's digital infrastructure has enabled civilians to live-stream battles, analyze open-source intelligence, and crowdfund military efforts. Yet, this transformation must be understood through the lens of Ukraine's political history. The legacy of Soviet surveillance, built on centralized authority, informant networks, and spatial control continues to inform institutional practices. What emerges is a hybrid surveillance regime: biometric databases

and telecom intercepts operate alongside decentralized, citizen-driven intelligence gathering. While empowering, this dual model also redistributes risk and responsibility, placing civilians in precarious positions where they may face retaliation or become subject to surveillance themselves [4].

To explore this transformation, this study adopts a theoretical framework rooted in surveillance studies. At its core is Michel Foucault's concept of disciplinary power, articulated through the Panopticon, a metaphor introduced by Jeremy Bentham and adapted by Foucault in Discipline and Punish. The Panopticon produces self-discipline through internalized surveillance, wherein visibility ensures compliance. However, Ukraine's contemporary surveillance practices increasingly align with Gilles Deleuze's "societies of control", where power operates fluidly through algorithmic governance and digital networks. Haggerty and Ericson's notion of the "surveillant assemblage" further illustrates how modern surveillance aggregates fragmented data from multiple sources, reconstituting individuals as "data doubles" in virtual space [5]. These frameworks help interrogate Ukraine's unique fusion of legacy institutional control and decentralized digital participation. This study thus asks: how has the rise of civilian participation reshaped state surveillance in Ukraine since the fall of the Soviet Union, and to what extent does it align with or diverge from Foucauldian theories of disciplinary power in the digital age? The conclusion is that while certain Foucauldian elements endure--particularly the internalization of surveillance and bureaucratic oversight reminiscent of Weber's rational-legal authority--the rise of participatory, digitally mediated surveillance practices has led to a clear divergence. Ukraine's hybrid model, forged in the crucible of war, reveals a reconfiguration of surveillance that empowers civic agency but also deepens civilian vulnerability in the evolving digital landscape.

2. Foucault's Conception of Disciplinary Power

Foucault's conception of disciplinary power represents a profound departure from traditional sovereign power, which relies on visible enforcement of direct punishment. Instead of compelling obedience through coercion, disciplinary power conditions individuals to regulate their own behaviour by embedding systems of control within everyday life, making discipline feel natural rather than imposed. As Foucault asserts in Discipline and Punish, this process unfolds through three interrelated mechanisms: hierarchical observation, normalizing judgment, and examination, all of which contribute to the formation of what he terms as "docile bodies". The first mechanism, hierarchical observation, ensures that individuals remain constantly visible and aware that they may be watched at any moment, compelling them to modify their actions accordingly. This principle is embodied in Bentham's Panopticon, a prison designed so that inmates never know whether they are under surveillance, leading them to regulate their behaviour even in the absence of direct oversight. However, this model extends far beyond prison walls; modern institutions, such as schools, workplaces, and even digital platforms operate all on the same logic, using cameras and algorithmic monitoring to create an environment where individuals internalize the gaze of authority. For instance, employees working under constant surveillance in open-office layouts or through digital tracking software often self-censor and adjust their productivity, not because they are actively being watched, but because the possibility of oversight is enough to ensure compliance. Similarly, normalizing judgment establishes implicit behavioral standards that distinguish between the acceptable and the deviant, reinforcing the idea that those who conform are rewarded, while those who deviate are disciplined. From early childhood, we are forced to follow arbitrary yet deeply ingrained rules, such as brushing our teeth before going to bed each night or raising our hands before speaking in class, without questioning even the necessity of these actions. Over time, these norms become so internalized that we begin to enforce them upon ourselves and others, perpetuating compliance without the need for explicit control. On top of this, the final mechanism, examination, transforms people into objects of knowledge that can be classified, assessed, and adjusted, reinforcing power structures through constant evaluation. School report cards, employee performance reviews, and credit scores function as modern tools of examination, turning individuals into measurable data points

whose worth is determined by institutionalized standards. In contemporary society, digital surveillance amplifies this dynamic, as social media platforms track and analyze behaviour, influencing everything from political opinions to consumer preferences. Individuals, often unaware of the extent to which they are being monitored, gradually conform to the expectations set by these invisible systems of control, reinforcing Foucault's argument that power is most effective when it operates unnoticed. While disciplinary power promotes social order and efficiency, it also curtails autonomy, creativity, and critical thought by making conformity feel instinctive rather than imposed. The most insidious aspect of this power is that individuals do not merely submit to external authority, instead people become complicit in their own regulation, upholding the very structures that limit their freedom without ever perceiving them as constraints.

3. From the Panopticon to Participation: Surveillance Culture from Soviet Roots to Civic Action

Ukraine's surveillance culture cannot be fully understood without tracing its Soviet origins. The Soviet Union developed one of the most pervasive surveillance systems in history, constructing an apparatus designed not merely to collect intelligence but to regulate societal behaviour at every level. Central to this system was the Komitet Gosudarstvennoy Bezopasnosti (KGB). KGB, established in 2954, functioned as the "sword and shield of the Communist Party". By some estimates, the KGB employed over 480,000 personnel--including 200,000 border guards--and oversaw millions of civilian informants [6]. At its peak, the KGB was the largest secret party in the world and was instrumental in constructing a surveillance regime that infiltrated every factor of life, including schools, workplaces, and even homes. The KGB cultivated a vast network of informers. Ordinary citizens were motivated to monitor those around them and to report "suspicious" behaviour. This strategy deliberately fractured communal bonds by eroding social trust and replacing solidarity with suspicion.

As Foucault argues in "Discipline and Punish", this internalization of the disciplinary gaze represents the ultimate success of surveillance power, where external control becomes unnecessary as subjects monitor and regulate themselves--a phenomenon that manifested clearly in Soviet society through what Arendt termed the "atomization" of individuals into isolated, compliant subjects disconnected from authentic social bonds. On top of this, the Main Administration for Safeguarding State Secrets in the Press reviewed all media, censoring any content that deviated from party doctrine. This included books, movies, and even songs. This form of epistemic control exemplifies what Foucault identified as power operating through "regimes of knowledge" or "regimes of truth". This is because the Soviet state monopolizes on truth, ensuring alternative discourses could not gain legitimacy or reach a public audience. Those who strayed from official lines faced severe consequences ranging from imprisonment to execution. This stunted collective intellectual and cultural growth by discouraging innovation, and creative risk-taking. The physical environments in which Soviet citizens lived further reinforced this architecture of surveillance, particularly through communal apartments--kommunalki--where multiple families shared kitchens, bathrooms, and living spaces. This virtually eliminated privacy as conversations could be overheard by neighbours who might have served as informants. This constant exposure blurred boundaries between public and private spheres, producing what scholars like Oleg Kharkhordin have described as a panoptic environment--a real-world manifestation of Jeremy Bentham's Panopticon design later theorized by Foucault as a structure of internalized surveillance where subjects become complicit in their own subjugation [7]. The kommunalki thus functioned as architectural extensions of state power, with spatial design serving political control by creating environments where privacy became impossible and mutual surveillance inevitable. This spatial dimension of Soviet surveillance reinforces Foucault's assertion that disciplinary power operates not only through institutions but through the organization of space itself, creating what Henri Lefebvre would term "representational spaces" that embody and reproduce power relations. The subsequent integration of surveillance into everyday life--from

housing arrangements to workplace organization--demonstrates how thoroughly the Soviet state embedded monitoring mechanisms into the fabric of daily existence, creating what Katherine Verdery describes as "a society organized for conspirative purposes" where ordinary social interactions became suffused with political significance and potential danger. The long-term effects of this comprehensive surveillance regime did not dissipate with the Soviet Union's collapse, as studies of post-Soviet societies indicate that regions subjected to intense repression, particularly under Stalin, continue to exhibit lower levels of social trust and civic participation. For instance, survey data from former Soviet republics show that generalized trust in others remains strikingly low, with confidence in government institutions ranking among the lowest in Europe [8]. Moreover, research has found that individuals in these regions are markedly less likely to engage in voluntary organizations or political activism, with civic participation rates trailing behind those in post-authoritarian states in Europe. The persistent institutional and psychological effects of Soviet authoritarianism, where decades of censorship, monitoring, and ideological conformity atomized citizens and stifled autonomous civic activity, are reflected in these patterns.

After gaining independence in 1991, Ukraine inherited a Soviet-style surveillance apparatus centred on the Security Service of Ukraine (SBU), the successor to the KGB. Throughout the 1990s and early 2000s, state surveillance remained hierarchical and opaque, echoing Michel Foucault's notion of disciplinary power. This strategy deliberately fractured communal bonds by eroding social trust and replacing solidarity with suspicion, as citizens were conditioned to assume that any conversation or privately expressed opinion could be reported to authorities. Consequently, surveillance evolved into a self-sustaining culture where the mere possibility of being observed led to widespread self-censorship, making overt repression almost unnecessary. This dynamic produced what political theorists describe as a "culture of fear" where individuals adjusted behaviour not simply out of legal obligation but due to the ever-present possibility of observation, fostering "performative loyalty" as a coping mechanism wherein individuals would publicly praise the regime and express exaggerated patriotism while harbouring private doubts.

Despite this, Ukraine began to diverge from its Soviet past through gradual reforms. A key milestone was the adoption of modern data protection and identification systems in the 2010s. To offer perspective, Ukraine enacted a personal data protection law in 2010 to align Ukraine's regulatory framework with European Union privacy standards, signalling a growing ambition to democratize surveillance structures and to modernize the state's data governance [9]. The country also introduced biometric passports--mandated for visa-free travel to the European Union by 2017--that embedded fingerprints and facial data into state databases. By the mid-2010s, Ukraine was issuing chip-enabled ID cards and integrating e-governance tools like the Diia platform, facilitating access to public services while expanding the digital reach of state monitoring. While these technologies improved bureaucratic efficiency and public service delivery, they also expanded the scope of state surveillance by integrating data collection into the everyday experiences of citizenship.

However, these reforms did not fully sever Ukraine from its Soviet surveillance inheritance. Institutional memory and bureaucratic habits persisted, especially within the security services and administrative elites. In fact, the longstanding tactic of framing state repression as the rogue actions of secret police rather than deliberate political strategy remained embedded in Ukraine's post-Soviet political culture. Historically, Soviet leaders from Stalin to Khrushchev manipulated this narrative to preserve the legitimacy of the Communist Party. During the Great Terror of 1936-1938, Stalin orchestrated mass purges through NKVD chief Nikolai Ezhov, only to later scapegoat him as the principal perpetrator of the violence--a period later known as the Ezhovshchina. Ezhov's eventual execution in 1938 allowed the regime to distance itself from its own atrocities. Even Khrushchev, in his post-Stalin de-Stalinization campaign, continued to portray the security services as autonomous agents of repression, deflecting responsibility away from the Party itself. This deflection strategy illustrates how authoritarian regimes have historically framed surveillance as an administrative malfunction rather than a systemic feature of governance. In post-Soviet Ukraine, although the architecture of surveillance has modernized and formal legal protections have been introduced,

remnants of this logic persist. State institutions continue to exercise substantial discretionary power, often without sufficient civilian oversight or accountability, highlighting the complex interplay between legacy authoritarian structures and contemporary democratic aspirations.

4. Civilian Surveillance in Wartime Ukraine: Operational Power and Participatory Risk

The transformation of Ukraine's surveillance ecosystem since Russia's full-scale invasion in 2022 has hinged as much on the enlistment of civilian observers as on advances in technology, forging a dynamic that intertwines empowerment with peril. Shortly after the invasion began, Ukraine's Ministry of Digital Transformation issued a virtual "call to arms", urging citizens to document and report Russian troop movements, suspected sabotage, and evidence of war crimes through platforms like the Diia app and Telegram-based bots such as eVorog. Over 200,000 reports were submitted by March 2022, fueling real-time drone strikes, ambushes, and OSINT (open-source intelligence) verification. This unprecedented mobilization exemplifies Mann, Nolan, and Wellman's concept of "sousveillance" --a bottom-up mode of observation that complements traditional top-down oversight. It also illustrates Haggerty and Ericson's "surveillant assemblage", a decentralized network of state, corporate, and civil-society actors merging to create a dense web of mutual scrutiny. Crucially, Ukraine has not restricted its appeals to citizens alone: diaspora communities, international volunteers, and human-rights organizations like Bellingcat have played pivotal roles in collecting, verifying, and disseminating evidence, including geotagged videos of military convoys and facial recognition matches of Russian soldiers using tools such as Clearview AI [10]. The strategic value of this participatory apparatus is difficult to overstate. Ukrainian forces credit civilian inputs with boosting tactical successes, while investigative bodies ranging from Human Rights Watch to the International Criminal Court rely on user-submitted footage to build cases against alleged perpetrators. In this sense, mass civilian involvement has become both a means of immediate defence and a mechanism for shaping international discourse. However, these gains come at significant human cost. Civilians face retaliatory violence if their digital activities are intercepted, especially in contested regions where phone and internet monitoring are pervasive. The psychological burden of conducting surveillance--from the kitchen table, behind makeshift barricades, or under bombardment--further complicates the notion of a purely empowering "digital defense". Lizzie Hughes underscores this tension by pointing out that patriotism, when channeled through smartphones and social media, can metamorphose into a form of militarized vigilance, potentially outlasting the war itself. Reports from the Office of the United Nations High Commissioner for Human Rights show at least 12,910 civilian deaths, including 682 children, and nearly 30,700 injuries in Ukraine from February 2022 to March 2025, alongside the displacement of millions [11]. While it is impossible to attribute each casualty to civilian surveillance efforts, the heightened risks faced by digitally engaged populations render the line between observer and participant all but invisible. The phenomenon illustrates Monahan's argument that surveillance is never merely a technical apparatus: it is a cultural and political practice, rooted in historical legacies and urgent crises. For Ukraine, this cultural practice blends state imperatives with a deeply personal sense of responsibility, placing everyday citizens at the nexus of personal vulnerability.

The annexation of Crimea in 2014 already signaled a pivot toward intensified surveillance, prompting Kyiv to adopt legislation that broadened electronic monitoring, data interception, and forms of content control in an effort to preempt destabilizing activities. But the 2022 invasion dramatically magnified these trends, catapulting Ukraine into a paradigm of participatory surveillance that resonates with broader Western security practices. Post 9/11 programs like the American "If You See Something, Say Something" campaign and the pervasive data gathering exposed by Edward Snowden highlight how liberal democracies increasingly co-opt private citizens into their national security frameworks. Larsson calls this mobilization the rise of "citizen-soldiers", where government hotlines and mobile applications transform everyday technologies into tools of communal oversight.

Ukraine's wartime adoption of these measures heightens the stakes, making each submitted photo, geotag, or IP trace potentially decisive in lethal confrontations. Yet, such practices echo Giorgio Agamben's warning about the "state of exception", wherein emergency laws, introduced under the banner of safeguarding the nation, risk becoming permanent features of governance. Balzacq and Cavelty's notion of "security dispositifs" likewise offers a framework for understanding how extraordinary countermeasures can quietly transition into routine policy, altering the social contract long after the initial crisis subsides. The Diia platform exemplifies this shift, evolving from a digital hub for e-governance and social services into a quasi-intelligence tool capable of crowdsourcing data that may be used for anything from refugee support to strategic targeting. Such capabilities raise worries about civil liberties violations during peacetime, even though they may be advantageous during times of war. The combination of tracking, predictive policing algorithms, and biometric databases indicates a significant increase in the Ukrainian state's monitoring capabilities, which could increase personal insecurity if or when these capabilities continue after the crisis is over. In essence, Ukraine's intensifying reliance on civilian intelligence signals a watershed moment in the militarization of society, forging a model that could resonate in other conflict zones. By fusing patriotic fervor with the ubiquity of smartphones and social media, the Ukrainian government has fashioned a formidable apparatus of citizen-led vigilance. This tool can be used to further war narratives and justice as well as to increase the personal danger. The contradiction of participatory monitoring is exposed by its two-pronged nature: while it makes it possible for regular people to become vital defence and accountability agents, it also blurs the border between civilian life and the front lines of a conflict. The moral, and legal questions emerging from this blurring of roles will likely linger long after the cannons fall silent. As Ukraine proceeds in its struggle against Russian aggression, the practices and policies formed under wartime exigencies could transform into lasting governance mechanisms, bringing into sharp relief the tension between collective security and the sanctity of individual rights. In the end, the Ukrainian experience forces us to reconsider what it means to be a resilient nation in a hyperconnected world and to consider how easily a seemingly empowering form of citizen-driven surveillance can give way to new institutional power structures.

5. Theoretical Convergence and Divergence

Ukraine's surveillance transformation illustrates both convergence with and divergence from established theoretical models. Foucault's conception of disciplinary power, articulated in Discipline and Punish, accurately described Soviet Ukraine's surveillance apparatus with hierarchical observations through informant networks and censorship that produced "docile bodies" through internal discipline. However, post-2014 Ukraine, particularly following Russia's 2022 invasion, has evolved beyond this model toward what Deleuze termed "societies of control." This transition marks a fundamental shift from institutional enclosures to continuous modulation across open networks. No longer confined to physical observation, surveillance now operates through vast data infrastructures that enable real-time tracking and algorithmic governance. Ukraine's implementation of biometric identification, predictive analytics, and facial recognition technologies like Clearview AI exemplifies this shift from disciplinary containment to fluid control. Citizens generate continuous data streams that, as Haggerty and Ericson theorized with their "surveillant assemblage" concept, are extracted, reassembled, and used to create "data doubles" that become the targets of governance strategies predicated on prediction rather than correction.

Within this framework of "control", Ukraine's model diverges significantly through its incorporation of civilian agency and bureaucratic rationalization. Unlike purely top-down or algorithmic surveillance, Ukraine has developed a participatory system where citizens actively contribute to security operations through applications like Diia, geotagging military movements, and participating in OSINT investigations. This citizen-driven dimension operates alongside Weber's theory of bureaucratic rationalization; wherein commercial surveillance technologies are integrated into state security infrastructure based on principles of procedural efficiency and technical superiority.

Further complicating these convergent strands is Foucault's later concept of "governmentality", evident in Ukraine's population-level risk-management strategies, which rely on statistical patterning rather than purely individualized discipline. However, this hybrid approach carries risks that Giorgio Agamben underscores in his "state of exception" concept, where emergency powers introduced for wartime exigencies may become normalized later on. Consequently, platforms like Diia, initially designed for social services, also serve intelligence functions and embed surveillance into everyday life. These enduring arrangements, or "security dispositifs", illustrate how Ukraine's unique context fuses Foucauldian and Deleuze an paradigm while also introducing new forms of citizen-led oversight that intensify, rather than merely displace, traditional mechanisms of control.

6. Conclusion

In conclusion, Ukraine's post-Soviet surveillance transformation demonstrates how civilian participation, enabled by digital technologies, has profoundly altered the balance of power between the state and society while retaining legacies of authoritarian oversight. By actively documenting troop movements, reporting suspicious activities, and gathering evidence of war crimes, ordinary citizens have become indispensable actors in Ukraine's intelligence networks. Moreover, this evolution partially aligns with Michel Foucault's conception of disciplinary power, as it involves a vigilant "gaze" that induces self-regulation. However, it diverges from classical Foucauldian frameworks by incorporating Gilles Deleuze's notion of "societies of control", characterized by algorithmic governance and continuous data flows. Thus, while Ukraine's hybrid model strengthens national defense and informs international legal proceedings, it also increases civilian risks, blurs the line between combatants and observers, and raises questions about the normalization of emergency powers after a conflict. As a result, these advancements highlight how digital engagement can both strengthen extensive control mechanisms and empower societies that face existential threats. In answering the study question, Ukraine's experience shows that while Foucauldian paradigms are still important for examining surveillance, they need to be broadened to include networked, participatory mechanisms that alter democratic norms and accountability in situations well outside of conflict.

References

[1] Pietsch, B., Dixon, R., & Suliman. A Russian soldier is sentenced to life for killing a civilian. The Washington Post. 2023. Information on: https://www.washingtonpost.com/world/2022/05/23/ukraine-war-crimes-shishimarin-russia/.

[2] Harwell, D. Ukraine's digital army is harnessing the internet to fight Russia. The Washington Post. 2022. Information on: https://www.washingtonpost.com/technology/2022/03/10/ukraine-civilian-surveillance/.

[3] Lyon, D. Surveillance. Snowden, and big data: Capacities, consequences, critique. Big Data & Society, 2014, 1 (2): 1 - 13.

[4] Hogue, S. Civilian surveillance in the war in Ukraine: Mobilizing the agency of the observers of war. Surveillance & Society, 2023, 21 (1): 109 - 113.

[5] Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. The British Journal of Sociology, 51 (4), 605 – 622.

[6] Knight, A. The KGB: Police and politics in the Soviet Union. Unwin Hyman, 1993.

[7] Kharkhordin, O. The collective and the individual in Russia: A study of practices. University of California Press, 1999.

[8] Rose, R., & Mishler, W. Comparing democratic values in consolidated and unconsolidated democracies. In D. Pollack, J. Jacobs, O. Müller, & G. Pickel (Eds.), Political culture in post-communist Europe, 2005: 73 - 93.

[9] Bohdan, S. Ukraine adopts new law on personal data protection. Privacy Laws & Business International Report, 2011, 110: 16 - 17.

[10] Murgia, M. Ukraine uses Clearview AI to identify dead Russian soldiers. Financial Times. 2022. Information on: https://www.ft.com/content/bc9eec79-04aa-4a8f-b6fc-bd9023d98c71.

[11] Office of the United Nations High Commissioner for Human Rights. Report on civilian casualties in Ukraine from February 2022 to March 2025. 2025. Information on: https://www.ohchr.org/en/documents/reports/report-civilian-casualties-ukraine-february-2022-march-2025.